THE US-CCU CYBER-SECURITY MATRIX

A New Type of Check List for Defending Against Cyber Attacks

Scott Borg and John Bumgarner

DRAFT VERSION 2

This is a second *draft version* of the US-CCU's new cyber-security matrix being offered for comments. Any suggestions for making this document better or more complete will be very welcome. People who offer suggestions that result in additions or changes will be acknowledged in the final version. Please e-mail comments to: checklist@usccu.us

The final, revised version will be released in 2017. In the final version, all the recommended security measures will be assigned reference numbers and marked to indicate the degree to which they should be made standard practice, given the security tools currently available.

The U.S. Cyber Consequences Unit (US-CCU) is a 501c3 charity. Financial contributions to fund this project are tax deductible and will be conspicuously acknowledged on the final version. *eBay* provided some early funding, for which the authors are very grateful. All subsequent work on this check list over the last several years was unpaid, with the authors' covering all of the expenses themselves. There are considerable costs still to come, including printing and translation costs. The final version of this matrix will display the logos of the companies that supported this work.

THE US-CCU CYBER-SECURITY MATRIX

A New Type of Check List for Defending Against Cyber Attacks

Scott Borg and John Bumgarner

 Draft Version 2

CONTENTS

INTRODUCTION

The Purpose of This Cyber-Security Matrix

This is a cyber-security check list for people who want to seize every possible opportunity to protect their organizations from damage due to cyber attacks. This check list does not treat cyber security as a discipline primarily concerned with maintaining information systems in some supposedly secure state. It doesn't treat cyber security, for example, as a discipline concerned with maintaining the confidentiality, integrity, and availability of systems. Instead, this check list treats cyber security, at an operational level, as a discipline concerned with foiling attackers. This means looking at all the things an attacker needs to do to carry out a successful attack and making these things harder. The idea is to stop the attackers from achieving whatever it is they want to achieve, to increase their costs by as large a factor as possible, to make sure that even if attackers succeed in accomplishing one phase on an attack, they are unable to do any significant damage.

This is a check list for people who want to look outward, at what attacks are coming and how to stop them from succeeding. It is not for people who want to look inward, at the condition of their own systems. This means that this check list is not for everyone. If you just want to show that you're compliant with some standard, that you've gone through the motions enough to fulfill legal obligations, then you should look elsewhere. If you just want to follow standard industry practices, leaving your organization just as vulnerable as other comparable organizations, then you won't want to consider all the additional security measures suggested here. On the other hand, if you're interested in introducing new security measures, designed to block attackers in new ways, while still employing all the old measures that actually work against today's attackers, then this is a document you are likely to find useful.

The underlying agenda of this check list is to push the practice of cyber security beyond "check list thinking." Instead of checking off boxes as each security measure is put into place, this check list is intended to make those using it think constantly about *why* they are carrying out each security measure and *what else* they could do to achieve that goal. Nearly all the corporations and government agencies that have suffered terrible losses from cyber attacks over the last several years were compliant with all the best known cyber-security standards and government guidelines. They had purchased the standard cyber-security tools. They had

"benchmarked" what they were doing, based on what similar organizations were doing. They were following what they believed were "industry best practices." They had "checked all the boxes." But this didn't prevent major cyber-security failures. One of the main reasons is that the people responsible weren't thinking about cyber security enough as a two player game. They focused on their own form, on perfecting their own practices. They were like a tennis player who concentrates on performing every stroke perfectly, but forgets that the purpose of these strokes is to defeat an opponent. They especially forgot to consider what an adversary would do in response to the things they were doing. The organization and content of this new check list is designed to push past this state of affairs. To accomplish this, it has adopted a different scope and a different organization than previous check lists. The effect of these differences is so great that it seems to warrant calling this new tool a "matrix," rather than a "check list."

The Scope of This Cyber-Security Matrix

This cyber-security matrix attempts to incorporate a much wider range of security measures than can be currently found in any other document. In fact, it aspires to encompass virtually *every* cost-effective measure a cyber security professional can take that will genuinely reduce vulnerabilities.

Most previous cyber-security check lists have been limited by four implicit assumptions:

1) They have assumed that the primary job of cyber security is to prevent systems from being penetrated.

2) They have assumed that defensive measures need to stop attackers completely.

3) They have assumed that good security measures are the sort that could be made mandatory.

4) They have assumed that their main job is to deal with the sorts of cyber attacks that have already proved to be a problem.

All four of these assumptions sound reasonable, but they have been far more limiting than most people in cyber-security have realized.

This new cyber-security matrix treats all four of these assumptions as far too restrictive. It attempts to push past these limiting assumptions by paying special attention to many kinds of security measures that these assumptions exclude.

First, this matrix includes many security measures that have nothing to do with stopping penetration. So much of past and present cyber security has been

concerned with preventing systems from being penetrated that it is easy to lose sight of how restrictive this focus it. When a system has been penetrated, security people often say, "Game Over!" as though a successful penetration means that the attackers have won and the defenders have lost. But the attackers had to do other things *before* penetrating the system, and, in order to benefit from their attack, they will have to do even more things *after* penetrating the system. This means there are many other opportunities and ways to stop an attack from succeeding. This matrix gives these other defensive opportunities even more attention than it gives to stopping penetration.

Second, this matrix includes many measures that are designed, not to stop attackers completely, but simply to increase their costs or reduce their gains. Cyber-security professionals often assume that if a defensive measure won't block or stop an attacker activity entirely, it should be considered ineffective. They conclude that such defensive measures aren't worth implementing, because they "don't work." But this is another case where many defenders don't understand the game being played. Cyber attackers can nearly always accomplish their immediate objective if they are willing and able to spend enough resources on achieving this. If the game is about stopping all attacks, the defenders lose. Fortunately, that isn't the game being played. Attackers need to minimize their costs and maximize their returns. They lose whenever their costs become too great or their returns too little. This means that *no defensive measure can be said to have failed if it substantially increases attacker costs or reduces attacker returns.* Appreciating this fact opens up a whole realm of defensive actions that have previously been neglected.

Third, this matrix includes many valuable security measures that it wouldn't be practical to make mandatory. Most cyber-security check lists consist mainly of measures that can be applied relatively mechanically and verified relatively mechanically. This is a good idea if the measures are going to be made legal requirements or items on an audit list. It is especially useful if the people who need to implement the security measures don't really want to implement them and are going to do as little as possible. But this attitude can cause many important measures to be omitted, because they can't be implemented mechanically, because they would be difficult to define legally, or because they shouldn't be required of every organization in every situation. Some of the most valuable security measures need to be applied with considerable discretion. They need to be implemented wherever it is cost-effective to do so. They require a bit of creative ingenuity to put into operation. They shouldn't be made into a fixed requirement and applied indiscriminately. But they shouldn't be neglected either.

Fourth, this matrix includes many security measures designed to deal with problems that haven't arisen yet. If defenders focus too exclusively on cyber attacks that have already proven to be a problem, they will be left unprepared for the more

destructive attacks that they actually face. In cyber security, the types, targets, and methods of attack change every three or four years. What's more, it's the new kinds of attacks that often do the most damage. Waiting until a given type of attack has proved to be a problem before taking steps to defend against it almost guarantees major security failures. It's true that there is no point in defending against attacks that no one would want to carry out. But it is not hard to identify attacks that we haven't seen yet, but that would be tempting for certain attackers. This new matrix includes many new security measures that were chosen on the grounds that they provide a cost-effective way of impeding or stopping likely future attacks.

Despite its comprehensiveness, this matrix is *not* a compilation of every cyber security measure in current use. It does not include all the items on some of the most widely used check lists. It even omits a few security measures that are currently in use in most large organizations. This is because the US-CCU has concluded that these omitted measures are either ineffective or else much too costly for the limited benefits they deliver. In many cases, this is because there are now other security measures that do the same job much better. Security measures that are outdated or misguided can be an actual impediment to good security practices. They create a false sense of security. They absorb resources that are better spent elsewhere. They create unnecessary complexity in which new vulnerabilities can arise and in which more important measures can get lost. Hence, if there is some fairly obvious security measure that this matrix has omitted, it was probably omitted on purpose.

Throughout this matrix, care has also been taken to avoid repeating items, just because they might seem relevant to more than one heading. It is assumed if someone using this matrix reads a question under one heading, that person will not need to read it again under a different heading. Statements about software and operating system security, for example, need to be applied to software and operating systems everywhere: in network servers, in the cloud, in automated control systems, and elsewhere. Statements about network security need to be applied to networks everywhere. If an equivalent question occasionally appears in more than one part of this matrix, this is because the measure in question needs to be carried out very differently in those different contexts, or because it often gets overlooked in one of those contexts.

It should be apparent that, despite its radical intentions, this matrix includes an enormous number of very familiar security measures. The main purpose of any security check list is to avoid missing things. Cyber-security writers and speakers sometimes compare cyber-security check lists to the check lists that even the most experienced pilots run through before take-off and landing. The point of a check list is not to be full of surprising ideas, although this check list aims to introduce some new ones. The point of a check list is to make sure that everything that needs to be

done *is* done. This means that the greater portion of any check list should consist of security basics. In fact, a lot of the check list should look like "Security 101." Furthermore, if a check list is well organized, many of the items it contains will seem obvious or commonsensical, in the context of the list. Even if an item on a check list is something you've never thought of before, once it has been pointed out, it should usually seem that it should have been obvious. The real value of a security check list, especially a new one, comes from the small number of items that a defender would have simply forgotten or never thought of, were it not for the list. Often just one item a defender would otherwise have missed will repay, many times over, the time spent going through the entire list.

The Need to Make Cyber Security Selective and Customized

The unprecedented comprehensiveness of this cyber-security matrix means that each item in it needs to be regarded in a new way. In the past, the items in cyber-security check lists were intended merely as instructions to be followed. The assumption was that everybody needs to do the same things to secure their information systems. This new cyber-security matrix no longer makes that assumption. Instead of treating every item simply as an instruction to be followed, this matrix asks cyber-security practitioners to be aware of the context in which they are operating and to be selective about what they do.

A truly useful cyber-security check list can no longer consist entirely of security measures that every organization should carry out. Cyber attackers have learned how to circumvent most of the basic security measures included in standard check lists. In fact, they do it all the time. This means that many new cyber-security measures are now needed. Because the attack techniques have become more sophisticated, many of these new security measures will also need to be more sophisticated. This creates a problem. Once we move beyond the basics, the number of things we could potentially do to improve cyber security become very numerous. Many of these new security options are also quite expensive. It is no long practical to implement every good security measure, everywhere, all the time. To be cost-effective, security measures need to be applied selectively.

Some cyber-security vendors and consultants have tried to deal with this situation without abandoning the idea that there is one set of security instructions everyone should follow. They have divided cyber-security measures into groups, according to which ones they think are a higher priority. Then they have advised all organizations, regardless of their type or industry, to work their way through these groups, adding security measures in a prescribed order. The successive groups are often described as "maturity levels." This is great for people selling security tools and services, because once an organization has bought all the tools and services for

one security level, it can then be sold all the tools and services for the next security level. This approach is tempting for organizations, because it tells them what to do about cyber security and the order in which to do it. If every organization followed this sort of program, they would all eventually arrive at the highest maturity level, at which point they would all be implementing all the same security measures.

The problem with this one-size-fits-all approach is that different organizations have very different security needs and priorities. What one organization needs to do as quickly as possible might be something another organization can afford to postpone for years or perhaps never do at all. What is cost-effective for one organization may simply not be cost-effective for another.

Different organizations need to protect different things. They create value in different places and by different means. Even companies that seem to be producing very similar products will often achieve their competitive advantages in different ways. The proprietary information that different companies most need to protect will be of different kinds and reside in different places. Different companies also face very different types of potential liabilities from cyber attacks. Carrying out the same operations in different locations can result in very different hazards if something goes wrong. The ways and places in which cyber attacks could cause the greatest losses are extremely different from one organization to another.

Different organizations face different sorts of attacks. The kinds of cyber attackers that go after different organizations will often have little in common. Attackers that regard one company as a prime target may have little interest in attacking another, similar company, simply because its public image or location is different. Different attackers will also employ different attack tools. Attackers who want to do physical damage to industrial equipment, for example, will employ very different tools than attackers who want to steal credit card information from a chain of retail stores. The kinds of cyber attacks one organization has to deal with will often be extremely different from the ones another organization must confront.

Different organizations will have different security costs, even for the same security measure. The cost of putting a new security measure into operation can vary enormously, depending on what components are already in place. To implement a security measure, one company might need to buy many expensive pieces of electronic equipment. To accomplish the same thing, another company might only need to make small adjustments in the equipment it is already running. Implementing the same security measure will also place different burdens on the users of an information system, depending on what those users are doing. In some businesses, the slight delay caused by an encryption program, for example, will be of no consequence. In other businesses, where fractions of a second matter, even a slight delay might be a major problem. The cost of any security measure, both in

direct expenditures and in time and trouble, will typically be quite different for different companies.

All of these factors make it essential to tailor cyber-security measures to the needs of the specific organization in question. There is no single set of security measures that will fit different industries or even different companies. There is no sequence of implementation stages or "maturity levels" that would be appropriate for different organizations. Every industry and organization has different priorities that its cyber security personnel need to take into account.

To tailor cyber security measures to a particular organization, it is necessary to start with a much longer list of security measures than the organization will want to employ. An organization can't invent its list of cyber security measures from scratch. What it *can* do is start with a much longer list and then winnow the list down until it fits the organization's needs quite closely. If an organization has a longer list to choose from, it can also select some measures to implement immediately, others to implement later, and perhaps others to implement later still. This is why this US-CCU Cyber-Security matrix is much longer than any previous list intended for general use. Even mid-sized corporations and small government agencies now need a much larger selection of security measures from which to craft their own cyber-security programs. The era of one-size-fits-all cyber security is over.

The Organization of This Cyber-Security Matrix

In order to make cyber-security measures outward looking and directed at foiling attacks, this check list is organized in a new way. Hence, this new check list should be thought of, not as a list at all, but as an enormous grid or matrix. It can't be printed that way, because the matrix is simply too large and too unevenly populated. But to find your way through it and to derive many of the benefits of the concepts that structure the list, it will be necessary to keep in mind where each item is located in the larger matrix structure.

To make the organization of this matrix clear, we will first outline how it is laid out. Then we will go back and explain reasons for this structure and how it can be used to improve security.

One dimension of this matrix is defined by the things a cyber attacker needs to do to carry out a successful attack. There are five basic things that a successful cyber attack needs to do:

1) *Find* the target.

2) *Penetrate* the target.

3) *Co-opt* the target in some way.

4) *Conceal* what is being done.

5) *Make* the attack's effect *irreversible*.

These are the five actions that any attacker always needs to perform in order to benefit from the attack. Occasionally, one of these actions will be trivial, but usually they will each require an attacker to go to considerable trouble. Sometimes one of these actions will need to be carried out several times in order for an attacker to succeed. This is usually true, for example, where there are layered defenses. Whatever the exact circumstances, each of these actions will need to be carried out successfully at least once or the cyber attack will fail.

These five categories should be interpreted as encompassing a wider range of attacker activities than some of the other attempts to divide attacks into separate steps. This is because most of those other attempts to describe successive attack stages are really just about penetration. They describe the things an attacker needs to do to prepare to penetrate a system, to penetrate the system, and to maintain the ability to penetrate the system. They don't take into account all the other things that an attacker must do to benefit or profit from an attack.

The other dimension of the matrix is defined by the various components of information systems. There are six basic categories of components in information systems:

1) Hardware

2) Software

3) Networks

4) Automation

5) Human Users

6) Suppliers

These are the six types of components that a defender needs to secure. In fact, to prevent a given type of attack from succeeding, a defender will usually need to secure all of these types of components to some degree. We will add further subdivisions to each of these component types to make them easier to handle. These subdivisions include a few information system components that are added for security purposes. Those security systems need to be secured, just like everything else. But the six main component categories are the ones to keep in mind.

The one category of components that might not be familiar to all information technology and cyber-security professionals is "Automation." This category should be understood as comprised of all the automatic or semi-automatic equipment that is controlled by computers. This includes industrial equipment, peripheral devices, data back-up devices, smart appliances, networked medical devices, smart

thermostats, modern airplanes and automobiles, railway switches, gaming equipment, robots, and drones. In general, anything that employs sensors, actuators, or device drivers falls under the heading of "Automation." Most of "the Internet of Things" belongs in this category of information system components.

The five things an attacker needs to do and the six types of components a defender needs to secure can be usefully combined into a five-by-six vulnerability grid. The attack steps can be understood as running across the top, and the component types can be understood as running down the side. All the things an attacker can do to carry out an attack can be located in this grid. All the things a defender can do to foil an attack can also be located in this grid. In effect, all the areas on this grid correspond to potential vulnerabilities that can be exploited by an attacker or secured against exploitation by a defender.

THE COMPREHENSIVE VULNERABILITY GRID **(BORG FRAMEWORK)**					
	Find	**Penetrate**	**Co-opt**	**Conceal**	**Make Irreversible**
Hardware					
Software					
Networks					
Automation					
Users					
Suppliers					

This grid has been amended slightly to provide the matrix structure for this current check list. In addition to looking at each information system component in terms of the attack categories, it is useful to look at how one would obtain an *overview* of that component. Hence, there is a sixth "administrative" or "survey" category that has been added for each component type. The headings have also been changed slightly to emphasize defense.

THE US-CCU CYBER-SECURITY MATRIX						
	Overview	**Harder to Find**	**Harder to Penetrate**	**Harder to Co-opt**	**Harder to Conceal**	**More Reversible**
Hardware						
Software						
Networks						
Automation						
Users						
Suppliers						

An attacker would normally go through this matrix by focusing on the successive steps in carrying out an attack. This is because carrying out an attack step, such as penetration, against one type of component will often make it easier or even unnecessary to carry out that same step against another type of component. Focusing on attack steps would mean reading each successive column in the matrix, top to bottom.

A defender, on the other hand, would normally implement security measures by focusing successively on each type of information system component. This is because it is generally more efficient to do all the things that will help to secure a given type of component, such as the hardware, before moving on to the next type of component, such as the software. Focusing on components would mean reading each successive row in the matrix, left to right.

Since it is useful for a defender to look at the defenses from the standpoint of *both* attackers *and* defenders, the items in the matrix are all included *twice* in this printed (or printable) version. First, the matrix items are arranged in the order in which an attacker would approach them. This is the best way to read the matrix if the goal is to think creatively about ways to foil attackers. It's the best way to approach the defensive options when the purpose is to choose which ones will be most useful in stopping an attacker from successfully manipulating the systems being defended.

Then, second, the matrix items are arranged in the order in which a defender would approach them. This is the best way to read the matrix if the goal is to implement cyber-security measures after they have already been chosen. It's also the best way to make sure that each information system component is being dealt with in a comprehensive enough way. Together, these two ways of ordering the defensive options, if used successively, will allow defenders to seize many opportunities to foil attackers that they might otherwise have missed.

How This Cyber-Security Matrix Can Be Used to Provide Better Defenses

The greatest advantage of this organizational scheme is that it puts every defensive measure under a heading that identifies the attacker action it is designed to foil. This should help to make defenders constantly aware of the *purpose* of each thing they are doing. To implement a security measure in an effective way, it is important to think about what that measure is designed to accomplish. If defenders lose sight of this, it is easy for them to allow some detail in the way a security measure is applied to undercut its effectiveness. Even more important, defenders should be constantly asking themselves whether a given defensive measure will work in the specific context in which it is being applied, or whether there are other measures that need to be taken to achieve the desired effect in that context.

Cyber-security measures should never be applied mechanically. Making them work often requires considerable insight and ingenuity. It requires the defender to think in terms of overall systems, not just individual items. The matrix organization of this check list is designed to encourage those qualities. It is also designed to do more than that. Making the purpose of each group of security measures explicit is intended to encourage active, creative thinking about ways to achieve that purpose.

To institute effective cyber defenses, it is important to think about what the attacker needs to do and, then, what can be done to make it much harder for that attacker to do that. Using the word "foil" in this context can be helpful. Attackers can be "foiled" in many ways. Stopping an attacker from carrying out an attack step is only one way to foil an attack. Often the best strategy will be to make the attacker's action less effective or more costly. Thinking about making attacks *harder*, rather than simply stopping them, is essential if we are going to expand our defensive options. This point deserves as much emphasis as we can give it.

Targets can be made *harder to find* in a variety of ways. We can make it more difficult for the attacker to discover that the organization in question is one they could benefit by attacking. By this and by other means, we might be able prevent an attacker from even noticing a promising target. We can cause the attacker to spend much more time searching, researching, and mapping. We can force the attacker to start this process over again by changing things, so that the attacker's previous

research is now obsolete. "Finding the target" should be interpreted to include finding out enough about the target to determine whether and how to attack it. There are many ways to make the exact features of a target much more difficult to research, observe, or deduce. Even if the attacker can potentially find the target, we can cause the attacker to waste time and resources on other, dummy targets that don't yield anything. In effect, we can make it harder for the attacker to find out which is the right target. We can also do other things that will increase the chance of the attacker coming up empty. In some cases, we can cause an attacker to uncover bogus information that will yield no returns or, worse, cause harm to anyone trying to utilize it. This can cause an attacker to spend additional time trying to find out if the information the attacker has obtained is authentic. Making a target harder to find does not mean "security by obscurity." If we have a genuinely effective way of making targets harder to find, we can announce what we are doing without diminishing its effectiveness.

Targets can be made *harder to penetrate* in a variety of ways. We can make it harder for the attacker to impersonate some person or some system that is allowed access to the target. We can utilize more sources and types of information to determine whether the person trying to obtain access to a system is who that person claims to be. We can cause the attacker to employ more elaborate and expensive tools to get through a barrier. We can require the attacker to penetrate more successive barriers or layers. We can reduce the attacker's ability to move laterally in order to circumvent barriers. These are mostly things that we are already doing fairly routinely. But if we think about ways to make penetration harder, rather than simply stopping it, there are more measures we can put in place to accomplish this.

Targets can be made *harder to co-opt* in a variety of ways. A successful cyber attack needs to co-opt an information system by utilizing it in some way that its designers and owners didn't intend. This can be as subtle a thing as siphoning information off the system or as bold a thing as inserting instructions into the system that will hijack it entirely. But regardless of how an attacker hopes to co-opt the system, there are ways to make it harder. We can make it harder for the attacker to understand how the system works. We can limit the attacker's ability to discover exactly how internal operations are carried out. We can reduce the variety of ways in which the system can be manipulated. We can limit the extent to which the system can be changed. We can make the system continually self-correcting or self-restoring. We can make it necessary for the attacker to go through more steps to co-opt the system.

Attacks can be made *harder to conceal* in a variety of ways. We can look for more symptoms and types of attacker activity. We can monitor more features of normal activity, so that that we can spot deviations from normal activity sooner. We can use human insights to define normal activity more narrowly. We can check to see if

more features of normal activity that are supposed to correlate do, in fact, correlate. We can lure attackers into doing more things that will betray their presence. We can make our detection efforts harder to subvert. We can force the attacker to carry out more steps to conceal what is being done. By doing these things, we can make it possible to interrupt the attack activity sooner, so that both the effects and the benefits to the attacker are greatly reduced.

Attacks can be made *more reversible* in a variety of ways. We can go through all the effects of a given attack and find more ways to undo them. We can improve the systems and activities that substitute for the normal ones in the event of an attack. We can capture and preserve more of the information and conditions that are disrupted as a result of an attack. We can find ways to return to normal functioning faster. We can reduce the gains to the attacker by finding ways to take away the benefits the attacker has achieved. Poisoning some of the proprietary software, documents, or data that an attacker might steal is one way to reverse the benefits to the attacker. Some of these measures are not always regarded as cyber defenses, because they are concerned with reducing adverse effects that would take place long after cyber defenses have supposedly failed. But this kind of thinking needs to be integrated into cyber defense to prevent many defensive opportunities from being overlooked.

This cyber-security matrix can be used as a guide for the creation, sales, and purchasing of cyber-security tools and services. Security vendors will be able to find many places in this matrix where security products that are greatly needed are not yet commercially available in an easy-to-use form. Security sales teams will be able to use this matrix as an effective vehicle for describing and explaining the suites of tools and services that they are offering to customers. Prospective purchasers should find this matrix an effective way of identifying and describing what they need to buy. Security products that perform overlapping tasks can be readily compared by locating the various things that they do in this matrix. Highlighting, in this matrix, the tasks accomplished by the security products that a company is currently using will make clear what additional security products are needed, even when the security tasks are numerous and collectively rather complicated. Most of all, this matrix should illuminate the ways in which security products need to be chosen and employed together, in order to prevent attackers from achieving their goals.

This cyber-security matrix should be used, not just as a guide for implementing the security measures it already contains, but as a framework for devising new measures. In other words, in addition to its immediate use as a practical tool, this cyber-security matrix should be taken as an invitation to engage in some collective brainstorming. Some commentators have declared that cyber security has reached a dead end. If this sometimes appears to be true, it is because cyber security has focused too much on preventing penetration, and because it has assumed that every

security measure has to work completely in order to be deemed successful. Once these constraints are thrown aside, many new defensive opportunities become available. It is the authors' conviction that far more defensive measures are ready to be discovered or invented than have so far been identified.

How This Cyber-Security Matrix Can Be Used to Analyze Attack Paths and Costs

The cyber-security matrix presented here can be used to analyze the cyber-security activities much the way one might analyze a large and complex game. The basic matrix can be used as a map of the playing field. This is because it can be used to locate all the obstacles an attacker might need to overcome and the successive actions connecting them. The horizontal rows represent the different information system locations where attack activities are focused and where the attacker might face obstacles. The vertical columns represent different stages in the sequence of an attack. The general matrix can be adapted for a specific case by populating it with the obstacles that are actually in place and identifying the actual pathways that connect the successive actions that an attacker might want to carry out. Once the matrix has been customized in this way, it represents the terrain in which the actual game of cyber attack and defense is played out.

The attacker will generally move across the matrix from left to right, completing the five successive steps necessary to carry out a successful attack and reach a payoff. Often, when there are layers of defenses, or when the systems under attack are fairly complex, the attacker will need to cycle through some of the attack steps more than once. An attacker might need to carry out as many as three or four of the steps several times, before moving on to the fifth step of doing something irreversible. Carrying out one of the attack steps successfully will provide a basis for carrying out the next step in the sequence. Finding a system (and finding out enough about it) provides a basis for penetrating it; penetrating a system provides a basis for co-opting it; and so on.

Carrying out one attack step will usually limit the options for the next step. If the attacker has penetrated a specific system, for example, she may have only set herself up to co-opt that one system. Vertical movement within a given attack phase can often open up more options for the next attack phase. Hence, the attacker may want to move vertically or laterally to expand the options for going forward. An attacker who finds out about one system, for example, may want to use that as a basis for finding out about other systems, rather than moving directly to penetration. An attacker who has penetrated one system may use that as a basis for penetrating another system, and then another system after that, until finally reaching a system

she wants to co-opt. The progression from left to right across the matrix rarely looks like a straight line.

Every move the attacker makes will have a cost in time, skill, and sometimes in equipment. The attacker will try to choose whichever pathways and obstacles can be overcome at the lowest cost to achieve the desired payoff. The attacker might not have enough knowledge of the specific matrix where the attack is being played out to make very good choices without a lot of trial and error. But unless the defender changes the matrix enough to restart part of the game, the attacker will gradually move toward a more optimum set of pathways.

A defender who knows the matrix can look at the available pathways and tell which ones the attacker is likely to try to follow. Then the defender can add up the cost in time and skill of overcoming the successive obstacles in those pathways. The defender can even estimate the expenditures in time and skill needed to identify a given low-cost pathway. This means that the defender can use this matrix-based analysis to estimate the resources an attacker would need to expend in order to have a good shot at making the attack in question a success. The key to arriving quickly at reasonably accurate cost estimate is to pay special attention to the highest cost obstacles on the pathway with the lowest overall attack costs. This is because those "highest cost obstacles" will generally determine the greater portion of the attacker's costs. Knowing the likely cost of a given type of attack in time and skill is enormously useful.

Once the defender has an idea of what a given pathway and type of attack costs an attacker, the defender can then set about increasing those costs in an optimum way. The attack analysis we just described makes it possible to identify how and where the attacker's costs could be increased most easily. Increased "most easily," in this context, means increased at the lowest cost to the defender. This kind of analysis is the key to making cyber defenses as cost-effective as possible. Even if this sort of analysis isn't done very thoroughly or rigorously, it can be enormously illuminating. Often a part of the cyber defenses that wasn't receiving much attention will suddenly be revealed as the highest priority thing to improve.

The contribution of offensive tools, such as multi-function malware, can be analyzed using this matrix. A given offensive tool will contribute to an attack by overcoming specific obstacles that the attacker faces. If an offensive tool does a number of different things, it will be possible to locate all of the things that it does on the matrix. A piece of advanced malware, for example, will carry out actions that can all be located and defined using this matrix. This makes it possible to compare and classify different offensive tools, even if these tools are very complex. It also makes it possible to quantify the contribution of an offensive tool by assessing the degree to which it lowers attacker costs.

The contribution of defensive tools and services can also be analyzed using this matrix. A given defensive tool or service will put more obstacles in the attacker's way or make the existing obstacles harder to overcome. These obstacles can all be located in the same matrix. The same defensive tool, for example, might make it harder for the attacker to penetrate a given network via its internet-facing servers and also harder to conceal this sort of penetration, should one take place. The defensive benefit of any defensive tool of service will be proportionate to the amount it increases attacker costs. Notice that the obstacles in question are not necessarily obstacles to penetration. They can be obstacles to any of the five basic things the attacker needs to accomplish.

Who wins and who loses this game is determined entirely by the costs and benefits. If the costs for the attacker become greater than the gains for the attacker, then the defender has won absolutely. There will be no reason for the attacker to carry out that sort of attack. It might take the attacker a game or two to learn this lesson, but very soon that sort of attack will cease. If the rate of payoff becomes lower for that target than for some alternative target, the defender has won relatively. In the future, the attacker will go after a different target where his return-on-investment is better. To tell how well a defender is doing in this ongoing game with attackers, it is essential to consider what is happening to attacker costs.

What a Cyber-Security Matrix or Check List Can *Not* Accomplish

This account of what the new US-CCU Cyber-Security Matrix can be used to accomplish would be somewhat misleading if it did not *also* contain an explanation of what this matrix can *not* accomplish. Despite illuminating many aspects of attacker activities, the defenses against them, and the resulting degrees of vulnerability, this defensive matrix, by itself, will tell you almost nothing about cyber threats, cyber consequences, cyber risk, or cyber risk reduction.

Being explicit about this seems especially important right now. This is because many tools that are essentially just defensive check lists or software implementations of such lists are currently being touted as providing threat metrics, risk metrics, or risk reduction metrics. Whenever the basis for these metrics is essentially a defensive check list, these metrics are completely bogus. The limitations of the US-CCU Cyber-Security Matrix, when it comes to assessing things like threats, risk, or risk reduction are the limitations of *all* defensive check lists.

A defensive check list can tell you nothing about *threats*. To assess cyber threats, it is necessary to have some idea of what attackers are out there, what benefits they could obtain from carrying out an attack, the scale of those benefits, what targets they would choose to maximize those benefits, the kinds of things they would like to do to those targets in order to obtain such benefits, what alternative attack

possibilities are available to them, what their current capabilities are, the costs of assembling any missing capabilities, and how all of these things are changing over time. A defensive check list cannot provide any of these answers.

A defensive check list can tell you nothing about *consequences*. To assess cyber consequences, it is necessary to know, at least approximately, how much value the operations supported by information systems are creating and how much liability these operations could be used to create. It is necessary to know how these operations would be disrupted by an attack, what activities would substitute for the ones that were disrupted, the knock-on effects, and how long all these effects would last at a business level. Then it is necessary to determine how much value would be created under the conditions that would arise after the attack, so that this amount can be compared with the value that would have been created without the attack. Once again, a defensive check list can provide none of these answers.

Because defensive check list can tell you nothing about threats or consequences, it can tell you almost nothing about *risk*. To assess cyber risk, it is necessary to know approximately how likely or how soon a given attack will occur (the Threat), what losses could be caused by that attack (the Consequence), and the degree to which the attack would cause those losses with a given set of defensive measures in place (the Vulnerability). The risk equation for cyber security is: Threat x Consequence x Vulnerability = Risk. If a defensive check list is used properly, it can tell you most of what you need to know about the last of the three risk factors (the Vulnerability). But it can't tell you anything about the other two.

There is no easy way to convert vulnerability estimates into risk estimates by assigning some standard threat level or consequence level to a vulnerability. Knowing how vulnerable a given information system is doesn't tell you whether anyone would want to attack it. Even knowing what kind of information system it is tells you almost nothing about the degree to which it will be a target. The same kind of information system will be a huge target in one company, but hardly a target at all in another company. Knowing how vulnerable an information system is and what kind it is tells you even less about the possible consequences of an attack on that system. An attack on the same kind of information system with the same vulnerabilities will have almost no effect on one business, whereas it might send another into bankruptcy.

Risk is defined as the likely loss, under a given set of conditions. This means risk can always be expressed as the amount an individual or organization can expect to lose over a period of time. This means that risk can normally be expressed as an "Annualized Expected Loss." A reduction in risk would be a reduction in the annualized expected loss. A defensive check list provides no way of estimating the amount of loss that a given cyber attack would cause. It also provides no way of estimating the amount by which that loss would be reduced if the conditions were

changed. Hence, a defensive check list can tell you almost nothing about either risk *or* risk reduction.

It is important to emphasize that winning the game of cyber security in the context of the cyber-security matrix is very different than reducing risk. In fact, if you've won the cyber-security game against some group of attackers, you don't actually know if you've reduced your organization's risk by doing so. This is because, if your field of view only encompasses the game, you can't tell what is at stake in the game. You can't tell whether any serious attacker wants to play the game. You can't tell how much of an increase in attacker costs will cause the attacker to abandon the game. You can't tell whether the game is one your organization can't afford to lose, or whether it's a game that doesn't actually matter much.

This cyber-security matrix is an indispensable tool in estimating cyber risk. But, at most, it can only supply one of the three factors that are necessary to make a credible cyber risk estimate.

The Practical Basis for This Cyber-Security Matrix

The cyber-security measures included in this matrix are based almost entirely on the real-world experiences of the authors, their colleagues, and the other cyber-security professionals with whom they regularly trade information and advice. The measures that are recommended here take account of all the vulnerabilities and solutions that the US-CCU teams have discovered in the course of their field studies. If an item included in this matrix occasionally seems a bit quirky, this is generally because a real-life case demonstrated its importance. For more than fifteen years, the authors have made a point of investigating any cyber attacks they have heard about that seemed innovative or in any way groundbreaking. In many cases, they were brought in to advise on these attacks while the attacks were underway. In some cases, they did the original monitoring or the pioneering analysis. As a result, the authors have had a first-hand acquaintance with nearly the whole range of attacks that have been carried out up to now. They have paid special attention to the way attack patterns change over time. All these experiences and research opportunities have contributed to this matrix.

No previous check lists were used as the basis for this matrix, except for the previous "US-CCU Cyber-Security Check List." That earlier US-CCU list was itself based almost entirely on the real world experiences of the same authors. Released in a draft version in 2006 and a final version in 2007, that earlier list has remained in constant use up to the present. This is partly because it was already future-oriented and included a much wider range of security measures than previous check lists. In particular, it already featured a number of security measures that were not

focused on preventing penetration, but were aimed at foiling attackers in other ways.

That previous 2007 check list was rapidly adopted across much of the world. It was translated into several languages, including some official translations posted by the US-CCU. It was recommended or referenced as a best practice document by the American National Standards Institute (ANSI), the Fondazione per la Ricerca sulla Migrazione e Integrazione della Tecnologie (FORMIT) in Italy, the Government Accountability Office (GAO) in the U.S., the International Telecommunication Union (ITU), the Internet Security Alliance (ISA), the Nationaal Adviescentrum Vitale Infrastructuut (NAVI) in the Netherlands, the National Infrastructure Advisory Council (NIAC) in the U.S., the Telecommunications Industry Association (TIA), the U.S. Computer Emergency Readiness Team (US-CERT), several of the world's largest information technology companies, and many other organizations. It was required reading in many cyber-security courses. It was eventually downloaded over 100,000 times and used in over eighty countries. Altogether, it is perhaps the most widely used cyber-security check list that is *not* an official standard. This current cyber-security matrix attempts to retain most of the virtues of that previous check list, while striving to be even more innovative and forward looking.

One of the advantages of both the current matrix and the previous US-CCU check list is that they were written by only two authors, rather than a series of committees. This made it possible to achieve an unusual consistency in approach across all parts of these documents. It allowed bolder formulations and clearer wordings to be employed wherever this seemed appropriate, rather than more cautious formulations and vaguer wordings. As with the earlier US-CCU check list, the authors went to great lengths to eliminate jargon and acronyms throughout. If a technical term for something was unavoidable, the rest of wording should still usually make the meaning clear. Most of the items were revised repeatedly in an effort to say everything as plainly as possible. The goal is to make all of the contents readily accessible to people from other professions, especially other engineering professions, to non-professional readers, and to people whose first language is not English. The final wordings should be relatively easy to translate into other languages, because they use words that already exist in more languages. Because many technical terms in cyber security do not yet have settled meanings, the ordinary words used here are actually less ambiguous than much of the field's technical jargon. The authors hope that "non-technical" business executives will be able to dip into this document to get a better idea of what cyber-security professionals actually do and what needs to be covered in their budgets. None of this would have been possible if the document had been produced by a series of technical committees.

Although this new cyber-security matrix was entirely written by only two authors, it has made use of comments and suggestions by a large number of cyber-security professionals. A few of these cyber-security experts deserve special thanks, because they had a considerable influence on this work or offered many suggestions that led to its improvement: Warren Axelrod, Brian Collins, Dave Cullinane, Mark Fabro, Dan Geer, Jim Gosler, Brian Honan, Mich Kabay, Tom Kellermann, Chris Michael, Mike Peters, Gideon Rasmussen, Bridget Rogers, Sami Saydjari, Winn Schwartau, Gene Spafford, and Amit Yoran. Other cyber-security experts whose suggestions resulted in specific changes, corrections, or additions include: Billie Black, Dawn Cappelli, Paolo De Francesco, Dennis Groves, John D. Johnson. [OTHER NAMES TO BE ADDED]

Without the generous help of these brilliant experts, this cyber-security matrix would not be at all as complete, as up-to-date, or as practically useful.

When work on this cyber-security matrix was still in its early stages, eBay provided some funding for it that was enormously helpful. The corporations that have helped with funding more recently include: [NAMES TO BE ADDED] Their company logos will be found on the cover of the final printed version.

Hundreds of individuals and organizations helped in smaller ways with the research that went into this matrix. They provided tips, insights, concrete examples, specialty knowledge, and inside access. No work of this kind could get very far without the help and support of a significant segment of the information technology, cyber-security, and hacker communities. The authors are very grateful for this help and support.

Finally, this cyber-security matrix should be taken, above all, as an invitation to participate in a new wave of cyber-security discussion and innovation. There are many under-utilized security possibilities identified here. Some of the less familiar measures included in this matrix should also suggest additional measures. The sections of this matrix that remain more thinly populated should be seen as opportunities for further innovation. Developing these possibilities will need ideas and insights from a larger portion of the cyber-security community.

I. ORGANIZED BY ATTACKER ACTIVITIES

Providing an Overview

AREA ONE: HARDWARE

Distributed Electronic Equipment

□ Does the organization maintain an accurate inventory of the electronic equipment housed in each room at each physical location?

□ Does the inventory of electronic equipment include all the memory devices allowed inside the organization's facilities, such as external hard drives, CD's, magnetic tapes, flash drives, zip disks, and other removable media?

□ Are employees required to leave all personal electronic devices with memories outside the organization's facilities, except those explicitly allowed by the organization?

□ Is there a quick and easy procedure for updating the electronic equipment inventory, whenever an employee with responsibility for a piece of equipment authorizes it to be moved?

□ Is the inventory of electronic equipment for each facility unit actually updated whenever a piece of new equipment is added or removed for disposal or recycling?

□ Are the electronic equipment inventories and records included in the organization's annual audits?

Operations Centers and Data Centers

□ Are important operational centers where the activities consist almost entirely of monitoring screens and working at terminals organized into separate physical units?

□ Are especially important pieces of electronic equipment consolidated into data centers for easier protection?

□ Is there an inventory and schematic plan of the data center equipment that is immediately updated each time a change is made in the equipment or in the way it is connected?

Environmental Systems

□ Is there a readily accessible document that lists the locations and types of all local environmental control devices, such as thermostats and water leak detection systems?

□ Is there a readily accessible document that lists the locations and types of any supervisory environmental control devices?

□ Is there an up-to-date document listing the temperature ranges and other environmental requirements for the organization's various types of electronic equipment to operate without damage?

Cables and Wiring Closets

□ Is there a floor plan or geographical map that shows exactly where the communication cables have been laid?

□ Is there a floor plan or geographical map that shows exactly where the electric power cables have been laid?

□ Are the layout and capacities of the electric power supply well-documented?

□ Are all documents diagramming communication cable routes rigorously protected from unauthorized access?

□ Have all communication cables and equipment been physically labeled and color coded inside the wiring closets and at other locations where they might need to be reconfigured?

□ Are there labels for equipment on both the front and rear of the equipment housings, to reduce the risk of equipment being improperly reconfigured or turned-off?

□ Does the organization investigate the physical security practices of internet service providers and other communication companies before choosing which companies to buy services from?

□ Are the projected electric power needs of the electronic equipment well-documented, with reliable estimates of peak needs as well as normal needs?

Physical By-Products (Used Equipment & Paper Printouts)

Electronic Equipment

□ Has the organization defined the procedures for the thorough wiping or secure destruction of each type of memory device?

□ Is there a list of the memory devices scheduled for destruction or recycling that shows the exact location of these items at each point in their processing?

□ Is a rigorous chain of custody maintained for memory devices being processed, transported, or sent for disposal?

□ Is the list of memory devices scheduled for destruction or recycling updated each time any of these devices are moved to a new location, wiped, or put through another process?

□ When the memory devices are removed from the room or area where they were in regular use, is the inventory of the electronic equipment in that room immediately updated?

□ Does the organization supply employees with locked collection boxes for the secure disposal of used cell phones and other electronic devices with memories?

□ Are the electronic devices collected for disposal from the deposit boxes properly inventoried and inserted into the regular process for wiping and secure destruction?

Paper Printouts

□ If a document is highly sensitive, is a record kept of each time it is printed or copied, how many copies are made, and by whom?

□ If a document is highly sensitive, is each copy labeled with a unique number?

□ If a document is highly sensitive, is a chain-of-custody record maintained, so that each person who takes possession of a copy must sign for it, and so that the date and time of the transfer is recorded?

□ If a document is highly sensitive, is the chain-of-custody maintained until the document is destroyed or its period of sensitivity expires?

AREA TWO: SOFTWARE

Applications and Operating Systems

□ Does the organization maintain an up-to-date inventory of all the software applications that are installed in its systems?

□ Does the organization have a policy of limiting each employee's use of software applications to those that the employee actually needs to carry out his or her work?

□ Has the organization formally assigned criticality classifications to its more important or more widely used software applications? (E.g., is a software application that controls a specialized process that is highly dangerous easy to distinguish from one that controls a commonplace process that cannot easily be used to do harm?)

□ Is there a procedure for documenting and tracking which application privileges are active for each individual employee?

□ Does the organization maintain a comprehensive list of all the applications that require an administrative level account to perform operations?

□ Does the organization maintain a comprehensive list of all scripts that use embedded credentials to perform operations?

□ Is there a system for tracking software patches and updates that logs the news that those patches or updates are needed, the announced release dates for those patches

or updates, the dates on which those patches or updates are actually received, and the dates on which they are applied?

Documents and Data

□ Is information generally disseminated throughout the organization on a need-to-know basis?

□ Do these need-to-know restrictions take account of the need for cross-disciplinary information sharing and the importance of employees' understanding the reasons for what they are doing?

□ Has the organization formally assigned sensitivity classifications to its information files?

□ Are the sensitivity classifications that the organization employs designed to provide a good basis for encryption policies?

□ Are the sensitivity classifications that the organization employs periodically reviewed to make sure that they are not excessively restrictive, encumbering corporate activities with necessary precautions, or insufficiently restrictive, exposing corporate activities to losses and harm?

□ Does the organization avoid storing types of data that could create liabilities, but do not serve any important business or government function? (E.g., does the organization erase credit card numbers as soon as the transactions using those numbers have been successfully processed, if the customers are going to be asked to enter these numbers again when making future purchases?)

□ Is access to genuinely sensitive data restricted to those users within the organization who actually need to use that data?

Identity Authentication Systems

□ Do corporate security policies outline the activation of passwords and other authentication credentials when an employee is hired?

□ Do corporate security policies outline the activation of passwords and other authentication credentials used for root-level or administrator-level operations?

□ Do corporate security policies mandate the immediate deactivation of passwords and other authentication credentials when an employee is terminated, leaves, or retires?

AREA THREE: NETWORKS

Permanent Network Connections

□ Has the organization considered establishing separate networks for activities that have very different security requirements, such as normal business activities,

production operations, environmental systems, corporate guests, and critically important research, design, and planning?

□ Does the organization maintain a list of all the devices on the corporate network, along with the manufacturer identification (MAC) numbers for those devices?

□ Does the organization maintain a comprehensive list of all the protocols and port numbers used by applications installed on the organization's computers?

□ Does the organization maintain a comprehensive list of all the system names and their associated network addresses on the organization's network?

□ Do detailed network topology diagrams exist of the corporate network, so that all the connection routes can be traced?

□ Do the detailed network topology diagrams list the service paths and network protocols being used?

□ Has the information on the network topology diagram been verified to be accurate, so that all the components and connections on the network are indeed included?

□ Are all documents diagramming network topologies rigorously protected from unauthorized access?

□ Does the organization maintain comprehensive access control lists for its routers, including the internet protocol addresses and port numbers being utilized?

□ Does the organization require that the access control lists for its routers be periodically reviewed, so that they take account of changes in the organization's traffic needs?

□ Does the organization require a second authorized employee to verify that the specific changes in access control lists are appropriate before these changes are implemented?

Cloud Provider Connections

□ Are the people in the organization who are responsible for cloud computing policies made aware that the use of an external cloud provider will require additional security measures?

□ Are the people in the organization who are responsible for cloud computing policies made aware that any *unencrypted* information stored with a cloud provider could potentially be obtained by a subpoena before the organization could take legal steps to prevent this?

□ Are the people in the organization who are responsible for cloud computing policies made aware that the extra encryption needed to secure information in the cloud could result in longer response times for information systems?

□ Are the people in the organization who are responsible for cloud computing policies aware that any plan for moving activities into the cloud needs to be accompanied by a plan for moving activities out of the cloud, in the event that changes in computing costs, computing methods, or computing security make this advisable?

□ Is the provider of cloud computing services contractually required to carry out a thorough wiping of any media used to store the organization's proprietary applications and data when the contract for handling that software ends?

□ Has the organization identified which kinds of documents and data can be handled using third-party collaborative platforms, such as Google Docs or Dropbox, depending on the sensitivity classification of those documents and data?

Intermittent Network Connections

□ Are employees on the road issued standardized laptops or standardized mobile devices that meet corporate security requirements?

□ If the organization is supplying laptops or mobile devices to its employees, does the organization withhold administrator privileges from those employees, so that it can limit the applications installed on those laptops or devices?

Public and E-Commerce Connections

□ Are web portals for e-commerce constructed by specialists in website and e-commerce security?

□ Are web portals for e-commerce checked more frequently for security issues than other corporate information systems?

□ Does the organization register its domains using a well-established domain registrar?

Encryption Systems and Digital Certificates

Encryption Systems

□ Do corporate policies define what type of data communications should be encrypted and which encryption technologies should be employed?

□ Is encryption explicitly required for the storage and transmission of all information above a designated sensitivity level?

□ Are the people in the organization who are responsible for encryption policies made aware that the organization's own encryption mechanisms could potentially be used by cyber attackers to make the encrypted information permanently inaccessible?

□ Does the organization have multiple encryption options available, such as individual document encryption, encryption containers, and full disk encryption, so that the scale of encryption can be adjusted to the quantity of information on a given computer that needs to be encrypted?

□ If the organization will need to encrypt transmissions of data between distributed, local devices with limited resources for computing and memory, do the

organization's encryption options include one that can be applied with those limited resources?

□ If the organization is handling extremely critical information, is there a separate encryption policy for the handling of that information?

□ If the organization is handling extremely critical information, does the organization have an appropriately advanced encryption tool available for encrypting that information?

□ If highly sensitive information is being handled using an advanced encryption tool, does that encryption tool require two-factor authentication for decryption?

Digital Certificates

□ Does the organization maintain a comprehensive list of the certificate of authorities and digital certificates used by their computer systems and applications?

□ Are digital certificates obtained only from well-established certificate issuers who investigate all the companies to which they issue certificates?

□ Are digital certificates used on any customer website to encrypt the connection and transactions with Secure Sockets Layer (SSL)?

□ Are digital certificates used for digitally signing applications under development?

□ Are digital certificates embedded in the firmware of hardware devices performing secure connections, which allow for trusted authentication between multiple systems?

□ Are digital certificates used for the organization's virtual private networks?

Firewalls, Intrusion Detection Systems, & Content Filters

□ Has the organization made lists of the traffic destinations and kinds of traffic, both inbound and outbound, that it wants to allow through its firewalls?

□ Does the organization require the lists of the traffic it allows through its firewalls to be periodically reviewed, so that they take account of changes in the organization's traffic needs?

AREA FOUR: AUTOMATION

Automated Operations and Processes

□ Is there an overall map that accurately identifies all the communication paths by which control systems are connected?

□ Does the map of control system connections identify all the places where the response time must be extremely short, so that no security measures are introduced that might cause dangerous response delays?

□ Have all computer controlled physical processes that could produce dangerous physical conditions been clearly identified?

□ Are software patches and updates for critical systems handled separately from patches and updates for other systems?

□ Are there additional verification and testing procedures for software patches that affect the safety or effectiveness of a critical device?

□ Is there a documented procedure which allows a system *not* to be patched or updated in cases where this might create a greater hazard than an unpatched system?

Peripheral Devices and Physical Equipment

□ Are the security features of distributed, local devices taken into consideration before those devices are purchased?

□ Does the organization collect information on the resources of distributed, local devices, in order to determine what kinds of encryption and other security measures would be possible with those devices, given their limited resources?

□ Is the ability of the purchaser to customize the security settings on distributed, local devices treated as a significant factor in decisions about whether to purchase these devices?

□ Are the procedures for the secure updating of firmware treated as a significant factor in decisions about whether to purchase distributed, local devices?

□ Is there a list of the peripheral devices, such as printers, scanners, that are shared between multiple employee computers, along with additional lists of the computers sharing them?

□ Is there a list of the local computers that provide coordination between multiple local devices?

□ Is there a list of the local device computers that can connect to the internet, along with an identification of the paths by which they can do this?

□ Are records kept of all modifications of the firmware and software in distributed, local devices?

□ Is there document that accurately identifies all the kinds of data that are being collected from the distributed, local devices that the organization owns or that are located in its facilities?

□ Is data collected from distributed, local devices only when there is a clear benefit from collecting that data?

□ Is there a limit on how long any data collected from distributed, local devices is retained, based on when the retention of that data would deliver no further benefits?

Information Backup Devices and Processes

□ Is there a comprehensive plan covering everything that needs to be backed up?

□ Are the operating systems, programs, and operating information backed up, as well as the data?

□ Is there a special automatic procedure for regularly backing up the contents of employee laptops and mobile devices?

□ Are the configurations of switches and routers backed up on a regular basis?

AREA FIVE: HUMAN USERS

Individual Employee Actions

Security Accountability

□ Is maintaining the security of the organization made part of each employee's job description?

□ Are all employees required to sign confidentiality and intellectual property agreements and told their practical implications?

□ Is each piece of information equipment the organization owns or leases the explicit responsibility of one designated employee?

□ Are there permanent tags or other identifying markings that make it easy for other employees to determine who "owns" a given piece of information equipment?

□ Is the employee who is responsible for a given piece of information equipment explicitly required to oversee the security of that equipment?

□ When employees are carrying or using their laptops or other portable information equipment outside the workplace, are they trained to keep those devices under watch or in secure places?

□ Do corporate policies define the proper use of e-mail, internet access, and instant messaging by employees?

□ Do corporate policies define the kinds of information about the corporation that can be posed on social media by employees and the kinds of information that should be treated as confidential or proprietary?

□ Are employees made strictly accountable for any actions they carry out on the corporate information system that are in violation of corporate security policies?

General Security Training

□ Are all employees given periodic training on the security policies that are important to the business with sufficient explanations of why these policies are important?

□ Are employees taught what sorts of information handled by the organization should be regarded as sensitive information?

□ Are employees taught how to create imaginary memory personae, so that they have a relatively easy way of remembering passwords and answers to challenge questions that cannot be discovered by researching them on the web?

□ Does the employees' training in security policies include practical exercises in which the employees act out some of the practical implications of these policies?

□ Are all employees periodically tested on their knowledge of security procedures, including their knowledge of newly emerging threats?

□ Are the employees' security behaviors regularly tested in practical ways that will not be easily recognized as tests?

□ When the employees' security behaviors are tested, are they given near-instantaneous feedback that will shape their future behavior? (E.g., does loud, comic music blare out from an employee's computer each time that employee clicks on a trojanized e-mail attachment that was sent as a test?)

Security Reporting

□ Are employees made aware that any time they install a new software application in a computer belonging to the organization, they must report this fact to the organization's cyber-security personnel?

□ Are employees given an easy way to report possible security vulnerabilities and rewarded for doing so?

□ Are employees given adequate incentives to report possible security breaches and bad security behavior, while simultaneously insulated from any blame or retribution for making such reports?

Administrative Actions

Senior Management

□ Are the organization's senior managers regularly briefed on the status of the organization's cyber security and the possible consequences of emerging cyber threats?

□ Are the organization's senior managers made aware that good cyber security needs to take account of what the organization's information systems are used to accomplish in business and operational terms?

□ Are the organization's senior managers made aware that the most cost-effective way to deal with many cyber-security issues is not to add more cyber-security measures, but to make small changes in the way operations are carried out?

□ Are the organization's senior managers made aware that dealing with cyber-security issues is usually much easier and much less expensive if these issues are taken into account when new business operations and new information systems are first being planned?

□ Does the organization have a designated Chief Information Security Officer?

□ Is the organization's Chief Information Security Officer periodically required to brief the organization's Chief Financial Officer or its Chief Executive Officer without the presence of anyone else to whom the Chief Information Security Officer might otherwise report?

□ Is the organization constantly using news about the attacks being carried out against other organizations to update its cyber-security plans and programs?

□ Does the organization provide a regular channel through which cyber-security personnel can provide advice and warnings about the cyber-security implications of corporate strategies, policies, practices, and public relations?

□ Are the organization's cyber-security personnel actively rewarded for bringing cyber-security considerations to the attention of managers and other personnel outside the cyber-security department, as long as this is done in an appropriate manner?

Audits and Outside Reviews

□ Are the organization's information security policies and their implementation reviewed annually by an expert outside auditor?

□ Are the organization's information security policies and their implementation carefully checked to verify that the organization is compliant with the regulations and recognized standards for that industry?

□ Is the annual review of the organization's information security policies and their implementation broad enough in scope to uncover information vulnerabilities in the physical facilities?

□ Is the annual review of the organization's information security policies and their implementation broad enough in scope to uncover information vulnerabilities in employee behavior?

□ Are the audits and reviews of the organization's information security examined analytically to identify areas where different or additional counter-measures may be needed?

□ Are the successive audits and reviews of the organization's information security compared, so that senior managers can make sure that the organization's information security is improving, rather than deteriorating?

Security Administration

□ Is there a reliable system for keeping track of all the logs and other sources of information that the security team needs to review and for verifying that they are being dealt with on an appropriate schedule?

□ Is there a reliable, continuously updated system for listing and tracking all of the vulnerabilities noticed by employees, discovered by audits, reported by vendors, or covered in the media?

□ Does the system for tracking vulnerabilities allow security personnel to determine quickly which vulnerabilities are still in need of attention, which vulnerabilities are currently being dealt with, and which vulnerabilities have already been remedied?

□ Are vulnerabilities assigned a priority level, so that more critical vulnerabilities are dealt with more quickly?

□ Does the priority level assigned to vulnerabilities take into account the nature of the business or production operations that are supported by the information systems in which those vulnerabilities occur?

□ Is the system for tracking vulnerabilities co-ordinated with the system for tracking software patches and updates, so that effort is not wasted dealing with the same issues more than once?

□ If an important vulnerability is going to be dealt with by a software patch or update, but not for some time, are temporary measures to reduce the effect of that vulnerability put into place in the meantime?

□ Is there a single designated security manager who is continually checking to make sure that the vulnerabilities are being dealt with in a timely manner and in an order that takes account of their relative priority?

□ Does the Chief Information Security Officer review the security programs and procedures on a monthly basis to make sure that these are staying ahead of security needs, rather than falling behind?

□ Does the work schedule of the security team set aside a significant amount of time for putting new security measures in place and renovating old ones, rather than allowing all the team's time to be taken up with patching vulnerabilities and responding to attacks?

Security Incident Handling

□ Does the organization have detailed plans for dealing with security incidents, both while they are underway and immediately after?

□ Do the organization's detailed plans for dealing with security incidents specify the points at which senior managers outside the cyber-security team should be notified?

□ Do employees know where they should turn for operational guidance during a continuing series of cyber attacks?

□ Are exercises periodically conducted in which key employees go through the motions of responding to a cyber attack in a reasonably realistic manner?

□ Have the key personnel been given opportunities to practice their emergency responses in actual simulations?

□ Are both real incidents and exercises followed by after-action discussions directed at identifying the lessons learned?

□ Is the organization constantly using news about the attacks being carried out against other organizations to update its response plans for the attacks it might suffer?

AREA SIX: SUPPLIERS

Procedures for Developing New Software

□ Does the organization have a written policy detailing the steps and procedures for the internal development of software?

□ Does the organization require in-house software developers to have periodic training in secure coding techniques?

□ Does the organization have clear policies regarding the use of open-source software libraries and third-party components in the software it develops?

□ Does the organization maintain an inventory of all open-source or third-party software components it has incorporated into the software it has developed, along with the details of exactly where and how those components were used?

□ Does the organization periodically check whether upgrades or patches are needed to correct bugs or security flaws in the open-source and third-party software components it has incorporated into its software?

□ Does the organization have a system for tracking the upgrades and patches that might be needed for the software it has developed in house, logging all reports of software issues that might need attention, the decisions about the actions to be taken, the dates by which any necessary patches or upgrades were completed, and the dates and methods by which these patches or upgrades were distributed?

Features to Build into New Software

□ Are proposed software designs, including plans for the modification or extension of existing software, evaluated from the standpoint of information security by experienced security specialists before the initial versions of that software are created?

□ Are the potential security issues in the software designs evaluated in relation to the software's ease of use and its business functions?

□ Is consideration explicitly given to the possibilities for incorporating security features into the software itself, rather than leaving the relevant security measures to be dealt with after the software is ready to install?

□ Are the software designs approved by the cyber-security team, as well as the software developers and the business managers, before the new software program is actually written?

External Vendors

□ Does the organization have a written policy detailing the steps and procedures for interacting with software vendors and outside developers?

□ Are all outside vendors or contract personnel contractually required to adhere to the security policies at least as stringent as those maintained by the client organization?

□ Are all outside vendors or contract personnel required to have briefings or training in the security policies of the client organization?

□ Do corporate policies require vendor personnel to sign non-disclosure agreements?

Making Targets Harder to Find

AREA ONE: HARDWARE

Distributed Electronic Equipment

□ Are the locations of areas handling sensitive information processes left off of building directories?

□ Are the locations of areas handling sensitive information processes omitted from public tours and are the employees providing those tours warned not to mention them or answer questions about them?

□ Are employees explicitly prohibited from publicly posting photos of all activities in areas handling sensitive information processes?

Operations Centers and Data Centers

□ If an operations center carries out highly critical activities and does not need to have many visitors, apart from those who work there, is the operations center left off of building directories?

□ Is the location of the data center left off of building directories?

□ Is the data center omitted from public tours and are the employees providing the tours warned not to mention it or answer questions about it?

□ Are those overseeing the organization's public facing website instructed to make sure that no mentions of the data center or operations centers are posted online?

□ Are employees explicitly prohibited from posting pictures of all activities in the operations centers and data center?

□ Are the doors to the data center marked in a way that does not reveal that they lead to the data center?

Environmental Systems

□ Are any outside contractors who support or manage the organization's environmental systems contractually prevented from advertising or publicizing the fact that the organization is a customer?

□ Are the environmental controls, other than local thermostats, for the areas with electronic equipment located behind panels or doors and not easy to identify?

□ Are the exterior air conditioner or cooling fans for facilities housing critical electronic equipment hidden from view and away from public areas?

Cables and Wiring Closets

□ Are the most critical communication cables installed in such a way that their locations and routes are not obvious?

□ Are labels on electronic equipment worded in such a way that their meaning is not immediately obvious to an outsider?

□ Are the connecting power cables that are farther away from the data center installed in such a way that they are not easy for unauthorized personnel to identify and access?

Physical By-Products (Used Equipment & Paper Printouts)

□ Do the labels on equipment being sent for thorough wiping or secure destruction avoid revealing what departments they are from?

AREA TWO: SOFTWARE

Applications and Operating Systems

□ Does the organization take steps to prevent the public release of information about which software applications it is running, whenever these applications are unusual or associated with special processes?

□ Are employees and former employees contractually obligated to keep information on their cv's about what software applications they have mastered generic, rather than listing the specific applications?

□ Are administrator accounts renamed, so that it is not easy to identify them as administrator accounts?

□ Are service accounts (e.g., backupserver, sp_content) renamed, so that it is not easy to identify them as special accounts linked to specific applications?

Documents and Data

□ Are critical files labeled in a way that does not reveal their contents?

□ Are the table and column labels in databases named in a way that does not reveal which ones contain sensitive information?

□ Are bogus files mixed in with the real ones, so that it would be difficult for an attacker to know which are the real ones?

Identity Authentication Systems

□ Are employees' log-in names different from their given names and e-mail addresses?

□ Are employees assigned log-in names that cannot be easily deduced?

□ If a database of challenge questions is being set up, is care taken to avoid any questions about employee's lives that could be readily answered by web research?

□ If a database of challenge questions is being set up, are employees given an opportunity to add their own questions, so that the answers would be too private to discover by web research?

□ If a database of challenge questions is being set up, are a large number of questions and answers created for each employee, so that it would difficult to collect enough information on the employee to be able to answer several randomly chosen questions?

AREA THREE: NETWORKS

Permanent Network Connections

□ Are the pieces of equipment connected to the corporate network assigned addresses that do not conform to any uniform system and are difficult to deduce?

□ If wireless technology is used for a sensitive network, is the beacon that would broadcast the network's presence disabled?

□ When there are categories of communication that only involve the organization's own computers, are unconventional (non-standard) port numbers being utilized?

□ If the organization is maintaining a separate network for security reasons, are all unnecessary services and broadcasts disabled on the gateway between networks, including responses to ping requests and traceroute requests, so that the existence of the gateway is difficult to detect?

□ If a network is used for highly critical functions, does the organization periodically change the port numbers used by those critical services, so that any previous unauthorized explorations by potential attackers of those port numbers and their uses will be made obsolete?

□ If a network is used for highly critical functions, does the organization periodically change the names of servers and other devices, so that any previous unauthorized explorations by potential attackers of those names and what they designate will be made obsolete?

□ If a network is used for highly critical functions, does the organization periodically change the network addresses of servers and other devices, so that any previous unauthorized explorations by potential attackers of those network addresses and their locations will be made obsolete?

Cloud Provider Connections

□ Are the subdomain names that the organization uses for external cloud computing services named in a way that will prevent someone determining the cloud provider from those names?

□ Do the uniform resource locators (URL's) used to access external cloud services mask the identity of the cloud provider?

Intermittent Network Connections

□ Does the organization arrange for its domain registrar to keep its identify and contact information confidential for any domains that are intended only for the organization's own private use?

□ Do any public-facing websites that are intended only for the organization's own private use omit any mention of the organization's identity and avoid including any information that could be used to deduce that identity?

□ If the organization is maintaining public-facing websites intended only for the organization's own private use, do these websites use internet protocol (IP) addresses that are not easily identifiable as belonging to the organization?

□ If the organization uses any dial-up modems for remote management or secure connections, do these have phone numbers that are unlisted and difficult to deduce?

Public and E-Commerce Connections

□ Has the organization disabled or modified the banners or strings that announce the name and version of the software products being used on public-facing web servers?

□ Are any names or logos that would identify the specific types of software incorporated into a website removed from the publicly accessible images and metadata?

□ Has the organization removed all software testing pages and scripts on public-facing web servers?

Encryption Systems and Digital Certificates

□ Are the encrypted repositories that contain encryption keys made to look like something else?

Firewalls, Intrusion Detection Systems, & Content Filters

□ If the organization is utilizing unconventional port numbers for communications involving its own computers, are its firewalls configured to block communications that appear to come from its own computers, but utilize the conventional port numbers?

□ Is network address translation (NAT) employed to conceal internal internet protocol (IP) address information?

AREA FOUR: AUTOMATION

Automated Operations and Processes

□ Are all documents that provide maps of the logical access routes to control systems rigorously protected from unauthorized access?

□ Are vendors of control system programs and components contractually prevented from revealing publicly or to third parties what kinds of programs and components they have supplied?

□ Has care been taken to make sure that intruders are not presented with clearly labeled schematic diagrams of the individual physical processes and the systems for managing them?

□ Have the addresses and labels for control system components, such as remotely operated switches and valves, been assigned in such a way that their functions are not too easy to guess or deduce?

□ Have the command codes for control system components, such as remotely operated switches and valves, been customized, wherever this can be done without creating hazards, so that they do not follow the default industry formulas?

Peripheral Devices and Physical Equipment

□ If distributed, local devices need to be located in public places, are they installed behind walls, in fixtures, or behind panels, so that their exact physical position and layout is not apparent?

□ If a local device, such as a piece of medical treatment equipment, performs a critical process, does the network name for that device conceal its true function?

Information Backup Devices and Processes

□ If backup media containing sensitive information are being transported physically to another location, are the routes and means of transport kept secret?

□ Are the location and nature of the facility where backup media are stored kept secret?

AREA FIVE: HUMAN USERS

Individual Employee Actions

□ Are employees contractually forbidden from posting information on the internet that would reveal which critical information systems they are able to access?

□ Are employees contractually forbidden from posting information on the internet that would reveal what security measures the organization has put in place?

□ Are employees made aware of the security risks they can incur by storing personal information, especially personal identification information, on their smart phones?

□ Are employees taught a variety of polite ways to say "no" to requests for information relevant to security, even when that information seems relatively innocuous?

Administrative Actions

□ Is the organization's publicity and public relations department made aware that its activities could have a significant impact on the organization's cyber security?

□ Does the organization refrain from publishing advertising and publicity materials that would draw attention to the organization's exact role in critical supply chains, unless there is a compelling business reason to do so?

□ Does the organization refrain from publishing advertising and publicity materials that would reveal the extent of the organization's dependence on key information systems?

□ Does the organization avoid making public statements that would be regarded as provocations by the hacker community, drawing attention to the organization as a possible target?

□ If the organization is an extremely high profile target, do advertisements and notices used for recruiting cyber-security personnel avoid revealing the organization's identity?

Security Incident Handling

□ Are the organization's detailed plans for dealing with security incidents kept highly confidential?

□ Are the after-action reports on the organization's security exercises and simulations kept highly confidential?

AREA SIX: SUPPLIERS

Procedures for Developing New Software

□ Do advertisements for recruiting software developers and programmers avoid revealing the specific nature of the software being developed?

□ If software developers are using websites where developers trade help, do they refrain from revealing their true identify, the organization they are working for, and the intended use of the program they are working on?

□ If developers post pieces of code on websites where developers trade help, do they take care to make sure that the piece of code being posted does not contain any labels or annotations that would reveal the organization it belongs to or its intended operational functions?

□ If developers let other users of websites where developers trade help critique their work or offer suggestions for solving problems they have encountered, are the

pieces of program being presented for discussion sufficiently short that shaping their functions will not shape the functions of the larger program being developed?

Features to Build into New Software

□ If the application under development is designed to carry out critical operations, are the functions of the individual program components masked or obfuscated, wherever possible?

□ Are the banners or strings that announce the name and version of the software application designed to be altered or removed when the application is put in service?

□ Is the application under development designed not to expose any unencrypted user or account ID's in the uniform resource locator (URL)?

External Vendors

□ Does the organization contractually require its vendors to abstain from advertising or publishing the fact that the organization is a customer?

□ Does the organization contractually require its vendors to abstain from revealing, even in private settings, exactly which products and services those vendors are supplying?

□ Does the organization periodically verify that its vendors are not advertising or publishing the fact that the organization is a customer?

Making Targets Harder to Penetrate

AREA ONE: HARDWARE

Distributed Electronic Equipment

Identification Badges

□ Are all employees required to wear personal photo ID badges, issued by the organization?

□ Are all visitors or vendors required to wear temporary photo ID badges, issued by the organization?

□ Are the photo ID badges designed to facilitate introductions and communication between personnel, rather than just used for security?

□ If the photo ID badges can be worn on cords, are they printed the same way on both sides, so that it won't matter which way a badge is facing?

□ Are the lettering and photo on the photo ID badge printed large enough and clearly enough so that they can be easily checked without being inspected up close?

□ Are the temporary photo ID badges color coded by date, so that it will be immediately apparent if a visitor or vendor is wearing a badge that has expired?

Physical Access Privileges

□ Are there strict controls on who goes in and out of the larger physical facilities in which the information systems operate?

□ Are there further controls preventing employees from entering the rooms and areas handling highly sensitive information, unless those employees have a need to be in those specific areas?

□ Is the time and exact place at which anyone enters or exits a physical facility automatically logged?

□ Is there a physical access list that a person's name must be on before he or she is admitted to a physical facility?

□ Does the access list for a physical facility also list the person who authorized each name on that list?

□ If the facility is a highly sensitive one, is the employee who authorized a name to be added to the physical access list asked to personally verify that authorization before the person is actually admitted?

□ Does every name on the physical access list have an expiry date on which the physical access privilege would need to be renewed?

□ Is there an access authorizer list, consisting of those who have the authority to add names to the physical access list?

□ When someone attempts to add a name to a physical access list, is the access authorizer list automatically checked to verify that the person adding the name is authorized to do so?

□ Does adding a name to the access authorizer list require at least two people whose names are already on this list?

□ Are both the access authorizer list and the physical access list regularly reviewed to see whether there are names that can be removed from these lists?

□ Are the physical access privileges for each employee changed when an employee's work role changes?

□ Are physical access privileges and devices such as badges immediately deactivated when an employee is terminated, leaves, or retires?

□ Are physical access privileges and devices for vendors frequently reviewed and promptly deactivated when there are changes in the status of vendor personnel?

Physical Equipment Features

□ Are there physical barriers, such as secure covers or plugs, put in place to disable any networked computers' unused media access ports, such as USB sockets and CD drives?

□ Are the connections where cables are plugged into networked computers secured with tamper-proof seals, so that it will be immediately apparent if a cable was unplugged without authorization?

□ Are unused access ports on network switches, especially the Switched Port Analyzer (SPAN) ports, turned off to prevent unauthorized access?

□ Are unused network access ports in the organization's facilities turned off in the network switches to prevent unauthorized access?

□ Is root level access disabled on routers and switches, so that attempts to gain unauthorized access during a reboot are prevented?

□ Is all physical access to the console interfaces of security appliances, such as those used to manage firewalls, intrusion prevention, and intrusion detection systems restricted to authorized users?

□ Are fax machines that receive and print sensitive information protected against unauthorized physical access?

Operations Centers and Data Centers

□ Are there walls or other physical barriers separating the operations center from other physical areas**?**

□ Does access to the operations center require a scannable badge, smart card, proximity card, biometric reading, or a lock requiring a personal combination?

□ Is the level of authentication required to enter the operations center adjusted to the criticality of the activities carried out there?

□ Are there physical security barriers established to protect electronic equipment in the data center from theft, malicious damage, or direct electronic access?

□ Are the walls of the data center painted with radio-wave scattering paint?

□ Are any drop ceilings or raised floors in the data center and other areas that house critical information equipment secured against access from adjacent spaces and ventilation systems?

□ Are the doors of the data center kept securely locked at all times for inbound traffic?

□ Are "restricted area" signs posted just inside the doors into the data center where anyone entering would see them?

□ Is access to the data center strictly controlled using technologies such as scannable badges, smart cards, proximity cards, biometrics, or locks requiring personal combinations?

□ Is the identify of the person entering the data center confirmed by means of a second factor, such as a password, personal identification number, or a second biometric feature?

□ Are there clear and rigorously enforced restrictions on which employees have access to the data center?

□ Are there strict controls on vendor access to the data center, so that only properly authorized vendor personnel are admitted?

□ Does the data center have a sign-in procedure that is used to log non-employees into the restricted area?

□ Are building maintenance personnel, such as janitors, prevented from entering the data center unless directly supervised by trusted personnel?

□ Are systems in place to allow very rapid access to the data center in the event of a fire?

□ If the data center needs to be quickly accessed in the event of a fire, is there a plan in place for immediately resecuring the data center's electronic equipment, as soon as it is safe to do so?

□ Are systems in place to allow access to the data center in cases, such as flooding or controlled facility evacuation, when equipment might need to be moved on short notice?

Environmental Systems

□ Are the panels or doors protecting the controls for the electronic equipment's physical environment kept locked?

□ Is there a secure delivery and loading area, physically separated from the data center, so that the addition or replacement of equipment doesn't provide an avenue for improper access or explosive devices?

□ Are pieces of electronic equipment and other supplies physically inspected before being moved into the data center, in order to make sure that they haven't been tampered with?

□ Is critical computer or communication equipment that could be a target for terrorists kept away from ordinary windows, which could provide a channel for thrown or projectile bombs, gunfire, or microwave weaponry?

□ Are the critical computer and communication facilities that could be a target for terrorists located a sufficient distance from public parking places, streets, and other locations where a bomb could be easily detonated?

□ If the electronic systems are sufficiently critical and represent sufficiently high-profile targets, are they surrounded by the sort of metal shielding that would protect against electro-magnetic pulse attacks?

□ Are the critical computer and communication facilities a sufficient distance from any permanent facilities that would be particularly susceptible to fire, explosions, or hazardous leakages?

Cables and Wiring Closets

Wiring Closets

□ Are wiring closets securely locked at all times?

□ Is there a list of which employees and contractors are allowed physical access to the wiring closets?

□ Is the list of employees and contractors who are allowed access to the wiring closets regularly updated to take account of what work needs to be done and who is assigned to do it?

□ Are the employees and contractors who are allowed to access the wiring closets required to sign out the relevant keys, tokens, or access codes each time they will need to use this physical access?

□ Are the times at which the keys, tokens, or access codes for the wiring closets are signed out, used, and signed in securely logged, along with the identities of those using them?

□ Are the keys, tokens, or access codes for the wiring closets changed on a schedule appropriate to the sensitivity and criticality of the equipment and cables in those wiring closets?

Communication Cables

□ Are physical security barriers established to protect the communication cables running to and from the system, so that they cannot be easily severed or damaged?

□ Are the critical communication cables and cable harnesses inside the organization's facilities laid out in a way that makes it difficult to access them physically for the purpose of intercepting transmissions?

□ Is there physical protection at the demarc point where telephone and data cables enter the building?

Electric Power

□ Have physical security barriers been established to protect the connecting power cables in the vicinity of the data center, so that they cannot be easily severed or damaged?

□ Are electrical supply components, such as power panels and breaker boxes, protected from unauthorized access?

□ If uninterrupted power supplies (UPS's) are being utilized, are these protected from authorized remote access?

□ Are backup power sources protected with security devices, such as locks, alarms, and reasonably secure fences?

□ Are backup power sources for facilities that could be a target for terrorists a sufficient distance from public parking places, streets, and other locations where a bomb could be easily detonated?

□ Are backup power sources in locations that are not susceptible to flooding?

Physical By-Products (Used Equipment & Paper Printouts)

Electronic Equipment

□ Are there sufficiently rigorous policies and procedures governing the use of removable storage media, such as flash drives and CD's, so that all of these devices are kept under the organization's control?

□ Is equipment marked for recycling kept in secure locations, at least until it has been thoroughly wiped?

□ Are there sufficiently rigorous procedures for properly shipping any removable data storage devices that need to be moved to offsite locations?

Paper Printouts

□ Are there sufficiently rigorous procedures to restrict unauthorized access to paper printouts that contain sensitive information?

□ Do corporate security policies require secure storage containers to hold paper printouts that contain sensitive information and are destined for destruction?

AREA TWO: SOFTWARE

Applications and Operating Systems

□ Does the organization have information security specialists conduct rigorous vulnerability testing on applications before they are deployed?

□ Are the vendor's default security settings changed on software applications before those applications are put into operation?

□ Are the vendor's default passwords and default log-in names changed on software applications before those applications are put into operation?

□ Are passwords for service accounts (e.g., backupserver, sp_content) extremely complex in their character sets and length?

□ Are the boot sequences on the organization's computers set so that the computers cannot be booted from external media, such as USB drives or CD's?

□ Is each type and level of application privilege assigned an appropriate type and level of authentication mechanism? (E.g., do administrator privileges require a more secure log-in mechanism than ordinary privileges?)

□ Is there a documented procedure for removing and verifying the removal of application privileges when these are no longer needed?

□ Before a patch or update is actually deployed, does the security team verify that the patch or update was announced on the vendor's website or that a notification to expect it was received from the vendor?

Documents and Data

□ Are all input fields for data restricted to an appropriate minimum and maximum length? (E.g., a Social Security Number field should only allow nine numerals.)

□ Are all input fields for data restricted to the appropriate characters and expressions? (E.g., a Social Security Number field should not allow anything but numerals and dashes.)

□ Are there limitations on the data fields for the database that correspond to the limitations in the fields on the user interface, so that improper data are not inserted directly into the database?

□ Are the service ports for critical applications configured to filter out data that is outside the proper operating parameters for those applications?

□ Are the limitations on what can be written into the input fields made sufficiently restrictive, wherever possible, so that those fields will not accept executable instructions?

□ Are all documents and data files classified at the higher sensitivity level stored in an encrypted form when not in use?

□ Are valid users required to provide additional passwords or other information to access highly sensitive documents and data?

Identity Authentication Systems

Authentication Policies

□ Are all corporate information systems protected with basic authentication mechanisms, such as log-in name and password?

□ Are log-in attempts limited to a certain number per minute (rather than a certain number altogether)?

□ Is the rate at which log-in's can be attempted automatically slowed further after multiple failed attempts?

□ If the log-in process is regularly under attack, is there a queuing system that would allow someone trying to properly access the system to get a turn at logging into it?

□ If an account is accessed only after a considerable number of failed log-in attempts, is that account then monitored for improper use?

□ Is there a simple automated procedure for cancelling any access provided by an employee's password, authentication token, or biometric information when that employee leaves the firm?

□ Are servers and workstation applications periodically reviewed to identify accounts that are unused or were assigned to former employees and to make sure that these accounts have been removed or assigned new passwords?

Passwords

□ Are passwords required to meet minimum length and complexity requirements, including a mixture of character types or characters chosen from large character sets?

□ Is there a program checking passwords when they are created to make sure that they meet the prescribed minimum length and complexity requirements?

□ Are password choices automatically rejected if they are on the list of most commonly used passwords or consist mostly of a commonly used password?

□ Are the characters typed into password fields masked, so that they can't be read by bystanders?

□ Do corporate policies require secure procedures for issuing and transmitting passwords?

□ Are passwords always stored in an encrypted form?

Advanced Authentication

□ If an application is sufficiently critical or the information sufficiently sensitive, does the system use advanced authentication mechanisms, such as biometrics, two-factor tokens, or challenge exchanges?

□ If advanced authentication is used as an access mechanism, is this technology applied in a consistent and effective way throughout the enterprise?

□ If an application allows access to highly sensitive information, does it require a second person to provide verification before allowing access?

Biometric Systems

□ If biometrics are employed, is a password or personal identification number also required to verify identity?

□ If biometrics are employed, are live-scans or other sensor devices employed to help verify that the readings are being taken from a live person?

□ When a biometric identifier is generated from a live reading, does it incorporate a key unique to that person, so that if the identifier is stolen, it can be replaced with another?

□ Is there a stringent enrollment process for biometric identifiers, so that there is a high degree of confidence that the data captured is from the right person?

□ Once a user's biometric information is captured, is it stored in a secure location that prevents tampering or theft?

□ Do corporate policies define the procedures for dealing with the destruction of biometric information when it is no longer required?

AREA THREE: NETWORKS

Permanent Network Connections

Connecting Equipment to the Network

□ Is each router, switch, server, work station, or other piece of information equipment required to meet minimum security standards before it is connected to the network?

□ Are the baseline standards for equipment connected to the organization's network periodically reviewed and updated?

□ Are the vendor's default security settings, including default passwords and user names, changed on systems before those systems are connected to the network?

□ Are vulnerability scans or penetration tests performed on critical systems both before they are connected to the corporate network and regularly thereafter?

□ Are employees explicitly forbidden to plug unauthorized electronic devices, such as flash drives, iPods, Kindles, smart phones, and digital cameras, into equipment inside the corporate network?

□ Are switches in critically important facilities configured so that they will not connect to any pieces of electronic equipment that are not on the list of authorized manufacturer identification (MAC) numbers?

Network Management

□ Is the network itself secured by authentication procedures, in addition to the securing of systems on the network?

□ Are the passwords used on networking equipment, such as routers and switches, required to meet especially strong minimum length and complexity requirements?

□ Does the organization require periodic checks of its routers to verify that the access control lists have been accurately implemented?

□ If the organization is maintaining multiple networks for security purposes, are the connections and communications between these separate networks limited to the absolute minimum that is necessary for the effective functioning of the organization?

□ If the organization is maintaining an internal network that is used for activities that do not require a connection to the internet, has care been taken to make sure that no direct connections between that network and the internet exist?

□ Are legitimate systems that do not require wider network connectivity kept off all wider networks?

Wireless and Special Connections

□ Are there clear and rigorously enforced rules for establishing and using wireless connections to the internal networks?

□ Is access to the wireless connections limited to authorized devices?

□ Are wireless access points in critically important facilities configured so that they will not connect to any pieces of electronic equipment that are not on the list of authorized manufacturer identification (MAC) numbers?

□ Do the wireless connections employ strong encryption technologies?

□ Are there strict requirements and procedures for deploying any modems within the corporate infrastructure?

□ Is there a documented approval process for giving people remote access to modems?

□ If it is necessary to use insecure protocols for receiving or sending data, such as the File Transfer Protocol (FTP), are these insecure protocols supplemented with security protocols at the session protocol layer (e.g., yielding FTPS) or else transmitted over a virtual private network?

□ Are virtual private network connections being utilized to provide secure communications with partner networks?

□ Is there a documented approval process for giving people access to the virtual private networks?

Cloud Provider Connections

□ Do all administrator accounts used for cloud computing resources require two-factor authentication?

□ Does the organization maintain separation between virtual machines performing more critical operations and those performing less critical operations?

□ Is the management of external cloud computing resources performed using encrypted channels?

□ Is any remote use of the cloud management interface performed over secure communication channels, such as a virtual private network?

□ Is the cloud management interface configured to restrict administrator access from unknown internet protocol addresses?

□ Is the cloud management interface designed with the minimum number of functions needed to manage the virtual machines, so that there are fewer opportunities to mount an attack utilizing those functions?

□ Is the cloud provider using hypervisors that have a boot configuration designed to disallow the use of non-certified drivers?

Intermittent Network Connections

Employee Laptops & Mobile Devices

□ Are employee laptops protected by anti-virus software?

□ Are all smart phones issued by the organization protected by anti-virus software if those devices are vulnerable to viruses?

□ Are the anti-virus signatures and definitions on employee laptops and smart phones updated as soon as new signatures are available?

□ Are employee laptops protected by internet-protection software that blocks access to dangerous websites or known hostile IP address ranges?

□ Are infrared, bluetooth, and wireless links on laptops and mobile devices disabled when not required for business functions?

□ Are remote log-in's from employee laptops required to use IP addresses that were used in the past or are consistent with the employee's expected geographical location?

□ Do remote log-in's from employee smart phones require geopositioning data from those devices that is consistent with the employee's expected geographical location?

□ Do corporate policies define security requirements for off-site wireless modems and wireless broadband connections?

□ If Voice over IP (VoIP) is employed for sensitive communications, are the transmissions encrypted?

Virtual Private Networks (VPN's)

□ Are telecommuters required to use virtual private network connections to obtain access to the corporate network?

□ If the organization uses virtual private networks, is two-factor authentication required?

□ If the organization uses a virtual private network to access highly-critical systems, are more stringent authentication mechanisms, such as tokens and biometrics, required?

□ If the organization uses virtual private networks, are the connecting computers first connected to a computer in an isolated network that runs a security check on the remote computer before it is granted access to the internal network?

□ If a web-based virtual private network is used, does it securely remove information about the session from the computer that initiated the session?

Dial-Up Modems

□ If the organization uses any dial-up modems for remote management or secure connections, do these devices have security features to verify authorized callers before connecting?

□ If the organization uses any dial-up modems for remote management or secure connections, do these devices have dial-back security features to ensure that only authorized callers are connected?

□ If the organization uses any dial-up modems for remote management or secure connections, do these devices have embedded authentication capabilities, such as pair-shared keys?

Temporary Connections Inside Facilities

□ Are there strict controls on any laptops, storage media, or other kinds of equipment that are periodically plugged into the corporate network to update software or perform other maintenance?

□ Does the organization scan all laptops that are temporarily connected to the corporate network by outside vendors and contractors to verify that they are free of viruses, worms, and other malware?

□ Are direct wireless connections to the corporate network protected by strong identification codes and strong passwords?

Public and E-Commerce Connections

Account Management

□ Does the organization mandate that accounts used to manage domain registration use two-factor authentication?

□ Has the organization enabled security features, such as a registrar-lock, on its domain registrations, to prevent unauthorized modifications?

□ Does the organization require two-factor authentication for accounts used to manage high-profile social media accounts, such as Facebook and Twitter?

Transaction Processing

□ If business transactions are being carried out over the internet, is data being collected from the customer and from the customer's computer or mobile device that will help authenticate the transaction?

□ If the mobile device uses geopositioning information, is that information employed as one of the factors that will determine whether a transaction will be allowed?

□ Is a hashed time stamp transmitted with the transaction, so that an unexplained transmission delay can trigger a demand for further authentication?

□ Are customer verifications for e-commerce transactions protected from automated attacks by the display of a visual image or audio play-back that contains a pattern which only be recognized by a human being (CAPTCHA)?

□ Is there a mechanism that will automatically terminate an e-commerce session after a period of inactivity?

□ If internet business transactions are sufficiently large financially, are these transactions authenticated both by digital certificates and by other advanced authentication mechanisms?

□ Is there a mechanism that allows customers to verify that they are on a legitimate website of the organization with which they are intending to do business?

□ If digital certificates are utilized for e-commerce transactions, are these certificates issued by an industry approved certificate authority?

□ When digital certificates are utilized for e-commerce transactions, is there a mechanism for verifying that the business is actually being conducted from the system for which the certificate was issued?

Instructions from Customers

□ Are vulnerability scans and penetration tests regularly performed on all internet or customer facing systems and applications?

□ Is all user-supplied information that is included in database queries between the client application and the database properly sanitized (i.e., escaped) prior to it use?

□ Are all queries from a client application that are not written in a highly constrained form blocked from reaching any database containing sensitive information?

□ Are all file uploads coming from public-facing websites restricted to files of a specific type and size?

□ Are all uploaded files coming from public-facing websites automatically scanned for malicious content?

Encryption Systems and Digital Certificates

□ Are encryption keys created in a secure manner, using approved industry methods?

□ Are encryption keys and digital certificates distributed in a secure manner that prevents theft?

□ Are encryption keys stored in a secure manner, using approved industry methods?

□ Are decryption procedures activated separately from ordinary log-in procedures and required to use different passwords?

□ Do systems that have certificates installed have adequate security measures that prevent the theft of the private keys of these certificates?

□ Are the repositories used to store copies of the root-certificates and code-signing certificates protected by strong encryption?

□ Is access to the repositories used to store copies of the root-certificates and code-signing certificates protected by two-factor authentication?

□ Is access to encrypted repositories for encryption keys restricted to the smallest number of administrators that will still allow access on short notice?

□ Is access to encrypted repositories for encryption keys organized so that no single administrator has access to multiple repositories?

□ Do the organization's encryption keys and digital certificates have expiration periods?

□ If a vulnerability has been discovered in the encryption software used for financial transactions, such as Secure Sockets Layer (SSL), is there a procedure to have that vulnerability patched within hours of when the patch first becomes available?

□ If a digital certificate is discovered to contain a vulnerable cryptographic component, are there procedures to have the certificate promptly re-issued by the certificate authority?

□ Are encryption keys destroyed in a secure manner, using approved industry methods?

□ Are computer systems and applications configured to verify digital certificates by automatically checking certificate revocation lists?

Firewalls, Intrusion Detection Systems, & Content Filters

Firewalls

□ Has the organization configured its network firewalls to allow only the types of traffic on its approved lists?

□ Has the organization enabled anti-spoofing on its firewalls to block ranges of private internet protocol (IP) addresses (e.g., the RFC 1918 list) coming from the internet?

□ Are personal firewalls employed on individual employees' computers, in addition to the network firewalls?

□ Are there additional internal firewalls deployed to protect critical systems from unauthorized access by internal personnel?

Intrusion Detection and Prevention

□ Are intrusion detection and/or intrusion prevention systems used on the organization's network?

□ Are signatures regularly updated on intrusion detection and prevention systems?

□ Are the instruction sets for intrusion prevention systems immediately revised when abnormal patterns of activity suggest that new kinds of attacks are being attempted?

□ Are additional signatures being collected from malware that was captured and from other intelligence sources?

□ Is there a regular procedure for adding other signatures that have been identified as dangerous to the list of those that the intrusion detection and prevention systems are blocking?

□ Is an up-to-date list maintained of the additional signatures that the intrusion prevention system has been instructed to block?

□ Is the list of additional signatures to be blocked periodically compared with the list of access attempts that *were* blocked, in order to verify these procedures are producing some benefit?

Content Filters

□ Are all e-mails and e-mail attachments received by employees automatically scanned for possible malware?

□ Are all web links in e-mails received by employees automatically checked against lists of websites known to be dangerous?

□ Are all files downloaded from the internet by employees automatically scanned for possible malicious content?

□ Does the organization use content filtering to limit to receipt of Active X, JavaScript, and Java Applets?

□ Does the organization make a serious effort to filter out all executable e-mail attachments?

□ Does the organization block internet downloads by employees that do not correspond to their work roles?

□ Are the instruction sets for content filters immediately revised when abnormal patterns of activity suggest that new kinds of attacks are being attempted?

AREA FOUR: AUTOMATION

Automated Operations and Processes

Control Networks

□ Are all control systems that do not need to be connected to the internet isolated from the internet?

□ Are all control systems that *do* need to be connected to the internet isolated by access control lists?

□ Are all connections between control systems and the internet periodically evaluated to see whether these connections are really necessary?

□ Are all control systems isolated from the corporate network whenever there is no compelling reason to connect them?

□ If a control system cannot be isolated from the corporate network, is the control system protected by highly restrictive firewalls and intrusion detection systems?

□ Are port numbers used by control systems blocked at the perimeter firewalls?

Control Devices

□ Do all new remote terminal units and other control devices being installed in the network have changeable passwords or other reprogrammable authentication mechanisms?

□ If remote terminal units and other control devices have the capability of employing passwords and the operational speed requirements allow this, are passwords being used?

□ Are the default passcodes for control systems changed before they are put into service?

□ Are status queries to remote terminal units and other control devices sent in a secure manner from a secure source?

□ Are updates to the operating systems of remote terminal units and other control devices sent in a secure manner from a secure source?

□ Do updates to the operating systems of remote terminal units and other control devices need to be digitally signed by the vendor before being applied?

□ Is the integrity of updates to the operating systems of remote terminal units and other control devices verified before these are applied?

Peripheral Devices and Physical Equipment

□ If it is economically practical, are the cases or housings of distributed, local devices closed or locked in a way that would make it difficult to access the internal electronic components without disabling the device? (E.g., are point-of-sale credit card readers designed so that it would be difficult to open them up without breaking a connection necessary for their operation?)

□ Are the default passcodes for wireless and bluetooth connected devices changed before they are put into service?

□ Are the infrared, bluetooth, and wireless links on printers and scanners disabled if they are not regularly required for business functions?

□ Is every device that could be used to do physical harm, such as medical treatment equipment, isolated from any network that is connected to the internet, unless there is a compelling reason to connect to the internet?

□ If there is a compelling reason to connect a potentially dangerous device to the internet, is this connection physically disabled (e.g., physically unplugged), except when the internet connection is needed?

Information Backup Devices and Processes

□ Is the backup regularly transferred to a storage device that is isolated from the organization's primary network?

□ Does the backup procedure include checking the data for hostile code, such as viruses and trojan horses, prior to backing-up the information?

□ Are there sufficiently rigorous procedures to restrict unauthorized physical access to backup media?

□ If the backup copy is sent electronically to a remote system, is the information transmitted to that location through encrypted means or across a dedicated secure network?

□ If the backup copies are being transported physically to a remote location, are they handled by a secure means of transport?

□ Are all of the backup media protected from physical theft during storage, whether they are stored locally or remotely?

AREA FIVE: HUMAN USERS

Individual Employee Actions

□ Are employees prohibited from using personal identification devices, such as badges and proximity cards, to give other employees access to information facilities and systems?

□ Are employees trained to avoid using passwords constructed out of personal biographical facts that might be publicly accessible?

□ Have employees been trained in the methods for constructing non-dictionary and phrase-based passwords?

□ Are employees made aware of the hazards of storing passwords in insecure places, such as on post-it notes in their work area?

□ Are employees made aware how hazardous it is to plug electronic devices, such as iPods, Kindles, smart phones, and digital cameras, into work computers, even if this is only done to charge the batteries of these devices?

□ Have physical security personnel been taught that preventing unauthorized electronic equipment, including flash drives, from being plugged in inside the organization's facilities is just as important as preventing the theft or vandalism of equipment?

□ Are employees regularly reminded not to open e-mail attachments if the e-mail is generic, seems unlikely, or has unexplained features?

□ Are employees prohibited from installing any software on corporate computers that is personal, recreational, or simply unauthorized?

□ Are employees trained to be suspicious of any software that arrives in the mail, even though it may appear to be packaged and sent by trusted vendors?

□ Are employees made aware that they should never plug in an unlabeled or suspiciously labeled memory device to see what it contains?

□ Are employees regularly reminded not to download file types from the internet that could contain executable code?

□ Have employees been made aware of the fact that mass produced and mass distributed software could still contain targeted malware?

Administrative Actions

□ Are background checks carried out on employees with higher levels of information access, even though their salaries and job titles might not indicate this level of access?

□ If an employee is promoted to a considerably higher level of responsibility and access, is a new background check carried out?

□ Is background screening carried out for building maintenance personnel with extensive physical access to information system components, such as janitors?

□ If there is a noticeable change in the personal or financial behavior of an employee with access to critical systems, is there a procedure for unobtrusively carrying out a new background check, covering such things as rapid changes in credit ratings or signs of unexplained wealth?

□ If an employee is going through a period of great difficulties in his or her personal life, is there a policy for temporarily reducing that employee's responsibilities for critical systems and access to critical systems?

Security Incident Handling

□ Do employees know how to quickly interrupt or shut down any channel of communication that is apparently being utilized by a cyber attack?

□ If a particular account is being utilized by the attack, are the account administrators ready to quickly force a log-out of that account and disable that account across the organization's networks?

AREA SIX: SUPPLIERS

Procedures for Developing New Software

□ Do corporate security policies require contractor personnel working on software development to meet minimum security requirements if the software is going to be used for critical processes or highly sensitive information?

□ Are software developers given background checks that are more thorough than those for other employees?

□ Does the organization have procedures for the orderly insertion of code during software production, so that no one has an opportunity to alter a line of code other than the programmer recorded as responsible for it?

□ If software components from third parties are going to be incorporated into libraries or applications under development, are these components examined for vulnerabilities before being accepted?

□ If software components or files from third parties are going to be installed with the program under development, but not actually incorporated into it, is the authenticity of those components and files verified before they are deployed?

□ Are changes to the source code library controlled and monitored, so that the source control module cannot be bypassed by someone with administrator privileges?

□ Is access to the software development tools that utilize code-signing digital certificates limited to authorized developers?

□ Are any user accounts employed for software testing systematically removed before the software is actually put into service?

Features to Build into New Software

Authentication Features

□ Is the application under development designed to require passwords for access that have a minimum and maximum number of characters?

□ Is the application under development designed to require passwords for access that include a mixture of character types and characters chosen from large character sets?

□ Does the application under development automatically reject weak password choices, such as those on the list of commonly used passwords?

□ Is the application under development designed to store only the hashed value of a user's password?

□ If the application under development is sufficiently critical, is it designed to require advanced authentication mechanisms, such as biometrics or two-factor tokens?

Data Management Features

□ If input fields are being built into the application, are those input fields designed to accept only data written in the appropriate characters?

□ If the application under development will receive data streams from other applications, are the characters accepted in those data streams limited to the ones needed for that type of data, so that other characters that could be used to write executable commands are excluded?

□ If a critically important program is going to call on supplementary files and separate components that are to be installed with the program, is there a mechanism that will automatically check the authenticity of those files and components each time they are used?

□ Is the application under development designed with appropriate buffer bound checking, which disregards any input that is too long?

□ Is the application under development designed to restrict direct memory access, so that buffer lengths can be controlled and enforced?

□ Is the application under development designed to protect sensitive data in memory, such as passwords and cryptographic keys, by locking memory and overwriting the memory location once the sensitive data has been used?

External Vendors

□ Do the service agreements require vendors to conduct background checks on their personnel before they are assigned to the corporate account?

□ If a software application was supplied by a third-party vendor, can the vendor demonstrate that precautions were taken to make sure that the application does not have backdoors that allow third-party access?

□ Are physical shipments from external vendors protected by tamper-resistant packaging?

□ Is there a regular procedure for verifying over the internet or by telephone that any physical shipment from the vendor is an authentic one?

□ Are there trusted channels for receiving updates from each software vendor?

□ Are there appropriate limitations and an expiry date on the access rights that the vendors need in order to install the software and updates?

□ Does the organization have processes in place to restrict internal information access by outside vendors or contractors?

□ Does the organization have processes established to identify and terminate vendor, contractor, and other outsourced personnel access when no longer required?

Making Targets Harder to Co-Opt

AREA ONE: HARDWARE

Distributed Electronic Equipment

□ Is there an explicit policy specifying what kinds of equipment can be taken off the corporate premises and what authorizations are required to remove that equipment?

□ If external hard drives and other storage devices that contain sensitive information would be easy to carry off, are they anchored down as an extra security precaution?

□ If authorized flash drives are used inside the organization's facilities, are these given a distinctive color and unique number that makes them easy to identify and trace?

□ Are employees required to declare and display any memory devices, such as flash drives, that they are carrying when they leave the organization's facilities?

□ If an employee is found leaving the facility with an unauthorized memory device, is the employee asked to submit that device for investigation, along with its access codes?

Operations Centers and Data Centers

□ Is all critical electronic equipment inside the data center physically locked in place?

□ If a piece of electronic equipment is extremely critical, is there an alarm that would warn when the rack space holding it has been unlocked, if that alarm hasn't been deactivated first?

□ Are there locking devices on empty rack spaces, so that unauthorized units cannot be easily added?

Environmental Systems

□ Do environmental controls exist, such as automatic heating and cooling systems, which can maintain a consistent operating temperature for the electronic equipment?

□ Do environmental controls exist that can keep the humidity in the areas housing electronic equipment within an acceptable range?

□ Do environmental controls exist that can protect the system from elements other than temperature and humidity, such as smoke, dust, and corrosive fumes?

Cables and Wiring Closets

□ If communication cables pass through areas that are publicly accessible, but difficult to monitor, are these cables sheathed in a manner that makes them difficult to cut or tap?

□ Are there alarms that would warn if communication cables have been cut?

□ Are emergency power shut-off switches conspicuously labeled and covered by safety panels to prevent the electric power from being inappropriately interrupted?

□ Is there protection against extreme power surges of the sort that could be produced by lightning or, possibly, by artificial means?

Physical By-Products (Used Equipment & Paper Printouts)

Electronic Equipment

□ Are there regular procedures to make sure that memory media, such as hard drives, tapes, and flash drives, are thoroughly wiped before they are reassigned to different business uses?

□ Are there sufficiently rigorous procedures to make sure memory media are thoroughly wiped before being returned for warranty replacement, publicly sold, or donated for charitable use?

□ Are the inventory labels, such as barcodes, radio frequency identification (RFID) chips, and other identifying tags removed from the equipment being destroyed or recycled, during the last stage of this process?

□ Are used CD's containing sensitive information properly destroyed (not just broken) prior to disposal?

Paper Printouts

□ Is there a rigorous plan for keeping paper printouts containing sensitive information separate from other printed materials?

□ Are documents that contain sensitive information protected from printing if there is no operational need for those documents to be printed?

□ If extremely sensitive documents need to be printed, is there a procedure in place to make sure these documents can only be printed on a supervised printer?

□ After extremely sensitive documents are printed on a supervised printer, is a physically documented chain of custody established, so that there is a designated person responsible for the security of those documents at all times?

□ Are there sufficiently rigorous procedures for the secure destruction of paper printouts by shredding or burning?

□ When extremely sensitive documents need to be destroyed, is a second person required to be physically present and to verify their destruction, before the chain of custody can be ended?

□ Has care been taken to make sure that any paper reuse and recycling programs do not undermine the secure handling of paper printouts?

AREA TWO: SOFTWARE

Applications and Operating Systems

Privilege Allocation

□ Is access to critical applications restricted to those users within the organization who actually need to use those applications?

□ Are the employees asked to provide lists of what software applications they need to access, so that these can be used as the basis for assigning them application privileges?

□ Are the employees' lists of the software applications they need to access reviewed before these application privileges are actually granted?

□ If an employee goes for many weeks without using a particular software application, is this application automatically removed from that employee's application privileges?

□ Are the software application privileges for individual employees reviewed and revised whenever there is a substantial change in their work assignments?

□ Is there an annual review of the application privileges for each employee, even if there has been no change in that employee's work assignments?

□ Are root-level and domain administrator privileges restricted to those who actually have need for those privileges?

□ If employees are given root-level or domain administrator privileges, is their need for those privileges reviewed at least semi-annually?

□ Are administrator privileges on individual computers normally kept turned off in order to prevent unauthorized software applications from being installed?

Application Usage

□ Are the relevant people within the organization alerted to any new software or hardware vulnerabilities, so that they can take protective and compensating measures to cover the period between the time those vulnerabilities were discovered and the time a relevant patch or update is installed?

□ Have the error messages been properly adjusted or designed, so that they do not reveal information about the internal design and configuration of the software?

□ Have the debugging features been disabled that would provide an avenue for obtaining information about the internal design and configuration of the software?

Patches and Updates

□ Are software patches and updates of critical systems tested prior to installation to minimize the risks of malfunctions?

□ Are the installation times for software patches and update chosen to minimize the disruption of operations?

□ Does the choice of times for the installation of software patches and updates take account of the fact that these installations might cause problems that will shut down the systems until troubleshooters can clear up the problems?

Documents and Data

General Data Access

□ Is there an automatic mechanism that can quarantine systems which may have been contaminated with false information, without shutting them down?

Data Inputs or Changes

□ Is the ability to alter or input data into documents or databases restricted to those employees who would have a valid need to do so in the course of their normal work?

□ Are data fields that would rarely need to be changed made read-only as soon as the data entry is verified as correct?

□ Are documents that present the organization's work or positions converted into formats that cannot be easily modified, before they are circulated electronically outside the organization?

□ When documents are converted into formats that cannot be easily modified, are those documents digitally signed to make them even harder to falsify?

□ Are the digital signatures on important documents routinely checked to verify their source before those documents are accepted and utilized?

□ Are critically important e-mails sent using an application that hashes their contents, so that the e-mails' contents cannot easily be falsified?

□ Are critically important e-mails sent using an application that adds a digital signature, so that their sender's identity cannot easily be falsified?

Data Exports

□ Is a valid user prevented from improperly uploading or downloading sensitive data files from the system to another system?

□ Is the ability to produce outputs of sensitive information, such as printed versions and e-mail attachments, restricted to what the user's job and responsibilities would require?

□ Are employees prevented from saving sensitive information to local storage devices, such as CD's, DVD's, or USB drives, except in cases where business needs require this?

□ Is there an automatic limitation on the amount of data that can be downloaded at any one time from any file repository or database containing sensitive information?

□ Are pieces of information that an attacker would want to use together kept in different files that need to be accessed in different ways? (E.g., are customers' Social Security Numbers stored in a file that is different from and is accessed differently than the file containing their account numbers and passwords?)

Identity Authentication Systems

□ Are employees required to change their passwords on a routine schedule mandated by corporate policy?

□ Are employees prevented from using previous passwords when a scheduled password change is required?

□ Are terminals and software systems set to lock out the user and require a new log-in when there is a period of inactivity or when some other device indicates that the employee has left the terminal?

AREA THREE: NETWORKS

Permanent Network Connections

Network Management

□ Is there a mechanism to automatically restart critical components, such as web server applications, whenever other applications are repeatedly unable to connect with them?

□ Are internal wireless networks segmented, using different service set identifiers (SSID's) or another method, so that access to one segment of the wireless network does not automatically provide access to the other segments, and so that more restrictive policies can be applied to the more critical parts of the network?

□ Does the organization have agreements with vendors in which they guarantee a specified level of network reliability and service?

□ Do corporate policies limit the use of unencrypted protocols, such as FTP, Telnet, or earlier versions of SNMP, for system management, unless the system explicitly requires these protocols?

□ If the systems require unencrypted protocols, such as FTP, Telnet, or earlier versions of SNMP, for their management, are the corresponding connections set to shut down after a limited period of time?

□ Does the corporation use access control lists to restrict SNMP requests from unauthorized systems to networking equipment, such as routers and switches?

□ Are there policies for limiting the use of any remote management tools that would allow systems to be controlled from outside the corporate network?

□ Is the remote management of routers, switches, and other network components restricted to authorized internet protocol addresses?

□ Are there policies for monitoring the use of any remote management tools that would allow systems to be controlled from outside the corporate network?

Traffic Handling

□ Have the networking components been configured to give more critical categories of traffic, such as process control instructions, priority over less critical categories of traffic, such as e-mails?

□ Are there procedures for rate-limiting traffic so that the network is not incapacitated by excessive loads on the services affected?

□ Have tests been conducted to make sure that critical systems cannot be taken offline too easily by large amounts of data or traffic, such as might be employed in a denial service attack?

□ Are there procedures for adding additional servers and redirecting traffic to prevent critical network components from being incapacitated by excessive loads on the services affected?

Cloud Provider Connections

Cloud Management

□ Is all sensitive information that the organization stores in the cloud encrypted?

□ Is all sensitive information transmitted between the client and the cloud encrypted?

□ Does the cloud provider maintain redundant secure communication channels for accessing the cloud management interfaces?

□ If the organization performs critical operations using external cloud computing resources, are these operations logically isolated from other virtual machines by the use of a separate hardware-level hypervisor?

□ Is the organization choosing virtual machines for its critical operations that are designed to fail to a state which protects the system from security compromises and data breaches?

□ If the organization performs *highly* critical operations using external cloud computing resources, is a special arrangement made with the cloud provider to host those operations on dedicated servers, used only by the organization?

Third-Party Collaborative Platforms

□ If the organization allows its employees to use third-party collaborative platforms, such as Google Docs or Dropbox, for standard business operations, do they require employees to use only those platforms that encrypt all files at rest?

□ Does the organization require its employees to refrain from putting any information on third-party collaborative platforms if it is considered very sensitive?

□ If the organization allows its employees to use third-party collaborative platforms, such as Google Docs or Dropbox for standard business operations, has two-step log-in verification been implemented for those accounts?

□ Are employees prevented from using personally owned smart phones to access third-party collaborative platforms used for work?

□ Are employees forbidden from placing work documents in personal accounts on third-party collaborative platforms?

□ Does the organization make it a policy to limit the length of time over which work documents are stored or handled on third-party collaborative platforms?

□ Does the organization periodically verify that documents which no longer need to be handled on third-party collaborative platforms have been removed from those platforms?

Intermittent Network Connections

□ If smart phones and other small mobile devices are allowed, does the organization restrict sensitive information from being downloaded to these devices?

□ If a large portion of the activities carried out on an employee's laptop involve highly sensitive information, is the entire hard drive on that laptop encrypted?

□ If only a modest portion of the activities carried out on an employee's laptop involve sensitive information, are the documents and data files containing that information encrypted using encryption containers or single file encryption?

□ If sensitive information needs to be stored on laptops or other mobile devices only temporarily, is the tool for encrypting and decrypting that information extremely convenient to use?

□ Are internal microphones and cameras on laptops disabled within sensitive areas?

□ If employee e-mails contain sensitive information, are these e-mails encrypted during transmission?

□ If an employee laptop contains a CD drive that could be used for booting in an emergency, is the boot sequence of that laptop set so that it cannot be booted from a USB connection?

□ If an employee laptop contains information sensitive enough to require full disk encryption, is the boot sequence of that laptop set so that it can only be booted from its internal hard drive?

□ If a service application needs to be kept proprietary for competitive purposes, is it made web-accessible only to trusted personnel, rather than web-accessible to a wider population?

Public and E-Commerce Connections

□ Does the organization make it a policy never to send links to its website in e-mails, except for the address of its home webpage?

□ Are customer log-in screens normally accessed from the organization's home webpage?

□ Has the organization purchased any available web addresses that could easily be mistaken for its own?

□ Are all transactions associated with an individual user session accompanied by a unique, unpredictable session code that is included to prevent the codes for establishing the session from being reused by an attacker?

□ Is sensitive customer information, such as credit card numbers and personal identifiers, handled by systems different from the one that handles the web transaction itself?

□ If a financial transaction or business order is considerably larger than the normal range, does the transaction automatically require extra verification?

□ Are the file names used for storing files uploaded from public-facing websites completely different from the names of the users who supplied the information?

□ If the organization allows customers to post reviews on its website, is care taken to make sure that these postings do not reveal the customers' e-mail addresses or log-in names?

□ If the organization uses a social media account, such as a Twitter, for communicating security warnings, are all matters that don't serve this purpose kept off of that account?

Encryption Systems and Digital Certificates

□ If private encryption keys are maintained, are they archived in a password protected and encrypted area to prevent tampering or theft?

□ Are encryption keys that are used for different tasks stored in different encrypted repositories?

□ Is there a reliable system for renewing digital certificates used on any customer website, so that customers will never have to ignore security warnings to proceed to the site?

Firewalls, Intrusion Detection Systems, & Content Filters

Firewalls

□ Does the organization have an approval process for any changes in the rule sets defining the traffic it will allow through its firewalls?

□ Is network access to the management interfaces of firewalls, intrusion prevention systems, and content filters restricted to only authorized internet protocol (IP) addresses?

Content Filters

□ Are all uploads to the internet by employees restricted by a content filter to information and files of specific types and below certain sizes?

□ Does the organization perform content filtering on all file attachments being sent through e-mail, so that any transmission of sensitive information by this means is either blocked or tracked?

□ Does the organization perform content filtering on all outbound file transfer protocol (FTP) or trivial file transfer protocol (TFTP) transmissions, so that any transmission of sensitive information by these means is either blocked or tracked?

□ Does the organization use content filtering to control instant messages that may contain sensitive information?

□ Are content filters set to block export of sensitive documents tagged with digital watermarks, unless special authorization has been provided to export them?

□ Are content filters employed to help prevent confidential information from being uploaded to third-party collaborative platforms, such as Google Docs or Dropbox?

□ Are content filters employed to help prevent confidential information from being uploaded to web-based e-mail applications?

□ Are content filters employed to help prevent the transmission of sensitive information through social media and electronic greeting card portals?

AREA FOUR: AUTOMATION

Automated Operations and Processes

Range of Action

□ Are the computers inside production facilities extremely limited in the software applications they contain?

□ Are the schematic diagrams and instructions for managing physical processes kept in a system that is separate from the system that is used for the command inputs controlling those processes?

□ Are there pre-set parameters for inputs governing critical processes, so that attempted inputs outside those parameters are either blocked or need confirmation from another source?

□ If control systems that manage highly critical processes, especially dangerous ones, are severely disrupted, do these processes automatically revert to a safe, stable state or go into a controlled shut-down?

□ Have the remote sensors been designed or modified to make it difficult for someone to cause them to report false data by manipulating them physically?

Transmission of Instructions

□ Are the computers in production facilities extremely limited in the kinds of information they can receive and send?

□ If the command codes for control system components have been customized to not use the default formulas, are the control systems configured to ignore any commands that *do* follow the default formulas?

□ Are all periodic automated transmissions of critical control data, where speed is not an issue, protected by encryption?

□ Is there a separate, second channel for putting highly critical processes, such as physically dangerous ones, into a safe, stable state or into a controlled shut-down?

□ If remote sensors communicate via cellular, satellite, or other wireless connections, have measures been taken to prevent information transmissions from being falsified?

Time Controls

□ Are all critical system components within the network synchronized, so that they are using the same time zone?

□ Are critical system components configured to regularly update their time from a secure time source?

□ Do especially critical system components periodically update their time from different time sources, so that any spoofing or corruption of the communications with one time source would be detected?

Peripheral Devices and Physical Equipment

□ Are the data storage components inside distributed, local devices installed in such a way that they cannot be easily removed from the device?

□ Whenever possible, is the data that is being transmitted between devices encrypted?

□ Whenever possible, is the data being transmitted between devices and the local computers coordinating their activities encrypted?

□ Are video feeds from drones and other autonomous or semi-autonomous devices encrypted?

□ Are different devices given different passcodes, so that they cannot all be accessed in the same way at the same time?

□ If peripheral devices used locally, such as printers and scanners, can hold large amounts of data, are these devices prevented from sending or receiving large amounts of data over the internet?

□ If a critically important device, such as a piece of medical treatment equipment, needs to be periodically recalibrated, is that recalibration carried out using a different computer than the one normally used to control the device?

□ If data collected from distributed, local devices could be used to deduce personal information, is that data stored only in an encrypted form?

Information Backup Devices and Processes

□ If the information being backed up is sensitive or proprietary in nature, is the information encrypted during the backup process, so that it is stored in an encrypted form?

□ Are any encryption keys used in backup stored in a secure location and rotated to ensure that the one compromised key does not expose all the data?

□ Are the encryption keys for the backups, along with a schedule of when and where they were used, stored in a secure form at another location?

□ Is the backup regularly transferred to a physically remote location?

□ If the loss of the backed-up information would jeopardize the enterprise, are there backups stored at more than one remote location?

□ When the backup storage media are no longer needed for backup purposes, are there secure procedures for destroying or reusing those media, whether they are stored locally or remotely?

AREA FIVE: HUMAN USERS

Individual Employee Actions

□ Have the employees been trained not to fall victim to social manipulations by telephone or over the internet that would led them to reveal security-related information?

□ Have the employees been trained never to type or dial specific sequences of numbers or characters when someone they do not know is requesting them to do this?

□ Does the organization restrict employee access to critical systems from unsupervised locations and at unsupervised times?

□ Are areas of responsibility distributed among employees in such a way that a single employee cannot carry out a critical operation without the knowledge of other employees?

□ If a given category of input is sufficiently critical, does the organization require a second employee to verify that input before it is processed?

□ Do extremely critical operations require the active, simultaneous participation of two or more employees?

□ Are information technology employees made aware of how dangerous it is to install network links, such as modems or wireless connections, that are undocumented and not authorized by security personnel, even though these links might be requested by senior executives?

□ Does the organization warn all employees who are leaving the organization that they need to respect the organization's intellectual property?

Administrative Actions

□ Are employees monitoring critical systems that seldom change given something to do that will make their jobs less boring?

□ Does the organization make fairness and good faith in the treatment of employees a higher priority than seizing every opportunity to gain a short-term competitive edge?

□ Does the organization make a point of acknowledging, at meetings attended by many other employees, any individual employee working with information systems who has done work that is especially reliable, skillful, or innovative?

□ Does the organization provide a channel through which employees can anonymously nominate other employees or themselves for special recognition, based on work with information systems that is unusually reliable, skillful, or innovative?

□ Does the organization provide adequate mechanisms for employees to express their grievances without penalty and for them to see those grievances being conscientiously addressed?

□ Does the organization handle down-sizings in a manner that minimizes hostile feelings on the part of former employees?

Security Incident Handling

□ If there is reason to believe a major cyber attack may be immanent, is there a plan for temporarily cutting back on vulnerable activities and shutting down dispensable communication channels, in order to limit the effects of that attack?

□ If a serious attack has occurred, are there procedures that can be implemented very rapidly that will isolate or quarantine any system that may have been contaminated with malware or false information *without* shutting it down?

□ Are there procedures that can be rapidly employed to *manually* isolate or quarantine each system if there is reason to distrust the computerized procedures for accomplishing this?

□ Are any cables that should be physically unplugged in the event of an attack clearly labeled?

□ Do employees know which cables to unplug in the event of an attack and what events should trigger this response?

□ If an attack is causing data to be deleted or encrypted on a local computer, have employees been authorized to immediately shut off that computer?

□ Are there procedures for rapidly modularizing or compartmentalizing operations and systems beyond those likely to have been affected by the attack, as a further precaution?

□ Are there separate systems or procedures for monitoring each of the systems that has been isolated or quarantined?

□ After the affected systems have been isolated or quarantined, do the procedures for dealing with a serious or sustained cyber attack require the cyber-security team to pause and consider what the attack is probably trying to accomplish before taking further steps to deal with it?

□ Does the procedure for responding to a cyber attack remind the cyber-security team that the observable attack might be intended to cover or distract from another attack?

□ Do employees know how to switch over to alternative channels of communication in the event of normal channels being compromised?

□ Is there a procedure for moving the quarantine lines when better information about the possible contamination becomes available?

AREA SIX: SUPPLIERS

Procedures for Developing New Software

□ Does the organization have pre-approved code modules that can be inserted into new software to accomplish standard security functions, such as authentication and encryption?

□ Does the organization have pre-approved code modules for managing file transfers and other communication functions?

□ Does the organization provide developers with dummy data, so that the applications under development do not have to be tried out on private, sensitive, or proprietary information?

□ Are all dummy data used for software testing systematically removed before the software is actually put into service?

□ Are the applications under development tried out in test bed environments that are completely isolated from the actual production environments?

□ If there are embedded comments by developers on the source code that survive the development process, are these comments manually removed before the program is deployed?

Features to Build into New Software

General Functions

□ Is the application under development designed to request and release resources in a systematic way?

□ Is the application under development designed to limit the demands its operations make on system resources, so that these are not overloaded?

□ If a process within the application under development receives or retrieves information that is not in the form on which the process is designed to operate, is the process given an alternative operation to perform, so that it does not crash?

□ If the application under development is intended to control highly critical or dangerous processes, is it written in a programming language that was designed to avoid type errors, buffer overflows, and other software vulnerabilities, such as Ada or its dialect Spark, rather than a programming language where these problems are chronic, such as C, C++, or Objective-C?

General Privilege Management

□ Is the application under development designed to use the concept of least privilege when executing instructions?

□ Is the application under development designed to have privilege separation during operations?

□ Is the application under development designed to set appropriate permissions on all resident files installed with the application?

□ Is the application under development designed to set appropriate permissions on temporary files?

Data Management

□ Is the application under development designed to create new, random file names for each operation, rather than reuse file names?

□ Is the application under development designed to verify that file writes are only allowed on files using an absolute path to the same disk location**?**

□ Is the application under development designed to write to a directory location that can only be accessed by that application, rather than to a standard temporary directory location (e.g., /tmp)?

□ Is the application under development designed to verify that commands to delete data are only allowed to file and folders using an absolute path to the same disk location**?**

□ Is the application under development designed to erase thoroughly any data generated during intermediate steps in the execution of the program (good garbage collection)?

□ Is the application under development designed to encrypt sensitive information that it stores in a file or database?

□ Is the application under development designed to encrypt sensitive information that it writes to cookies?

External Vendors

□ Are prospective software vendors and outside developers limited to those who can be verified to meet industry standards for information security?

□ Are software vendors required to keep records of which employee or outside contributor wrote each line of code for any software being purchased?

□ Are software vendors required to certify that their code has undergone a rigorous and thorough security inspection before it is delivered for deployment?

□ Do vendors provide physical shipments with packaging and labels that are difficult to counterfeit or tamper with?

□ If a vendor is sending out software, updates, or patches, does it post hashes of these software products on its website, so that the integrity of these products can be verified?

□ When software updates need to be applied, is there a guarantee that those updates were adequately tested in the relevant kind of software environment before being installed?

□ Are there procedures for verifying that copies of proprietary information were destroyed after the vendors delivered the contracted software?

Making Attacks Harder to Conceal

AREA ONE: HARDWARE

Distributed Electronic Equipment

Physical Access Privileges

□ Are any changes in the lists of employees who are allowed access to highly sensitive areas promptly reviewed to make sure these changes are authorized and reasonable?

□ Are the people who authorize physical access asked, at random intervals, to verify that they did indeed authorize the physical entries that they are recorded as having authorized?

□ If employees use their identification badges or other authentication to enter sensitive areas, are both their entrances into and exits from these areas logged, with the exact times noted?

□ Are the logs of the times employees spend in sensitive areas regularly reviewed to see whether these times are consistent with the employee's work responsibilities?

□ Are the logs of the times employees spend in sensitive areas regularly reviewed to see whether these correspond to times when the employee was also recorded as being present in the larger facility?

□ If there is an unexplained discrepancy between the logs recording employees' times spent in sensitive areas and their work responsibilities or other logs of their movements, are these discrepancies investigated in a timely fashion?

□ Is video surveillance used to monitor access to areas where critical information processing equipment is located outside of data centers?

□ If security cameras, especially wireless ones, are used for monitoring, are they protected from jamming, unauthorized viewing, and the spoofing of images?

Physical Equipment

□ Is each piece of electronic equipment labeled with a barcode or other identifier for easy tracking?

□ If electronic equipment needs to be taken off the corporate premises, is there an efficient procedure for tracking the movement of that equipment?

□ Are authorized flash drives and other memory devices tagged with radio frequency identification (RFID) chips, so that their movements can be traced almost in real time?

□ Are people leaving the organization's facilities electronically scanned for radio frequency identification (RFID) chips or other signs that they removing electronic equipment from the facility without authorization?

□ Are unannounced spot checks periodically carried out to verify that the electronic equipment is present at the locations designated in the equipment inventory?

□ Is there a system for electronically verifying that the right pieces of equipment, identified by manufacturer identification (MAC) number, are plugged into the right locations, identified by IP address?

□ If there are discrepancies between the inventory of electronic equipment and the equipment actually found in the corresponding facility unit or room, are these discrepancies immediately investigated?

□ Where the physical media access ports are regularly used and, hence, not disabled, are there procedures to electronically monitor for unauthorized access of these ports?

□ If employees observe personal, unauthorized electronic devices, including flash drives, being used inside the organization's facilities, is there an easy-to-use, private channel for reporting this and an incentive to do so?

Operations Centers and Data Centers

□ Are all activities inside the operations center clearly visible through large windows or on large video screens that are in easy view of other employees (but not casual visitors)?

□ Are personnel leaving the data center registered as doing so by an automatic system or by actively scanning their identification device?

□ Is each instance when someone enters or leaves the data center automatically reported to a remote location and securely logged?

□ Is the data center equipped with an intrusion alarm that would be triggered by signs of activity there when no one with authorized access is known to be inside?

□ Is the intrusion alarm for the data center monitored offsite?

□ Is video surveillance used to monitor access routes to the data centers?

□ If there is video surveillance of the data center, is it monitored off-site?

□ If there is video surveillance of the data center, is the video recorded in a permanent medium that prevents tampering?

□ If there is video surveillance of the data center, are the video recordings retained long enough so that they would still be available to investigate a security breach that wasn't detected for several months?

□ If employees observe unauthorized activities going on inside the data center, such as unauthorized personnel entering or equipment being moved without proper authorization and documentation, is there an easy-to-use, private channel for reporting this and an incentive to do so?

□ Are the logs for the data center's access control mechanisms (e.g., key cards and video surveillance logs) reviewed on a regular basis?

□ Does the review of the data center's physical access records include an analysis of failed physical access attempts?

□ If there are indicators of suspicious activity involving access to the data center or behavior inside it, are these cases investigated in a timely manner?

Environmental Systems

□ Are the environmental control consoles in locations monitored by video cameras?

□ Are there an independent set of sensors for temperature, smoke, and moisture in the data center and wiring closets that would warn when a hazardous condition develops, even if the normal environmental control systems are not registering a problem?

□ Is there an alarm, including both sound and light, that will be automatically triggered if the conditions in the physical environment become dangerous for people or for the electronic equipment?

□ If the dangerous conditions involve fire, will firefighters and other first responders automatically be summoned?

Cables and Wiring Closets

□ Are the wiring closets equipped with intrusion alarms?

□ Is access to the wiring closets monitored by video cameras?

□ Are the intrusion alarms for the wiring closets monitored offsite?

□ Are the logs recording when the keys, tokens, or access codes for the wiring closets are signed out, used, and signed in regularly reviewed to make sure that the access periods correspond to the work that needed to be done?

□ Are there video cameras inside the larger wiring closets that are activated by motion sensors?

□ Are emergency power shut-off switches in locations monitored by video cameras?

Physical By-Products (Used Equipment & Paper Printouts)

Electronic Equipment

□ Are the occasions when memory devices are removed for destruction or recycling used as an opportunity to verify that the inventory of electronic equipment in that room or area corresponds to the electronic equipment that can actually be found in that room or area?

□ Is the thorough wiping or secure destruction of each memory device regularly attested by two parties?

□ Are the records documenting the thorough wiping or secure destruction of each memory device themselves securely stored in a tamper-proof format?

Paper Printouts

□ If a document is highly sensitive, is it only printed or copied onto paper that has a distinctive shade or color, so that employees will be able to tell if it turns up in a context where it doesn't belong?

□ Are the locations where paper printouts containing sensitive information are stored prior to their secure destruction subject to video surveillance?

□ Is the actual process by which paper printouts containing sensitive information are physically destroyed subject to video surveillance?

AREA TWO: SOFTWARE

Applications and Operating Systems

□ Is every computer belonging to the organization regularly scanned for malware and hacking tools?

□ Are all increases in application privileges logged and reviewed?

□ Are any grants of root-level or domain administrator privileges immediately reviewed to confirm that they were necessary for operational purposes?

□ Does the periodic review of root-level or domain administrator privileges include verification that these privileges were being used correctly?

□ Are security settings and configurations automatically rechecked after patches and upgrades have been installed to make sure that they have not been inadvertently reset to less secure or default settings?

□ Is there a regular procedure to verify that the software patches and updates that were being tracked were indeed installed in a timely and orderly manner?

□ Does the organization have information security specialists conduct regular vulnerability testing on applications after they are deployed?

□ If applications are more critical, is the vulnerability testing of these applications carried out more often?

Documents and Data

General Data Access

□ Is there an alarm mechanism that warns if files are being accessed in unusual quantities or in sequences that are not consistent with normal work patterns?

□ Are "normal work patterns" specified using descriptions by employees of what work patterns would make sense, rather than relying exclusively on the patterns that would be detected by an unassisted software program?

□ Is there an alarm mechanism that warns if files are being accessed at unusual hours of the day or night, when computers could carry out unauthorized processes unobserved?

□ Are false "honeypot" files employed to detect unauthorized explorations of the organization's documents or data?

□ Is there an alarm mechanism that warns if unusual database commands are suddenly being used?

Data Inputs or Changes

□ Is there an automatic process for monitoring systems for symptoms that false information may have been inserted?

□ If there is reason to believe an attacker could benefit greatly from altering a body of data, is that data associated with a hash that would reveal if the data has been altered?

□ Is there a mechanism for monitoring and logging all changes to critical databases?

□ Are all uploads of sensitive data files monitored and logged?

□ Are all uploads of encrypted data files monitored and logged?

□ Is there an alarm mechanism that warns if data is apparently being entered by employees in quantities or with distributions that are not consistent with those employees' normal work patterns?

□ If logging of data change has been implemented, is the log regularly analyzed for any unusual alteration patterns in databases?

□ Is the log of changes made to critical databases regularly analyzed for unusual access patterns, including unusual access times and frequencies?

□ Is there any provision for detecting situations in which bogus data or instructions are being inserted without detectable intrusions?

□ Is there any provision for detecting situations in which there are unusual patterns of alteration in databases, even when there might not have been any unusual access patterns?

Data Exports

□ If employees can save sensitive information to a local memory device, is this action monitored and logged?

□ Does the organization tag highly sensitive documents with digital watermarks, so that content filters can more easily identify them if an effort is made to export them?

□ Does the organization embed beacons in highly sensitive documents that will contact the document's source if those documents are opened by a user on a device connected to the internet?

Identity Authentication Systems

□ Do corporate policies require that all access attempts be logged, regardless of whether they are successful or unsuccessful, for applications that perform critical functions or store sensitive information?

□ Are all access logs written to a non-rewriteable disk or other permanent medium where even the systems administrator cannot tamper with them?

□ Are there automatic alarms triggered by multiple failed log-in attempts, even if distributed across time, across user ID's, or different systems?

□ Are multiple failed attempts to access applications reviewed in a timely manner, even if those failed access attempts are by authorized employees?

□ Is an effort made to identify and investigate successful access authentications that are carried out at unusual hours of the day or night?

□ Is there an alarm mechanism that would warn of the theft of a file in which passwords are stored?

□ Is there an alarm mechanism that would warn if a large number of passwords are being accessed from the files in which they are stored?

□ Is there an alarm mechanism that would warn if an unassigned general root-level or domain administrator account is utilized?

□ Are all changes that a systems administrator makes to passwords logged and reviewed?

□ Is there an alarm mechanism that sends a notification signal if an attempt is made to use a two-factor token or smart card after it has been revoked?

□ Is there an alarm mechanism that sends a notification signal if an attempt is made to use a deactivated user account?

AREA THREE: NETWORKS

Permanent Network Connections

Unauthorized Equipment

□ Is the network automatically and frequently scanned for connections to pieces of electronic equipment with manufacturer identification (MAC) numbers that are not on the list of authorized devices?

□ Does the organization monitor for symptoms of manufacturer identification (MAC) numbers being spoofed, such as a mismatched operating system, mismatched device type, incorrect device location, and uncharacteristic behavior of the device?

□ Is a wireless analyzer periodically run to identify any unauthorized wireless devices that may have been connected to the network?

□ Are internal war-dialing campaigns periodically carried out to identify unauthorized modems that can be reached by dialing in?

□ Are corporate phone exchanges periodically checked to detect outside attempts at finding unauthorized modems by war-dialing campaigns?

Network Management

□ Is there a mechanism to automatically inform the system operator whenever critical components are shut down and restarted?

□ Are network software components automatically tested on startup for changes in security configurations that have been made since the system was last started and, if changes are found, is the system administrator automatically notified?

□ Are all modifications of server configurations logged?

□ Are the logs of server configurations regularly reviewed to make sure that any changes in the configurations did not undermine security?

□ If the servers are performing critical operations or store very sensitive information, are the logs recording changes in their configurations reviewed daily?

□ Are all modifications of router and switch configurations logged?

□ Are the logs of router and switch configurations regularly reviewed to make sure that changes in configurations did not undermine security?

□ Are all modifications of wireless access point configurations logged?

□ Are the logs of wireless access point configurations regularly reviewed to make sure that changes in configurations did not undermine security?

Network Monitoring

□ Is the network traffic regularly monitored to establish normal usage patterns?

□ If the organization is maintaining multiple networks for security purposes, are there special provisions for monitoring traffic between those networks?

□ If there are significant changes in the volumes and pathways of network traffic, are the reasons for these changes investigated in a timely fashion?

□ Are measures taken to monitor domain name system (DNS) servers for attacks that reroute requests to unauthorized locations?

□ Is the network traffic regularly monitored for covert communication channels?

Cloud Provider Connections

□ Are databases located at external provider of cloud computing services monitored for large data transfers that are outside normal behavior?

□ Are the access logs for the cloud management interfaces transmitted over a secure channel to an external server, where even the systems administrator cannot tamper with them?

Intermittent Network Connections

□ If removable information devices are allowed, does the organization monitor the usage of such devices?

□ Is each employee assigned a different identification code and password for connecting to the wireless network, so that employee activities using this network can be readily tracked?

□ Are the activities carried out by laptops that are temporarily connected to the corporate network by outside vendors and contractors tracked and monitored?

□ If Voice over IP (VoIP) is employed for sensitive communications, are the transmissions randomly scanned to detect content consisting of data, rather than voice?

□ If the organization uses any dial-up modems for remote management or secure connections, do these devices provide an audit trail for authorized log-ins and activities such as "break in" attempts?

□ Is there extra monitoring of remote connection activities to compensate for the fact that they are less supervised in other respects?

□ Does the organization monitor its inbound internet traffic for signs of session hijacking (e.g. sequence numbers out of sequence)?

□ If there are indicators of session hijacking activity being carried out, are these cases investigated in a timely manner?

Public and E-Commerce Connections

□ Is there an alarm mechanism that warns if internet business transactions involve unusual combinations of customer identities, billing addresses, and shipping addresses?

□ Does the organization choose easily recognizable uniform resource locators (URL's) for its e-commerce web pages, so that customers will see that these URL's look authentic?

□ Does the organization regularly search the web for bogus websites that pretend to belong to the organization?

□ Does the organization regularly search the web for bogus smart phone applications that pretend to facilitate secure connections to the organization's websites?

□ Does the organization monitor its high-profile social media accounts, such as Facebook and Twitter, for signs of unauthorized access or use?

□ Has the organization implemented the Sender Policy Framework for all their mail servers, in order to detect and prevent e-mail spoofing?

□ Does the organization provide the public with contact channels, including both a phone number and e-mail address, that are to be used only for reporting possible security issues?

Encryption Systems and Digital Certificates

□ Is the generation of encryption keys logged in a tamper-proof file that records the generating employee's identity and the time?

□ Does the organization periodically review Secure Sockets Layer (SSL) traffic to identify locations which are inconsistent with normal business operations?

□ Does the organization periodically review Secure Sockets Layer (SSL) traffic to identify traffic that might be using a custom encryption scheme masquerading as legitimate SSL?

Firewalls, Intrusion Detection Systems, & Content Filters

Firewalls

□ Does the organization require periodic checks of its firewalls to verify that the rule sets have been accurately implemented with no ad hoc changes?

□ Are configuration modifications to firewalls logged?

□ Are security logs for firewalls maintained in a way that prevents them from being modified or deleted?

□ Are security logs for firewalls regularly reviewed to establish baselines for normal traffic patterns?

□ Are security logs for firewalls regularly reviewed for unauthorized traffic?

Intrusion Detection and Prevention

□ Are security alerts from intrusion detection systems continuously monitored?

□ Are configuration modifications to intrusion detection systems and intrusion prevention systems automatically logged?

□ Are security logs for intrusion detection and intrusion prevention systems maintained in a way that prevents them from being modified or deleted?

□ Are security logs for intrusion detection systems regularly reviewed to detect abnormal patterns of activity?

□ If an attempt is made to access the organization's internal network using the organization's own range of private internet protocol addresses, does this trigger a warning alarm?

□ If the organization is utilizing unconventional port numbers for communications involving its own computers, do communications that appear to come from its own computers, but utilize the conventional port numbers, trigger a warning alarm?

□ If abnormal patterns of activity are detected in the intrusion detection logs, are these immediately analyzed to determine what new types of attacks are potentially being attempted?

Content Filters

□ Are content filters regularly tested to make sure they are actually blocking what they are supposed to be blocking?

□ Does the organization have procedures for reviewing e-mail attachments that have been quarantined?

AREA FOUR: AUTOMATION

Automated Operations and Processes

□ Are there sufficient alarms to warn operators when any critical processes are in danger of moving outside the normal parameters of safe operation?

□ If a large portion of the schematic diagrams and instructions for managing physical processes are accessed in a short period of time, does this automatically trigger a warning alarm?

□ Are there provisions, such as remote alarms, which would warn that remote sensors are being physically manipulated on site to produce false readings?

□ Are there second sets of sensors that monitor critical processes with a different measuring technique, so that a false reading from the first set of sensors would be rapidly detected?

□ Are there regular procedures for checking adjustments and changes in control systems to make sure that the changes which should correlate do, in fact, correlate?

□ Are "honeypot" controls that appear to function, but don't actually do anything, employed to detect unauthorized explorations of the automated control systems?

□ Are the computers and systems that run quality control checks kept separate from the computers and systems that control production operations?

□ Are access procedures and codes for the computers and systems that run quality control checks considerably different from the access procedures and codes for the computers and systems that control production operations?

□ Are the details of the quality control test procedures known only to those employees who are actually carrying out those test procedures?

□ Are the records of production outputs that fail their quality control tests periodically examined to determine if those quality control problems could have been caused by cyber attacks?

Peripheral Devices and Physical Equipment

□ Are distributed, local devices equipped with tamper-proof seals that will reveal if their cases or housings have been opened?

□ If a local device that needs to be connected to the internet sends or receives data at unusual times, frequencies, or volumes, does this trigger an automatic warning alarm?

□ If there are indicators of unusual types or quantities of activity being carried out by local devices, are these cases investigated in a timely manner?

□ Is the traffic generated by local devices periodically scanned to determine if any data is being sent in clear text that should be encrypted?

□ If a local device, such as a piece of medical treatment equipment, contains customized settings that are highly important, are the most critical of these settings regularly checked to be verify that they have not been improperly changed?

Information Backup Devices and Processes

□ Are the backups regularly tested to ensure that they are readable and uncorrupted?

□ Are the backups randomly tested to ensure that the data has not been modified?

□ If the backup copies are being transported physically to a remote location, are they placed in tamper-proof containers and tracked in transit?

□ Are the protective cases for transporting backup media equipped with global position tracking devices?

□ Are all logs of activity that could have relevance for security backed up frequently and stored in a form that would prevent tampering?

□ Are the log files of application access regularly backed up to a secure location?

□ Are the log files of application access held for a long enough periods, so that any sources of gradual data corruption could be tracked down?

AREA FIVE: HUMAN USERS

Individual Employee Actions

Security Accountability

□ Are employees prohibited from letting other employees use their work computers?

□ Are employees prohibited from sharing passwords, even with other employees who are authorized to access the same systems?

Employee Monitoring

□ Is there a system for collecting and collating information on which physical facilities and information resources each employee is accessing?

□ Is video surveillance carried out on building maintenance personnel, such as janitors, even in areas that are only moderately sensitive?

□ Are the employees' physical and electronic access logs periodically reviewed to identify access patterns that are not motivated by normal work responsibilities?

□ Are employees prevented from accessing files that would reveal when their behavior is being monitored and whether it has attracted special attention?

□ Are employees required to take periodic vacations, so that ongoing activities they might otherwise be able to conceal would be noticed by their temporary replacements?

□ Are special web searches periodically carried out to discover if employees are improperly posting information that could be useful to cyber attackers?

□ Does the organization begin closely monitoring the data accessed by employees as soon as those employees give notice that they intend to leave the organization?

□ Does the organization review the data accessed by any employees during the ninety days prior to the date they give notice that they intend to leave the organization?

Security Reporting

□ Are various cyber-attack strategies described to employees in enough detail and with enough variations, so that the employees would have a good chance of recognizing the early signs of such attacks?

□ If employees use an internet link supplied to them by another employee or anyone else, are they taught always to check the uniform resource locator (URL) that appears in their browser window to make sure that has an appropriate domain and looks authentic?

□ Are employees provided with an easy way of reporting possible warning signs of a cyber attack and encouraged to do so, even when it seems likely that no actual attack is involved?

□ Are employees made aware that, even though they are expected to make a serious effort to avoid security lapses, occasional lapses are inevitable and can often be made harmless by prompt reporting?

□ Are employees provided with an easy way of reporting potentially bogus phone calls and other possible efforts to obtain information that might be useful in mounting a cyber attack?

Administrative Actions

□ Does the organization offer a procedure which would allow employees to report attempts by outsiders to extort their cooperation in circumventing security, without having the basis for that extortion widely revealed or made part of that employee's permanent record?

□ Is an effort made to track the current whereabouts of former employees who were deeply acquainted with critical systems and procedures?

Security Incident Handling

□ Do employees know whom they should notify if they are observing symptoms of an apparent cyber attack?

□ Do employees know what additional symptoms or developments should prompt further notifications?

□ Is it standard procedure, in the event of a significant cyber attack, to verify the nature and extent of the attack's effects by direct human communication, rather than relying entirely on automated reports?

□ Are employees with access to highly critical systems or facilities provided with special access codes that would signal that they are acting under duress?

□ Are automated detection systems in place that would raise silent, remote alarms if the duress codes are used?

□ Do the key response personnel know how to collect and preserve the evidence necessary for proper forensic investigations and legal prosecutions?

AREA SIX: SUPPLIERS

Procedures for Developing New Software

□ Does the organization have a system for tracking exactly which employee or outside contributor wrote each line of code for any software produced internally?

□ Are all the programmers working on each software application made aware that records are being kept of exactly who wrote each line of code?

□ Is the use of digital certificates for code-signing of applications under development regularly audited?

□ Does the organization have software vulnerability specialists conduct reviews and tests of the software it has developed, regardless of whether it was outsourced or produced in-house?

□ Do the reviews and tests run on the newly developed software include a search for possible "back doors"?

□ Is stress testing been conducted against the software ports utilized by applications under development to make sure that they are not susceptible to buffer overflows at the software port level?

□ If the application under development is mission critical, is it required to undergo a source code review by an independent third-party**?**

Features to Build into New Software

□ Is the application under development designed to report to a log file all failed log-in attempts and to send an alert if the number of attempts surpasses a specific threshold?

□ Is the application under development designed to report to a log file all attempts to insert executable commands into input files that should not contain such commands?

□ Is the application under development designed to report to a log file all requests to modify permissions and also to send an alert when these modifications are outside normal parameters?

□ Is the application under development designed to report to a log file all cases where data streams from other applications that include characters that are not normal part of such data?

□ Is the application under development designed to report to a log file all cases in which a supplementary file or separate component installed with the program fails an authenticity test?

External Vendors

□ Are the vendors' physical comings and goings inside the organization's facilities logged and monitored?

□ Does the organization scan all laptops that are temporarily connected to the corporate network by outside vendors and contractors to verify that they are free of standard hacking tools?

□ Does the organization have processes established to monitor electronic activities carried out by outside vendors or contractors from *inside* the organization's facilities?

□ Does the organization have processes established to monitor electronic activities carried out by outside vendors or contractors from *outside* the organization's facilities?

□ Are steps regularly taken to verify that access rights for past vendors and contractors were, in fact, eliminated as soon as they were no longer necessary?

□ Are the actions of former vendors or contractors who handled critical information or critical systems monitored for non-compliances with non-disclosure agreements?

Making Effects More Reversible

AREA ONE: HARDWARE

Distributed Electronic Equipment

□ Is there a procedure in place for rapidly determining what sensitive information was being stored on a missing piece of electronic equipment and whether that information was encrypted?

□ If a piece of equipment on the network is identified as having an unknown manufacturer identification (MAC) number, is there way to rapidly locate that equipment and disabled it?

□ Are replacements on hand for the most functionally important servers, desktop computers, laptop computers, and other equipment, in case these are stolen or physically damaged?

□ Are these replacement computers already loaded with properly configured operating systems and applications?

Operations Centers and Data Centers

□ Is there a plan for shifting the more critical activities of each operations center to other computers belonging to the organization if the operations center needs to be evacuated or for some other reason shut down?

□ Is there an understudy system at another location that is being used for something less critical, but is ready to take over the functions of the more critical equipment in the data center?

□ Is the understudy system far enough away from the data center, so that it will not be subject to the same kinds of physical damage from the same causes?

Environmental Systems

□ Are the areas where electronic equipment is housed equipped with a fire suppression system appropriate for electrical equipment?

□ Are there fire suppression systems that can control fire outbreaks in the areas adjoining those that house the electronic equipment?

□ Are there heat and fire barriers between the areas containing electronic equipment and any areas containing or built of flammable materials?

Cables and Wiring Closets

□ Is each extremely critical communication cable backed up by a second communication cable that follows a different route?

□ If the systems are sufficiently critical, are they connected to electric power by two different connection routes?

□ Is there an adequate backup power source for any system critical to the business's overall survivability?

□ Does the backup power source have ample fuel for a fairly long interruption in the fuel supply chain?

□ Is the backup power source regularly tested under a full load and run for long enough periods to verify that everything is in working order?

Physical By-Products (Used Equipment & Paper Printouts)

□ If electronic equipment or paper printouts are recovered from areas where their content could have been accessed by outsiders, is there a clearly defined procedure for determining what actions should be taken to minimize the possible adverse consequences?

AREA TWO: SOFTWARE

Applications and Operating Systems

□ Does the organization maintain an approved master reference copy (i.e., "golden image") for each operating system and suite of applications?

□ Does the organization have information security specialists conduct rigorous vulnerability testing on master reference copies (i.e., "golden images") before approval?

□ Does the organization store approved master reference copies (i.e., "golden images") in a secure repository, which is only accessible from authorized internet protocol addresses and user accounts?

□ Does the organization post hashes of these approved master reference copies (i.e., "golden images"), so that the integrity of these images can be verified?

□ Are there verification and testing procedures for adding software patches to master reference copies (i.e., "golden images")?

□ Are there provisions in place to limit the number of system components that will be affected if a software patch or update fails?

□ Are there procedures in place to restore the system to its last known good state if a software patch or update causes serious problems?

Documents and Data

□ After a data field has been made read only, is there an appropriate procedure for correcting that field under special circumstances and for verifying that correction?

□ Is the database designed so that sensitive information cannot be over-written, without successive, time-stamped revisions being securely archived?

□ Wherever practical, is any authentic information that might be stolen intermixed with bogus information that would cause harm or lead to the possible prosecution of anyone who tries to use it?

□ Are receipts for important e-mails collected and stored to provide a record verifying that they reached the intended recipients?

□ If log files need to be preserved for an extended period of time for legal reasons, are these files stored in a tamper-proof form at more than one physical location?

Identity Authentication Systems

□ Is there a procedure for rapidly and securely changing passwords across the organization if there is any reason to believe they may have been compromised?

□ If an employee needs to recover a password from a remote location, is that employee required to answer a series of challenge questions selected randomly from a database that contains many possible questions?

□ If an employee needs to recover a password from a remote location, is a link to recover or reset the password sent in an e-mail to that employee's regular e-mail account after the employee has successfully answered the challenge questions?

□ Is there a simple automated procedure for rapidly revoking the privileges for tokens and smart cards, if they become compromised?

□ Is there an efficient procedure for replacing tokens and smart cards?

□ Is there a simple automated procedure for revoking the privileges for any biometric identifier that is compromised?

□ Is there an efficient procedure for assigning a new key to someone whose biometric identifier has been compromised, so that person's identifier becomes different?

□ If it becomes necessary, does the organization have a way of accessing data and applications ordinarily protected by personal two-factor authentications, such as biometric authentication?

□ Do the organization and its vendors have a plan for replacing compromised biometric information with alternative information?

AREA THREE: NETWORKS

Permanent Network Connections

□ If the organization detects a manufacturer identification (MAC) number that is exhibiting suspicious activity, is the device quarantined until the suspicious activity is investigated?

□ Do critical systems have redundant communication connections?

□ Do critical systems use redundant domain name system (DNS) servers to lessen the effect due to interruptions of that service from one source?

□ Do any networks that are extremely critical have redundancy in the switching equipment?

Cloud Provider Connections

□ Is special care taken to make sure that the approved master reference copy (i.e., "golden image") for each operating system and suite of applications in the cloud is complete and up-to-date?

□ Are backups of sensitive information that are made by the cloud provider periodically duplicated and stored at a third site, physically separate both from the cloud provider's facilities and from the organization's main facilities?

□ Are copies of cryptographic keys used to encrypt sensitive information at the external provider of cloud computing services stored at a third site, physically separate both from the cloud provider's facilities and from the organization's main facilities?

□ Does the organization have a set of procedures ready for moving all of its cloud operations and data out of the cloud?

□ Does the organization have a set of procedures ready for moving all of its cloud operations and data to another cloud provider?

□ Have the procedures the organization has ready for moving its cloud operations been designed so that its proprietary applications and data will be encrypted during their transmission to a new set of computers?

Intermittent Network Connections

□ Does the organization provide employees with an efficient internal service for removing malware from their laptops and mobile devices if the employee believes that these may have been infected?

□ If an employee's entire laptop hard drive is encrypted, does that employee have a way of conducting essential business if the hard drive cannot be accessed?

Public and E-Commerce Connections

□ Are public-facing websites equipped with anti-tampering software, which will automatically restore each site to its proper condition if an attempt is made to deface it?

□ Is there a plan in place for working with the provider of a social media account to get the account rapidly shut down if it is compromised?

□ Is there a procedure for acting rapidly to get bogus social media posts that pretend to belong to the organization taken down?

□ Is there a procedure for acting rapidly to get bogus websites that pretend to belong to the organization taken down?

□ If the organization's website is defaced, is there a plan in place for getting the defaced copies of the website rapidly removed from the caches of the leading search engines?

□ Is the contact information periodically updated that the organization provides to its domain registrar?

□ Is the contact information periodically updated that the organization provides to the regional internet registrar that maintains its assigned internet protocol (IP) addresses?

Encryption Systems and Digital Certificates

□ Are there regular and reliable procedures for the archiving of private encryption keys and the associated pass phrases for individual users?

□ Are copies of the private keys of digital certificates stored in a password protected and encrypted area that allows recovery and prevents theft?

□ Is there a quick and effective procedure for dealing with compromised encryption keys?

□ Is there a procedure in place that will allow compromised private keys of digital certificates to be rapidly revoked?

□ Are archives of private encryption keys and associated pass phrases keys maintained after they are no longer in active use, so previously encrypted files can be retrieved if necessary?

Firewalls, Intrusion Detection Systems, & Content Filters

□ When restrictions implemented by content filters are relaxed or removed, are these changes automatically archived, so that the content filters could later be restored to their more restrictive condition?

□ If the reviews of the firewall and intrusion detection logs reveal unauthorized traffic, is this traffic immediately investigated to determine what steps might be taken to reduce its possible effects?

AREA FOUR: AUTOMATION

Automated Operations and Processes

□ If communications involving control settings are interrupted, do the controls automatically reset to normal or safe levels?

□ Are highly critical controls accessible by a secure secondary control channel, so that they can still be accessed if the first control channel fails?

□ Are there plans and procedures for dealing with the possibility of critical wireless links being jammed or disrupted?

Peripheral Devices and Physical Equipment

□ If a local device, such as a piece of medical treatment equipment, contains customized settings that are highly important, is there a complete record or backup copy of these customized settings?

Information Backup Devices and Processes

□ Is the data being backed up at a frequency appropriate to its economic value and the rate at which it is being changed?

□ Is there a plan for restoring and reloading the information that has been backed up, as well as for storing it?

□ Are there multiple backups, so that if one is lost or corrupted, the system could still be restored?

□ Are there procedures for dealing with backup data that has become corrupted, especially during a crisis?

□ Are there procedures for dealing with the loss or theft of unencrypted backup tapes that contain proprietary or sensitive information?

□ Is the backup data stored long enough so that there would still be an uncorrupted copy if the data was gradually being corrupted in a hard-to-detect manner over a long period of time?

□ Are crucial backups that have not yet been transferred to a remote location stored and tagged in such a way that they could be easily be taken along in the event of a physical evacuation?

AREA FIVE: HUMAN USERS

Individual Employee Actions

□ Does the organization have a prescribed procedure for collecting forensic evidence on any attempts by employees to use the organization's computer systems for theft of information or to cause other harm?

Administrative Actions

□ If employees with access to competitively important information leave the organization, does the organization check for signs that they are improperly using that information in their new jobs?

Security Incident Handling

□ Does the security team know the names, e-mail addresses, and phone numbers of the people outside the organization that the team may need to contact in order to deal with an attack and its effects?

□ If important information systems are shut down as a result of a cyber attack, is it standard procedure to inform employees immediately how long they should plan on operating without those systems?

□ If the automatic procedures for saving documents and data to remote locations will be disrupted as a result of the attack, are employees warned to save these documents and data locally?

□ If there are other information systems that could substitute for the systems that have been shut down or made unreliable as a result of the attack, do employees know how to switch over to them?

□ Do employees know how to go about restoring compromised information systems to their last known good state?

□ Is there a mechanism for retrieving "last known good state" when that state is a considerable time into the past?

□ Are employees trained to handle storage media and by-products securely in the special circumstances produced by disaster recovery?

□ If a potential cyber attack would affect people outside the organization, is the organization's publicity and public relations department prepared to deal with this?

□ If the organization is supplying urgently needed services to regular customers, is there an ordered list of which customers are the highest priority for the restoration of services?

AREA SIX: SUPPLIERS

Procedures for Developing New Software

□ Are annotations maintained on each section code as it is being written, so that other developers and security specialists can rapidly understand what a given section is designed to do?

□ Are successive versions of software under development archived, so that it will be possible to return to a last known good version, even if corrupt code was inserted and went undetected for a considerable period of time?

Features to Build into New Software

□ Is the application under development designed to automatically reinstall supplementary files and separate components from a trusted repository if the authenticity of the current ones cannot be verified?

□ Is the application under development designed to place special items (terminator canaries) in its buffer areas that will trigger an alarm if they are overwritten?

External Vendors

□ Are software vendors required to make escrow arrangements for the preservation and protection of the source code used in the applications being purchased or licensed?

II. ORGANIZED BY INFORMATION SYSTEM COMPONENTS

Area One: Hardware

DISTRIBUTED ELECTRONIC EQUIPMENT

Overview

□ Does the organization maintain an accurate inventory of the electronic equipment housed in each room at each physical location?

□ Does the inventory of electronic equipment include all the memory devices allowed inside the organization's facilities, such as external hard drives, CD's, magnetic tapes, flash drives, zip disks, and other removable media?

□ Are employees required to leave all personal electronic devices with memories outside the organization's facilities, except those explicitly allowed by the organization?

□ Is there a quick and easy procedure for updating the electronic equipment inventory, whenever an employee with responsibility for a piece of equipment authorizes it to be moved?

□ Is the inventory of electronic equipment for each facility unit actually updated whenever a piece of new equipment is added or removed for disposal or recycling?

□ Are the electronic equipment inventories and records included in the organization's annual audits?

Harder to Find

□ Are the locations of areas handling sensitive information processes left off of building directories?

□ Are the locations of areas handling sensitive information processes omitted from public tours and are the employees providing those tours warned not to mention them or answer questions about them?

□ Are employees explicitly prohibited from publicly posting photos of all activities in areas handling sensitive information processes?

Harder to Penetrate

Identification Badges

□ Are all employees required to wear personal photo ID badges, issued by the organization?

□ Are all visitors or vendors required to wear temporary photo ID badges, issued by the organization?

□ Are the photo ID badges designed to facilitate introductions and communication between personnel, rather than just used for security?

□ If the photo ID badges can be worn on cords, are they printed the same way on both sides, so that it won't matter which way a badge is facing?

□ Are the lettering and photo on the photo ID badge printed large enough and clearly enough so that they can be easily checked without being inspected up close?

□ Are the temporary photo ID badges color coded by date, so that it will be immediately apparent if a visitor or vendor is wearing a badge that has expired?

Physical Access Privileges

□ Are there strict controls on who goes in and out of the larger physical facilities in which the information systems operate?

□ Are there further controls preventing employees from entering the rooms and areas handling highly sensitive information, unless those employees have a need to be in those specific areas?

□ Is the time and exact place at which anyone enters or exits a physical facility automatically logged?

□ Is there a physical access list that a person's name must be on before he or she is admitted to a physical facility?

□ Does the access list for a physical facility also list the person who authorized each name on that list?

□ If the facility is a highly sensitive one, is the employee who authorized a name to be added to the physical access list asked to personally verify that authorization before the person is actually admitted?

□ Does every name on the physical access list have an expiry date on which the physical access privilege would need to be renewed?

□ Is there an access authorizer list, consisting of those who have the authority to add names to the physical access list?

□ When someone attempts to add a name to a physical access list, is the access authorizer list automatically checked to verify that the person adding the name is authorized to do so?

□ Does adding a name to the access authorizer list require at least two people whose names are already on this list?

□ Are both the access authorizer list and the physical access list regularly reviewed to see whether there are names that can be removed from these lists?

□ Are the physical access privileges for each employee changed when an employee's work role changes?

□ Are physical access privileges and devices such as badges immediately deactivated when an employee is terminated, leaves, or retires?

□ Are physical access privileges and devices for vendors frequently reviewed and promptly deactivated when there are changes in the status of vendor personnel?

Physical Equipment Features

□ Are there physical barriers, such as secure covers or plugs, put in place to disable any networked computers' unused media access ports, such as USB sockets and CD drives?

□ Are the connections where cables are plugged into networked computers secured with tamper-proof seals, so that it will be immediately apparent if a cable was unplugged without authorization?

□ Are unused access ports on network switches, especially the Switched Port Analyzer (SPAN) ports, turned off to prevent unauthorized access?

□ Are unused network access ports in the organization's facilities turned off in the network switches to prevent unauthorized access?

□ Is root level access disabled on routers and switches, so that attempts to gain unauthorized access during a reboot are prevented?

□ Is all physical access to the console interfaces of security appliances, such as those used to manage firewalls, intrusion prevention, and intrusion detection systems restricted to authorized users?

□ Are fax machines that receive and print sensitive information protected against unauthorized physical access?

Harder to Co-opt

□ Is there an explicit policy specifying what kinds of equipment can be taken off the corporate premises and what authorizations are required to remove that equipment?

□ If external hard drives and other storage devices that contain sensitive information would be easy to carry off, are they anchored down as an extra security precaution?

□ If authorized flash drives are used inside the organization's facilities, are these given a distinctive color and unique number that makes them easy to identify and trace?

□ Are employees required to declare and display any memory devices, such as flash drives, that they are carrying when they leave the organization's facilities?

□ If an employee is found leaving the facility with an unauthorized memory device, is the employee asked to submit that device for investigation, along with its access codes?

Harder to Conceal

Physical Access Privileges

□ Are any changes in the lists of employees who are allowed access to highly sensitive areas promptly reviewed to make sure these changes are authorized and reasonable?

□ Are the people who authorize physical access asked, at random intervals, to verify that they did indeed authorize the physical entries that they are recorded as having authorized?

□ If employees use their identification badges or other authentication to enter sensitive areas, are both their entrances into and exits from these areas logged, with the exact times noted?

□ Are the logs of the times employees spend in sensitive areas regularly reviewed to see whether these times are consistent with the employee's work responsibilities?

□ Are the logs of the times employees spend in sensitive areas regularly reviewed to see whether these correspond to times when the employee was also recorded as being present in the larger facility?

□ If there is an unexplained discrepancy between the logs recording employees' times spent in sensitive areas and their work responsibilities or other logs of their movements, are these discrepancies investigated in a timely fashion?

□ Is video surveillance used to monitor access to areas where critical information processing equipment is located outside of data centers?

□ If security cameras, especially wireless ones, are used for monitoring, are they protected from jamming, unauthorized viewing, and the spoofing of images?

Physical Equipment

□ Is each piece of electronic equipment labeled with a barcode or other identifier for easy tracking?

□ If electronic equipment needs to be taken off the corporate premises, is there an efficient procedure for tracking the movement of that equipment?

□ Are authorized flash drives and other memory devices tagged with radio frequency identification (RFID) chips, so that their movements can be traced almost in real time?

□ Are people leaving the organization's facilities electronically scanned for radio frequency identification (RFID) chips or other signs that they removing electronic equipment from the facility without authorization?

□ Are unannounced spot checks periodically carried out to verify that the electronic equipment is present at the locations designated in the equipment inventory?

□ Is there a system for electronically verifying that the right pieces of equipment, identified by manufacturer identification (MAC) number, are plugged into the right locations, identified by IP address?

□ If there are discrepancies between the inventory of electronic equipment and the equipment actually found in the corresponding facility unit or room, are these discrepancies immediately investigated?

□ Where the physical media access ports are regularly used and, hence, not disabled, are there procedures to electronically monitor for unauthorized access of these ports?

□ If employees observe personal, unauthorized electronic devices, including flash drives, being used inside the organization's facilities, is there an easy-to-use, private channel for reporting this and an incentive to do so?

More Reversible

□ Is there a procedure in place for rapidly determining what sensitive information was being stored on a missing piece of electronic equipment and whether that information was encrypted?

□ If a piece of equipment on the network is identified as having an unknown manufacturer identification (MAC) number, is there way to rapidly locate that equipment and disabled it?

□ Are replacements on hand for the most functionally important servers, desktop computers, laptop computers, and other equipment, in case these are stolen or physically damaged?

□ Are these replacement computers already loaded with properly configured operating systems and applications?

OPERATIONS CENTERS AND DATA CENTERS

Overview

□ Are important operational centers where the activities consist almost entirely of monitoring screens and working at terminals organized into separate physical units?

□ Are especially important pieces of electronic equipment consolidated into data centers for easier protection?

□ Is there an inventory and schematic plan of the data center equipment that is immediately updated each time a change is made in the equipment or in the way it is connected?

Harder to Find

□ If an operations center carries out highly critical activities and does not need to have many visitors, apart from those who work there, is the operations center left off of building directories?

□ Is the location of the data center left off of building directories?

□ Is the data center omitted from public tours and are the employees providing the tours warned not to mention it or answer questions about it?

□ Are those overseeing the organization's public facing website instructed to make sure that no mentions of the data center or operations centers are posted online?

□ Are employees explicitly prohibited from posting pictures of all activities in the operations centers and data center?

□ Are the doors to the data center marked in a way that does not reveal that they lead to the data center?

Harder to Penetrate

□ Are there walls or other physical barriers separating the operations center from other physical areas**?**

□ Does access to the operations center require a scannable badge, smart card, proximity card, biometric reading, or a lock requiring a personal combination?

□ Is the level of authentication required to enter the operations center adjusted to the criticality of the activities carried out there?

□ Are there physical security barriers established to protect electronic equipment in the data center from theft, malicious damage, or direct electronic access?

□ Are the walls of the data center painted with radio-wave scattering paint?

□ Are any drop ceilings or raised floors in the data center and other areas that house critical information equipment secured against access from adjacent spaces and ventilation systems?

□ Are the doors of the data center kept securely locked at all times for inbound traffic?

□ Are "restricted area" signs posted just inside the doors into the data center where anyone entering would see them?

□ Is access to the data center strictly controlled using technologies such as scannable badges, smart cards, proximity cards, biometrics, or locks requiring personal combinations?

□ Is the identify of the person entering the data center confirmed by means of a second factor, such as a password, personal identification number, or a second biometric feature?

□ Are there clear and rigorously enforced restrictions on which employees have access to the data center?

□ Are there strict controls on vendor access to the data center, so that only properly authorized vendor personnel are admitted?

□ Does the data center have a sign-in procedure that is used to log non-employees into the restricted area?

□ Are building maintenance personnel, such as janitors, prevented from entering the data center unless directly supervised by trusted personnel?

□ Are systems in place to allow very rapid access to the data center in the event of a fire?

□ If the data center needs to be quickly accessed in the event of a fire, is there a plan in place for immediately resecuring the data center's electronic equipment, as soon as it is safe to do so?

□ Are systems in place to allow access to the data center in cases, such as flooding or controlled facility evacuation, when equipment might need to be moved on short notice?

Harder to Co-opt

□ Is all critical electronic equipment inside the data center physically locked in place?

□ If a piece of electronic equipment is extremely critical, is there an alarm that would warn when the rack space holding it has been unlocked, if that alarm hasn't been deactivated first?

□ Are there locking devices on empty rack spaces, so that unauthorized units cannot be easily added?

Harder to Conceal

□ Are all activities inside the operations center clearly visible through large windows or on large video screens that are in easy view of other employees (but not casual visitors)?

□ Are personnel leaving the data center registered as doing so by an automatic system or by actively scanning their identification device?

□ Is each instance when someone enters or leaves the data center automatically reported to a remote location and securely logged?

□ Is the data center equipped with an intrusion alarm that would be triggered by signs of activity there when no one with authorized access is known to be inside?

□ Is the intrusion alarm for the data center monitored offsite?

□ Is video surveillance used to monitor access routes to the data centers?

□ If there is video surveillance of the data center, is it monitored off-site?

□ If there is video surveillance of the data center, is the video recorded in a permanent medium that prevents tampering?

□ If there is video surveillance of the data center, are the video recordings retained long enough so that they would still be available to investigate a security breach that wasn't detected for several months?

□ If employees observe unauthorized activities going on inside the data center, such as unauthorized personnel entering or equipment being moved without proper authorization and documentation, is there an easy-to-use, private channel for reporting this and an incentive to do so?

□ Are the logs for the data center's access control mechanisms (e.g., key cards and video surveillance logs) reviewed on a regular basis?

□ Does the review of the data center's physical access records include an analysis of failed physical access attempts?

□ If there are indicators of suspicious activity involving access to the data center or behavior inside it, are these cases investigated in a timely manner?

More Reversible

□ Is there a plan for shifting the more critical activities of each operations center to other computers belonging to the organization if the operations center needs to be evacuated or for some other reason shut down?

□ Is there an understudy system at another location that is being used for something less critical, but is ready to take over the functions of the more critical equipment in the data center?

□ Is the understudy system far enough away from the data center, so that it will not be subject to the same kinds of physical damage from the same causes?

ENVIRONMENTAL SYSTEMS

Overview

□ Is there a readily accessible document that lists the locations and types of all local environmental control devices, such as thermostats and water leak detection systems?

□ Is there a readily accessible document that lists the locations and types of any supervisory environmental control devices?

□ Is there an up-to-date document listing the temperature ranges and other environmental requirements for the organization's various types of electronic equipment to operate without damage?

Harder to Find

□ Are any outside contractors who support or manage the organization's environmental systems contractually prevented from advertising or publicizing the fact that the organization is a customer?

□ Are the environmental controls, other than local thermostats, for the areas with electronic equipment located behind panels or doors and not easy to identify?

□ Are the exterior air conditioner or cooling fans for facilities housing critical electronic equipment hidden from view and away from public areas?

Harder to Penetrate

□ Are the panels or doors protecting the controls for the electronic equipment's physical environment kept locked?

□ Is there a secure delivery and loading area, physically separated from the data center, so that the addition or replacement of equipment doesn't provide an avenue for improper access or explosive devices?

□ Are pieces of electronic equipment and other supplies physically inspected before being moved into the data center, in order to make sure that they haven't been tampered with?

□ Is critical computer or communication equipment that could be a target for terrorists kept away from ordinary windows, which could provide a channel for thrown or projectile bombs, gunfire, or microwave weaponry?

□ Are the critical computer and communication facilities that could be a target for terrorists located a sufficient distance from public parking places, streets, and other locations where a bomb could be easily detonated?

□ If the electronic systems are sufficiently critical and represent sufficiently high-profile targets, are they surrounded by the sort of metal shielding that would protect against electro-magnetic pulse attacks?

□ Are the critical computer and communication facilities a sufficient distance from any permanent facilities that would be particularly susceptible to fire, explosions, or hazardous leakages?

Harder to Co-opt

□ Do environmental controls exist, such as automatic heating and cooling systems, which can maintain a consistent operating temperature for the electronic equipment?

□ Do environmental controls exist that can keep the humidity in the areas housing electronic equipment within an acceptable range?

□ Do environmental controls exist that can protect the system from elements other than temperature and humidity, such as smoke, dust, and corrosive fumes?

Harder to Conceal

□ Are the environmental control consoles in locations monitored by video cameras?

□ Are there an independent set of sensors for temperature, smoke, and moisture in the data center and wiring closets that would warn when a hazardous condition develops, even if the normal environmental control systems are not registering a problem?

□ Is there an alarm, including both sound and light, that will be automatically triggered if the conditions in the physical environment become dangerous for people or for the electronic equipment?

□ If the dangerous conditions involve fire, will firefighters and other first responders automatically be summoned?

More Reversible

□ Are the areas where electronic equipment is housed equipped with a fire suppression system appropriate for electrical equipment?

□ Are there fire suppression systems that can control fire outbreaks in the areas adjoining those that house the electronic equipment?

□ Are there heat and fire barriers between the areas containing electronic equipment and any areas containing or built of flammable materials?

CABLES AND WIRING CLOSETS

Overview

□ Is there a floor plan or geographical map that shows exactly where the communication cables have been laid?

□ Is there a floor plan or geographical map that shows exactly where the electric power cables have been laid?

□ Are the layout and capacities of the electric power supply well-documented?

□ Are all documents diagramming communication cable routes rigorously protected from unauthorized access?

□ Have all communication cables and equipment been physically labeled and color coded inside the wiring closets and at other locations where they might need to be reconfigured?

□ Are there labels for equipment on both the front and rear of the equipment housings, to reduce the risk of equipment being improperly reconfigured or turned-off?

□ Does the organization investigate the physical security practices of internet service providers and other communication companies before choosing which companies to buy services from?

□ Are the projected electric power needs of the electronic equipment well-documented, with reliable estimates of peak needs as well as normal needs?

Harder to Find

□ Are the most critical communication cables installed in such a way that their locations and routes are not obvious?

□ Are labels on electronic equipment worded in such a way that their meaning is not immediately obvious to an outsider?

□ Are the connecting power cables that are farther away from the data center installed in such a way that they are not easy for unauthorized personnel to identify and access?

Harder to Penetrate

Wiring Closets

□ Are wiring closets securely locked at all times?

□ Is there a list of which employees and contractors are allowed physical access to the wiring closets?

□ Is the list of employees and contractors who are allowed access to the wiring closets regularly updated to take account of what work needs to be done and who is assigned to do it?

□ Are the employees and contractors who are allowed to access the wiring closets required to sign out the relevant keys, tokens, or access codes each time they will need to use this physical access?

□ Are the times at which the keys, tokens, or access codes for the wiring closets are signed out, used, and signed in securely logged, along with the identities of those using them?

□ Are the keys, tokens, or access codes for the wiring closets changed on a schedule appropriate to the sensitivity and criticality of the equipment and cables in those wiring closets?

Communication Cables

□ Are physical security barriers established to protect the communication cables running to and from the system, so that they cannot be easily severed or damaged?

□ Are the critical communication cables and cable harnesses inside the organization's facilities laid out in a way that makes it difficult to access them physically for the purpose of intercepting transmissions?

□ Is there physical protection at the demarc point where telephone and data cables enter the building?

Electric Power

□ Have physical security barriers been established to protect the connecting power cables in the vicinity of the data center, so that they cannot be easily severed or damaged?

□ Are electrical supply components, such as power panels and breaker boxes, protected from unauthorized access?

□ If uninterrupted power supplies (UPS's) are being utilized, are these protected from authorized remote access?

□ Are backup power sources protected with security devices, such as locks, alarms, and reasonably secure fences?

□ Are backup power sources for facilities that could be a target for terrorists a sufficient distance from public parking places, streets, and other locations where a bomb could be easily detonated?

□ Are backup power sources in locations that are not susceptible to flooding?

Harder to Co-opt

□ If communication cables pass through areas that are publicly accessible, but difficult to monitor, are these cables sheathed in a manner that makes them difficult to cut or tap?

□ Are there alarms that would warn if communication cables have been cut?

□ Are emergency power shut-off switches conspicuously labeled and covered by safety panels to prevent the electric power from being inappropriately interrupted?

□ Is there protection against extreme power surges of the sort that could be produced by lightning or, possibly, by artificial means?

Harder to Conceal

□ Are the wiring closets equipped with intrusion alarms?

□ Is access to the wiring closets monitored by video cameras?

□ Are the intrusion alarms for the wiring closets monitored offsite?

□ Are the logs recording when the keys, tokens, or access codes for the wiring closets are signed out, used, and signed in regularly reviewed to make sure that the access periods correspond to the work that needed to be done?

□ Are there video cameras inside the larger wiring closets that are activated by motion sensors?

□ Are emergency power shut-off switches in locations monitored by video cameras?

More Reversible

□ Is each extremely critical communication cable backed up by a second communication cable that follows a different route?

□ If the systems are sufficiently critical, are they connected to electric power by two different connection routes?

□ Is there an adequate backup power source for any system critical to the business's overall survivability?

□ Does the backup power source have ample fuel for a fairly long interruption in the fuel supply chain?

□ Is the backup power source regularly tested under a full load and run for long enough periods to verify that everything is in working order?

PHYSICAL BY-PRODUCTS (USED EQUIPMENT & PAPER PRINTOUTS)

Overview

Electronic Equipment

□ Has the organization defined the procedures for the thorough wiping or secure destruction of each type of memory device?

□ Is there a list of the memory devices scheduled for destruction or recycling that shows the exact location of these items at each point in their processing?

□ Is a rigorous chain of custody maintained for memory devices being processed, transported, or sent for disposal?

□ Is the list of memory devices scheduled for destruction or recycling updated each time any of these devices are moved to a new location, wiped, or put through another process?

□ When the memory devices are removed from the room or area where they were in regular use, is the inventory of the electronic equipment in that room immediately updated?

□ Does the organization supply employees with locked collection boxes for the secure disposal of used cell phones and other electronic devices with memories?

□ Are the electronic devices collected for disposal from the deposit boxes properly inventoried and inserted into the regular process for wiping and secure destruction?

Paper Printouts

□ If a document is highly sensitive, is a record kept of each time it is printed or copied, how many copies are made, and by whom?

□ If a document is highly sensitive, is each copy labeled with a unique number?

□ If a document is highly sensitive, is a chain-of-custody record maintained, so that each person who takes possession of a copy must sign for it, and so that the date and time of the transfer is recorded?

□ If a document is highly sensitive, is the chain-of-custody maintained until the document is destroyed or its period of sensitivity expires?

Harder to Find

□ Do the labels on equipment being sent for thorough wiping or secure destruction avoid revealing what departments they are from?

Harder to Penetrate

Electronic Equipment

□ Are there sufficiently rigorous policies and procedures governing the use of removable storage media, such as flash drives and CD's, so that all of these devices are kept under the organization's control?

□ Is equipment marked for recycling kept in secure locations, at least until it has been thoroughly wiped?

□ Are there sufficiently rigorous procedures for properly shipping any removable data storage devices that need to be moved to offsite locations?

Paper Printouts

□ Are there sufficiently rigorous procedures to restrict unauthorized access to paper printouts that contain sensitive information?

□ Do corporate security policies require secure storage containers to hold paper printouts that contain sensitive information and are destined for destruction?

Harder to Co-opt

Electronic Equipment

□ Are there regular procedures to make sure that memory media, such as hard drives, tapes, and flash drives, are thoroughly wiped before they are reassigned to different business uses?

□ Are there sufficiently rigorous procedures to make sure memory media are thoroughly wiped before being returned for warranty replacement, publicly sold, or donated for charitable use?

□ Are the inventory labels, such as barcodes, radio frequency identification (RFID) chips, and other identifying tags removed from the equipment being destroyed or recycled, during the last stage of this process?

□ Are used CD's containing sensitive information properly destroyed (not just broken) prior to disposal?

Paper Printouts

□ Is there a rigorous plan for keeping paper printouts containing sensitive information separate from other printed materials?

□ Are documents that contain sensitive information protected from printing if there is no operational need for those documents to be printed?

□ If extremely sensitive documents need to be printed, is there a procedure in place to make sure these documents can only be printed on a supervised printer?

□ After extremely sensitive documents are printed on a supervised printer, is a physically documented chain of custody established, so that there is a designated person responsible for the security of those documents at all times?

□ Are there sufficiently rigorous procedures for the secure destruction of paper printouts by shredding or burning?

□ When extremely sensitive documents need to be destroyed, is a second person required to be physically present and to verify their destruction, before the chain of custody can be ended?

□ Has care been taken to make sure that any paper reuse and recycling programs do not undermine the secure handling of paper printouts?

Harder to Conceal

Electronic Equipment

□ Are the occasions when memory devices are removed for destruction or recycling used as an opportunity to verify that the inventory of electronic equipment in that room or area corresponds to the electronic equipment that can actually be found in that room or area?

□ Is the thorough wiping or secure destruction of each memory device regularly attested by two parties?

□ Are the records documenting the thorough wiping or secure destruction of each memory device themselves securely stored in a tamper-proof format?

Paper Printouts

□ If a document is highly sensitive, is it only printed or copied onto paper that has a distinctive shade or color, so that employees will be able to tell if it turns up in a context where it doesn't belong?

□ Are the locations where paper printouts containing sensitive information are stored prior to their secure destruction subject to video surveillance?

□ Is the actual process by which paper printouts containing sensitive information are physically destroyed subject to video surveillance?

More Reversible

□ If electronic equipment or paper printouts are recovered from areas where their content could have been accessed by outsiders, is there a clearly defined procedure for determining what actions should be taken to minimize the possible adverse consequences?

Area Two: Software

APPLICATIONS AND OPERATING SYSTEMS

Overview

□ Does the organization maintain an up-to-date inventory of all the software applications that are installed in its systems?

□ Does the organization have a policy of limiting each employee's use of software applications to those that the employee actually needs to carry out his or her work?

□ Has the organization formally assigned criticality classifications to its more important or more widely used software applications? (E.g., is a software application that controls a specialized process that is highly dangerous easy to distinguish from one that controls a commonplace process that cannot easily be used to do harm?)

□ Is there a procedure for documenting and tracking which application privileges are active for each individual employee?

□ Does the organization maintain a comprehensive list of all the applications that require an administrative level account to perform operations?

□ Does the organization maintain a comprehensive list of all scripts that use embedded credentials to perform operations?

□ Is there a system for tracking software patches and updates that logs the news that those patches or updates are needed, the announced release dates for those patches or updates, the dates on which those patches or updates are actually received, and the dates on which they are applied?

Harder to Find

□ Does the organization take steps to prevent the public release of information about which software applications it is running, whenever these applications are unusual or associated with special processes?

□ Are employees and former employees contractually obligated to keep information on their cv's about what software applications they have mastered generic, rather than listing the specific applications?

□ Are administrator accounts renamed, so that it is not easy to identify them as administrator accounts?

□ Are service accounts (e.g., backupserver, sp_content) renamed, so that it is not easy to identify them as special accounts linked to specific applications?

Harder to Penetrate

□ Does the organization have information security specialists conduct rigorous vulnerability testing on applications before they are deployed?

□ Are the vendor's default security settings changed on software applications before those applications are put into operation?

□ Are the vendor's default passwords and default log-in names changed on software applications before those applications are put into operation?

□ Are passwords for service accounts (e.g., backupserver, sp_content) extremely complex in their character sets and length?

□ Are the boot sequences on the organization's computers set so that the computers cannot be booted from external media, such as USB drives or CD's?

□ Is each type and level of application privilege assigned an appropriate type and level of authentication mechanism? (E.g., do administrator privileges require a more secure log-in mechanism than ordinary privileges?)

□ Is there a documented procedure for removing and verifying the removal of application privileges when these are no longer needed?

□ Before a patch or update is actually deployed, does the security team verify that the patch or update was announced on the vendor's website or that a notification to expect it was received from the vendor?

Harder to Co-opt

Privilege Allocation

□ Is access to critical applications restricted to those users within the organization who actually need to use those applications?

□ Are the employees asked to provide lists of what software applications they need to access, so that these can be used as the basis for assigning them application privileges?

□ Are the employees' lists of the software applications they need to access reviewed before these application privileges are actually granted?

□ If an employee goes for many weeks without using a particular software application, is this application automatically removed from that employee's application privileges?

□ Are the software application privileges for individual employees reviewed and revised whenever there is a substantial change in their work assignments?

□ Is there an annual review of the application privileges for each employee, even if there has been no change in that employee's work assignments?

□ Are root-level and domain administrator privileges restricted to those who actually have need for those privileges?

□ If employees are given root-level or domain administrator privileges, is their need for those privileges reviewed at least semi-annually?

□ Are administrator privileges on individual computers normally kept turned off in order to prevent unauthorized software applications from being installed?

Application Usage

□ Are the relevant people within the organization alerted to any new software or hardware vulnerabilities, so that they can take protective and compensating

measures to cover the period between the time those vulnerabilities were discovered and the time a relevant patch or update is installed?

□ Have the error messages been properly adjusted or designed, so that they do not reveal information about the internal design and configuration of the software?

□ Have the debugging features been disabled that would provide an avenue for obtaining information about the internal design and configuration of the software?

Patches and Updates

□ Are software patches and updates of critical systems tested prior to installation to minimize the risks of malfunctions?

□ Are the installation times for software patches and update chosen to minimize the disruption of operations?

□ Does the choice of times for the installation of software patches and updates take account of the fact that these installations might cause problems that will shut down the systems until troubleshooters can clear up the problems?

Harder to Conceal

□ Is every computer belonging to the organization regularly scanned for malware and hacking tools?

□ Are all increases in application privileges logged and reviewed?

□ Are any grants of root-level or domain administrator privileges immediately reviewed to confirm that they were necessary for operational purposes?

□ Does the periodic review of root-level or domain administrator privileges include verification that these privileges were being used correctly?

□ Are security settings and configurations automatically rechecked after patches and upgrades have been installed to make sure that they have not been inadvertently reset to less secure or default settings?

□ Is there a regular procedure to verify that the software patches and updates that were being tracked were indeed installed in a timely and orderly manner?

□ Does the organization have information security specialists conduct regular vulnerability testing on applications after they are deployed?

□ If applications are more critical, is the vulnerability testing of these applications carried out more often?

More Reversible

□ Does the organization maintain an approved master reference copy (i.e., "golden image") for each operating system and suite of applications?

□ Does the organization have information security specialists conduct rigorous vulnerability testing on master reference copies (i.e., "golden images") before approval?

□ Does the organization store approved master reference copies (i.e., "golden images") in a secure repository, which is only accessible from authorized internet protocol addresses and user accounts?

□ Does the organization post hashes of these approved master reference copies (i.e., "golden images"), so that the integrity of these images can be verified?

□ Are there verification and testing procedures for adding software patches to master reference copies (i.e., "golden images")?

□ Are there provisions in place to limit the number of system components that will be affected if a software patch or update fails?

□ Are there procedures in place to restore the system to its last known good state if a software patch or update causes serious problems?

DOCUMENTS AND DATA

Overview

□ Is information generally disseminated throughout the organization on a need-to-know basis?

□ Do these need-to-know restrictions take account of the need for cross-disciplinary information sharing and the importance of employees' understanding the reasons for what they are doing?

□ Has the organization formally assigned sensitivity classifications to its information files?

□ Are the sensitivity classifications that the organization employs designed to provide a good basis for encryption policies?

□ Are the sensitivity classifications that the organization employs periodically reviewed to make sure that they are not excessively restrictive, encumbering corporate activities with necessary precautions, or insufficiently restrictive, exposing corporate activities to losses and harm?

□ Does the organization avoid storing types of data that could create liabilities, but do not serve any important business or government function? (E.g., does the organization erase credit card numbers as soon as the transactions using those numbers have been successfully processed, if the customers are going to be asked to enter these numbers again when making future purchases?)

□ Is access to genuinely sensitive data restricted to those users within the organization who actually need to use that data?

Harder to Find

□ Are critical files labeled in a way that does not reveal their contents?

□ Are the table and column labels in databases named in a way that does not reveal which ones contain sensitive information?

□ Are bogus files mixed in with the real ones, so that it would be difficult for an attacker to know which are the real ones?

Harder to Penetrate

□ Are all input fields for data restricted to an appropriate minimum and maximum length? (E.g., a Social Security Number field should only allow nine numerals.)

□ Are all input fields for data restricted to the appropriate characters and expressions? (E.g., a Social Security Number field should not allow anything but numerals and dashes.)

□ Are there limitations on the data fields for the database that correspond to the limitations in the fields on the user interface, so that improper data are not inserted directly into the database?

□ Are the service ports for critical applications configured to filter out data that is outside the proper operating parameters for those applications?

□ Are the limitations on what can be written into the input fields made sufficiently restrictive, wherever possible, so that those fields will not accept executable instructions?

□ Are all documents and data files classified at the higher sensitivity level stored in an encrypted form when not in use?

□ Are valid users required to provide additional passwords or other information to access highly sensitive documents and data?

Harder to Co-opt

General Data Access

□ Is there an automatic mechanism that can quarantine systems which may have been contaminated with false information, without shutting them down?

Data Inputs or Changes

□ Is the ability to alter or input data into documents or databases restricted to those employees who would have a valid need to do so in the course of their normal work?

□ Are data fields that would rarely need to be changed made read-only as soon as the data entry is verified as correct?

□ Are documents that present the organization's work or positions converted into formats that cannot be easily modified, before they are circulated electronically outside the organization?

□ When documents are converted into formats that cannot be easily modified, are those documents digitally signed to make them even harder to falsify?

□ Are the digital signatures on important documents routinely checked to verify their source before those documents are accepted and utilized?

□ Are critically important e-mails sent using an application that hashes their contents, so that the e-mails' contents cannot easily be falsified?

□ Are critically important e-mails sent using an application that adds a digital signature, so that their sender's identity cannot easily be falsified?

Data Exports

□ Is a valid user prevented from improperly uploading or downloading sensitive data files from the system to another system?

□ Is the ability to produce outputs of sensitive information, such as printed versions and e-mail attachments, restricted to what the user's job and responsibilities would require?

□ Are employees prevented from saving sensitive information to local storage devices, such as CD's, DVD's, or USB drives, except in cases where business needs require this?

□ Is there an automatic limitation on the amount of data that can be downloaded at any one time from any file repository or database containing sensitive information?

□ Are pieces of information that an attacker would want to use together kept in different files that need to be accessed in different ways? (E.g., are customers' Social Security Numbers stored in a file that is different from and is accessed differently than the file containing their account numbers and passwords?)

Harder to Conceal

General Data Access

□ Is there an alarm mechanism that warns if files are being accessed in unusual quantities or in sequences that are not consistent with normal work patterns?

□ Are "normal work patterns" specified using descriptions by employees of what work patterns would make sense, rather than relying exclusively on the patterns that would be detected by an unassisted software program?

□ Is there an alarm mechanism that warns if files are being accessed at unusual hours of the day or night, when computers could carry out unauthorized processes unobserved?

□ Are false "honeypot" files employed to detect unauthorized explorations of the organization's documents or data?

□ Is there an alarm mechanism that warns if unusual database commands are suddenly being used?

Data Inputs or Changes

□ Is there an automatic process for monitoring systems for symptoms that false information may have been inserted?

□ If there is reason to believe an attacker could benefit greatly from altering a body of data, is that data associated with a hash that would reveal if the data has been altered?

□ Is there a mechanism for monitoring and logging all changes to critical databases?

□ Are all uploads of sensitive data files monitored and logged?

□ Are all uploads of encrypted data files monitored and logged?

□ Is there an alarm mechanism that warns if data is apparently being entered by employees in quantities or with distributions that are not consistent with those employees' normal work patterns?

□ If logging of data change has been implemented, is the log regularly analyzed for any unusual alteration patterns in databases?

□ Is the log of changes made to critical databases regularly analyzed for unusual access patterns, including unusual access times and frequencies?

□ Is there any provision for detecting situations in which bogus data or instructions are being inserted without detectable intrusions?

□ Is there any provision for detecting situations in which there are unusual patterns of alteration in databases, even when there might not have been any unusual access patterns?

Data Exports

□ If employees can save sensitive information to a local memory device, is this action monitored and logged?

□ Does the organization tag highly sensitive documents with digital watermarks, so that content filters can more easily identify them if an effort is made to export them?

□ Does the organization embed beacons in highly sensitive documents that will contact the document's source if those documents are opened by a user on a device connected to the internet?

More Reversible

□ After a data field has been made read only, is there an appropriate procedure for correcting that field under special circumstances and for verifying that correction?

□ Is the database designed so that sensitive information cannot be over-written, without successive, time-stamped revisions being securely archived?

□ Wherever practical, is any authentic information that might be stolen intermixed with bogus information that would cause harm or lead to the possible prosecution of anyone who tries to use it?

□ Are receipts for important e-mails collected and stored to provide a record verifying that they reached the intended recipients?

□ If log files need to be preserved for an extended period of time for legal reasons, are these files stored in a tamper-proof form at more than one physical location?

IDENTITY AUTHENTICATION SYSTEMS

Overview

□ Do corporate security policies outline the activation of passwords and other authentication credentials when an employee is hired?

□ Do corporate security policies outline the activation of passwords and other authentication credentials used for root-level or administrator-level operations?

□ Do corporate security policies mandate the immediate deactivation of passwords and other authentication credentials when an employee is terminated, leaves, or retires?

Harder to Find

□ Are employees' log-in names different from their given names and e-mail addresses?

□ Are employees assigned log-in names that cannot be easily deduced?

□ If a database of challenge questions is being set up, is care taken to avoid any questions about employee's lives that could be readily answered by web research?

□ If a database of challenge questions is being set up, are employees given an opportunity to add their own questions, so that the answers would be too private to discover by web research?

□ If a database of challenge questions is being set up, are a large number of questions and answers created for each employee, so that it would difficult to collect enough information on the employee to be able to answer several randomly chosen questions?

Harder to Penetrate

Authentication Policies

□ Are all corporate information systems protected with basic authentication mechanisms, such as log-in name and password?

□ Are log-in attempts limited to a certain number per minute (rather than a certain number altogether)?

□ Is the rate at which log-in's can be attempted automatically slowed further after multiple failed attempts?

□ If the log-in process is regularly under attack, is there a queuing system that would allow someone trying to properly access the system to get a turn at logging into it?

□ If an account is accessed only after a considerable number of failed log-in attempts, is that account then monitored for improper use?

□ Is there a simple automated procedure for cancelling any access provided by an employee's password, authentication token, or biometric information when that employee leaves the firm?

□ Are servers and workstation applications periodically reviewed to identify accounts that are unused or were assigned to former employees and to make sure that these accounts have been removed or assigned new passwords?

Passwords

□ Are passwords required to meet minimum length and complexity requirements, including a mixture of character types or characters chosen from large character sets?

□ Is there a program checking passwords when they are created to make sure that they meet the prescribed minimum length and complexity requirements?

□ Are password choices automatically rejected if they are on the list of most commonly used passwords or consist mostly of a commonly used password?

□ Are the characters typed into password fields masked, so that they can't be read by bystanders?

□ Do corporate policies require secure procedures for issuing and transmitting passwords?

□ Are passwords always stored in an encrypted form?

Advanced Authentication

□ If an application is sufficiently critical or the information sufficiently sensitive, does the system use advanced authentication mechanisms, such as biometrics, two-factor tokens, or challenge exchanges?

□ If advanced authentication is used as an access mechanism, is this technology applied in a consistent and effective way throughout the enterprise?

□ If an application allows access to highly sensitive information, does it require a second person to provide verification before allowing access?

Biometric Systems

□ If biometrics are employed, is a password or personal identification number also required to verify identity?

□ If biometrics are employed, are live-scans or other sensor devices employed to help verify that the readings are being taken from a live person?

□ When a biometric identifier is generated from a live reading, does it incorporate a key unique to that person, so that if the identifier is stolen, it can be replaced with another?

□ Is there a stringent enrollment process for biometric identifiers, so that there is a high degree of confidence that the data captured is from the right person?

□ Once a user's biometric information is captured, is it stored in a secure location that prevents tampering or theft?

□ Do corporate policies define the procedures for dealing with the destruction of biometric information when it is no longer required?

Harder to Co-opt

□ Are employees required to change their passwords on a routine schedule mandated by corporate policy?

□ Are employees prevented from using previous passwords when a scheduled password change is required?

□ Are terminals and software systems set to lock out the user and require a new log-in when there is a period of inactivity or when some other device indicates that the employee has left the terminal?

Harder to Conceal

□ Do corporate policies require that all access attempts be logged, regardless of whether they are successful or unsuccessful, for applications that perform critical functions or store sensitive information?

□ Are all access logs written to a non-rewriteable disk or other permanent medium where even the systems administrator cannot tamper with them?

□ Are there automatic alarms triggered by multiple failed log-in attempts, even if distributed across time, across user ID's, or different systems?

□ Are multiple failed attempts to access applications reviewed in a timely manner, even if those failed access attempts are by authorized employees?

□ Is an effort made to identify and investigate successful access authentications that are carried out at unusual hours of the day or night?

□ Is there an alarm mechanism that would warn of the theft of a file in which passwords are stored?

□ Is there an alarm mechanism that would warn if a large number of passwords are being accessed from the files in which they are stored?

□ Is there an alarm mechanism that would warn if an unassigned general root-level or domain administrator account is utilized?

□ Are all changes that a systems administrator makes to passwords logged and reviewed?

□ Is there an alarm mechanism that sends a notification signal if an attempt is made to use a two-factor token or smart card after it has been revoked?

□ Is there an alarm mechanism that sends a notification signal if an attempt is made to use a deactivated user account?

More Reversible

□ Is there a procedure for rapidly and securely changing passwords across the organization if there is any reason to believe they may have been compromised?

□ If an employee needs to recover a password from a remote location, is that employee required to answer a series of challenge questions selected randomly from a database that contains many possible questions?

□ If an employee needs to recover a password from a remote location, is a link to recover or reset the password sent in an e-mail to that employee's regular e-mail account after the employee has successfully answered the challenge questions?

□ Is there a simple automated procedure for rapidly revoking the privileges for tokens and smart cards, if they become compromised?

□ Is there an efficient procedure for replacing tokens and smart cards?

□ Is there a simple automated procedure for revoking the privileges for any biometric identifier that is compromised?

□ Is there an efficient procedure for assigning a new key to someone whose biometric identifier has been compromised, so that person's identifier becomes different?

□ If it becomes necessary, does the organization have a way of accessing data and applications ordinarily protected by personal two-factor authentications, such as biometric authentication?

□ Do the organization and its vendors have a plan for replacing compromised biometric information with alternative information?

Area Three: Networks

PERMANENT NETWORK CONNECTIONS

Overview

□ Has the organization considered establishing separate networks for activities that have very different security requirements, such as normal business activities, production operations, environmental systems, corporate guests, and critically important research, design, and planning?

□ Does the organization maintain a list of all the devices on the corporate network, along with the manufacturer identification (MAC) numbers for those devices?

□ Does the organization maintain a comprehensive list of all the protocols and port numbers used by applications installed on the organization's computers?

□ Does the organization maintain a comprehensive list of all the system names and their associated network addresses on the organization's network?

□ Do detailed network topology diagrams exist of the corporate network, so that all the connection routes can be traced?

□ Do the detailed network topology diagrams list the service paths and network protocols being used?

□ Has the information on the network topology diagram been verified to be accurate, so that all the components and connections on the network are indeed included?

□ Are all documents diagramming network topologies rigorously protected from unauthorized access?

□ Does the organization maintain comprehensive access control lists for its routers, including the internet protocol addresses and port numbers being utilized?

□ Does the organization require that the access control lists for its routers be periodically reviewed, so that they take account of changes in the organization's traffic needs?

□ Does the organization require a second authorized employee to verify that the specific changes in access control lists are appropriate before these changes are implemented?

Harder to Find

□ Are the pieces of equipment connected to the corporate network assigned addresses that do not conform to any uniform system and are difficult to deduce?

□ If wireless technology is used for a sensitive network, is the beacon that would broadcast the network's presence disabled?

□ When there are categories of communication that only involve the organization's own computers, are unconventional (non-standard) port numbers being utilized?

□ If the organization is maintaining a separate network for security reasons, are all unnecessary services and broadcasts disabled on the gateway between networks, including responses to ping requests and traceroute requests, so that the existence of the gateway is difficult to detect?

□ If a network is used for highly critical functions, does the organization periodically change the port numbers used by those critical services, so that any previous unauthorized explorations by potential attackers of those port numbers and their uses will be made obsolete?

□ If a network is used for highly critical functions, does the organization periodically change the names of servers and other devices, so that any previous unauthorized explorations by potential attackers of those names and what they designate will be made obsolete?

□ If a network is used for highly critical functions, does the organization periodically change the network addresses of servers and other devices, so that any previous unauthorized explorations by potential attackers of those network addresses and their locations will be made obsolete?

Harder to Penetrate

Connecting Equipment to the Network

□ Is each router, switch, server, work station, or other piece of information equipment required to meet minimum security standards before it is connected to the network?

□ Are the baseline standards for equipment connected to the organization's network periodically reviewed and updated?

□ Are the vendor's default security settings, including default passwords and user names, changed on systems before those systems are connected to the network?

□ Are vulnerability scans or penetration tests performed on critical systems both before they are connected to the corporate network and regularly thereafter?

□ Are employees explicitly forbidden to plug unauthorized electronic devices, such as flash drives, iPods, Kindles, smart phones, and digital cameras, into equipment inside the corporate network?

□ Are switches in critically important facilities configured so that they will not connect to any pieces of electronic equipment that are not on the list of authorized manufacturer identification (MAC) numbers?

Network Management

□ Is the network itself secured by authentication procedures, in addition to the securing of systems on the network?

□ Are the passwords used on networking equipment, such as routers and switches, required to meet especially strong minimum length and complexity requirements?

□ Does the organization require periodic checks of its routers to verify that the access control lists have been accurately implemented?

□ If the organization is maintaining multiple networks for security purposes, are the connections and communications between these separate networks limited to the absolute minimum that is necessary for the effective functioning of the organization?

□ If the organization is maintaining an internal network that is used for activities that do not require a connection to the internet, has care been taken to make sure that no direct connections between that network and the internet exist?

□ Are legitimate systems that do not require wider network connectivity kept off all wider networks?

Wireless and Special Connections

□ Are there clear and rigorously enforced rules for establishing and using wireless connections to the internal networks?

□ Is access to the wireless connections limited to authorized devices?

□ Are wireless access points in critically important facilities configured so that they will not connect to any pieces of electronic equipment that are not on the list of authorized manufacturer identification (MAC) numbers?

□ Do the wireless connections employ strong encryption technologies?

□ Are there strict requirements and procedures for deploying any modems within the corporate infrastructure?

□ Is there a documented approval process for giving people remote access to modems?

□ If it is necessary to use insecure protocols for receiving or sending data, such as the File Transfer Protocol (FTP), are these insecure protocols supplemented with security protocols at the session protocol layer (e.g., yielding FTPS) or else transmitted over a virtual private network?

□ Are virtual private network connections being utilized to provide secure communications with partner networks?

□ Is there a documented approval process for giving people access to the virtual private networks?

Harder to Co-opt

Network Management

□ Is there a mechanism to automatically restart critical components, such as web server applications, whenever other applications are repeatedly unable to connect with them?

□ Are internal wireless networks segmented, using different service set identifiers (SSID's) or another method, so that access to one segment of the wireless network does not automatically provide access to the other segments, and so that more restrictive policies can be applied to the more critical parts of the network?

□ Does the organization have agreements with vendors in which they guarantee a specified level of network reliability and service?

□ Do corporate policies limit the use of unencrypted protocols, such as FTP, Telnet, or earlier versions of SNMP, for system management, unless the system explicitly requires these protocols?

□ If the systems require unencrypted protocols, such as FTP, Telnet, or earlier versions of SNMP, for their management, are the corresponding connections set to shut down after a limited period of time?

□ Does the corporation use access control lists to restrict SNMP requests from unauthorized systems to networking equipment, such as routers and switches?

□ Are there policies for limiting the use of any remote management tools that would allow systems to be controlled from outside the corporate network?

□ Is the remote management of routers, switches, and other network components restricted to authorized internet protocol addresses?

□ Are there policies for monitoring the use of any remote management tools that would allow systems to be controlled from outside the corporate network?

Traffic Handling

□ Have the networking components been configured to give more critical categories of traffic, such as process control instructions, priority over less critical categories of traffic, such as e-mails?

□ Are there procedures for rate-limiting traffic so that the network is not incapacitated by excessive loads on the services affected?

□ Have tests been conducted to make sure that critical systems cannot be taken offline too easily by large amounts of data or traffic, such as might be employed in a denial service attack?

□ Are there procedures for adding additional servers and redirecting traffic to prevent critical network components from being incapacitated by excessive loads on the services affected?

Harder to Conceal

Unauthorized Equipment

□ Is the network automatically and frequently scanned for connections to pieces of electronic equipment with manufacturer identification (MAC) numbers that are not on the list of authorized devices?

□ Does the organization monitor for symptoms of manufacturer identification (MAC) numbers being spoofed, such as a mismatched operating system, mismatched device type, incorrect device location, and uncharacteristic behavior of the device?

□ Is a wireless analyzer periodically run to identify any unauthorized wireless devices that may have been connected to the network?

□ Are internal war-dialing campaigns periodically carried out to identify unauthorized modems that can be reached by dialing in?

□ Are corporate phone exchanges periodically checked to detect outside attempts at finding unauthorized modems by war-dialing campaigns?

Network Management

□ Is there a mechanism to automatically inform the system operator whenever critical components are shut down and restarted?

□ Are network software components automatically tested on startup for changes in security configurations that have been made since the system was last started and, if changes are found, is the system administrator automatically notified?

□ Are all modifications of server configurations logged?

□ Are the logs of server configurations regularly reviewed to make sure that any changes in the configurations did not undermine security?

□ If the servers are performing critical operations or store very sensitive information, are the logs recording changes in their configurations reviewed daily?

□ Are all modifications of router and switch configurations logged?

□ Are the logs of router and switch configurations regularly reviewed to make sure that changes in configurations did not undermine security?

□ Are all modifications of wireless access point configurations logged?

□ Are the logs of wireless access point configurations regularly reviewed to make sure that changes in configurations did not undermine security?

Network Monitoring

□ Is the network traffic regularly monitored to establish normal usage patterns?

□ If the organization is maintaining multiple networks for security purposes, are there special provisions for monitoring traffic between those networks?

□ If there are significant changes in the volumes and pathways of network traffic, are the reasons for these changes investigated in a timely fashion?

□ Are measures taken to monitor domain name system (DNS) servers for attacks that reroute requests to unauthorized locations?

□ Is the network traffic regularly monitored for covert communication channels?

More Reversible

□ If the organization detects a manufacturer identification (MAC) number that is exhibiting suspicious activity, is the device quarantined until the suspicious activity is investigated?

□ Do critical systems have redundant communication connections?

□ Do critical systems use redundant domain name system (DNS) servers to lessen the effect due to interruptions of that service from one source?

□ Do any networks that are extremely critical have redundancy in the switching equipment?

CLOUD PROVIDER CONNECTIONS

Overview

□ Are the people in the organization who are responsible for cloud computing policies made aware that the use of an external cloud provider will require additional security measures?

□ Are the people in the organization who are responsible for cloud computing policies made aware that any *unencrypted* information stored with a cloud provider could potentially be obtained by a subpoena before the organization could take legal steps to prevent this?

□ Are the people in the organization who are responsible for cloud computing policies made aware that the extra encryption needed to secure information in the cloud could result in longer response times for information systems?

□ Are the people in the organization who are responsible for cloud computing policies aware that any plan for moving activities into the cloud needs to be accompanied by a plan for moving activities out of the cloud, in the event that changes in computing costs, computing methods, or computing security make this advisable?

□ Is the provider of cloud computing services contractually required to carry out a thorough wiping of any media used to store the organization's proprietary applications and data when the contract for handling that software ends?

□ Has the organization identified which kinds of documents and data can be handled using third-party collaborative platforms, such as Google Docs or Dropbox, depending on the sensitivity classification of those documents and data?

Harder to Find

□ Are the subdomain names that the organization uses for external cloud computing services named in a way that will prevent someone determining the cloud provider from those names?

□ Do the uniform resource locators (URL's) used to access external cloud services mask the identity of the cloud provider?

Harder to Penetrate

□ Do all administrator accounts used for cloud computing resources require two-factor authentication?

□ Does the organization maintain separation between virtual machines performing more critical operations and those performing less critical operations?

□ Is the management of external cloud computing resources performed using encrypted channels?

□ Is any remote use of the cloud management interface performed over secure communication channels, such as a virtual private network?

□ Is the cloud management interface configured to restrict administrator access from unknown internet protocol addresses?

□ Is the cloud management interface designed with the minimum number of functions needed to manage the virtual machines, so that there are fewer opportunities to mount an attack utilizing those functions?

□ Is the cloud provider using hypervisors that have a boot configuration designed to disallow the use of non-certified drivers?

Harder to Co-opt

Cloud Management

□ Is all sensitive information that the organization stores in the cloud encrypted?

□ Is all sensitive information transmitted between the client and the cloud encrypted?

□ Does the cloud provider maintain redundant secure communication channels for accessing the cloud management interfaces?

□ If the organization performs critical operations using external cloud computing resources, are these operations logically isolated from other virtual machines by the use of a separate hardware-level hypervisor?

□ Is the organization choosing virtual machines for its critical operations that are designed to fail to a state which protects the system from security compromises and data breaches?

□ If the organization performs *highly* critical operations using external cloud computing resources, is a special arrangement made with the cloud provider to host those operations on dedicated servers, used only by the organization?

Third-Party Collaborative Platforms

□ If the organization allows its employees to use third-party collaborative platforms, such as Google Docs or Dropbox, for standard business operations, do they require employees to use only those platforms that encrypt all files at rest?

□ Does the organization require its employees to refrain from putting any information on third-party collaborative platforms if it is considered very sensitive?

□ If the organization allows its employees to use third-party collaborative platforms, such as Google Docs or Dropbox for standard business operations, has two-step log-in verification been implemented for those accounts?

□ Are employees prevented from using personally owned smart phones to access third-party collaborative platforms used for work?

□ Are employees forbidden from placing work documents in personal accounts on third-party collaborative platforms?

□ Does the organization make it a policy to limit the length of time over which work documents are stored or handled on third-party collaborative platforms?

□ Does the organization periodically verify that documents which no longer need to be handled on third-party collaborative platforms have been removed from those platforms?

Harder to Conceal

□ Are databases located at external provider of cloud computing services monitored for large data transfers that are outside normal behavior?

□ Are the access logs for the cloud management interfaces transmitted over a secure channel to an external server, where even the systems administrator cannot tamper with them?

More Reversible

□ Is special care taken to make sure that the approved master reference copy (i.e., "golden image") for each operating system and suite of applications in the cloud is complete and up-to-date?

□ Are backups of sensitive information that are made by the cloud provider periodically duplicated and stored at a third site, physically separate both from the cloud provider's facilities and from the organization's main facilities?

□ Are copies of cryptographic keys used to encrypt sensitive information at the external provider of cloud computing services stored at a third site, physically separate both from the cloud provider's facilities and from the organization's main facilities?

□ Does the organization have a set of procedures ready for moving all of its cloud operations and data out of the cloud?

□ Does the organization have a set of procedures ready for moving all of its cloud operations and data to another cloud provider?

□ Have the procedures the organization has ready for moving its cloud operations been designed so that its proprietary applications and data will be encrypted during their transmission to a new set of computers?

INTERMITTENT NETWORK CONNECTIONS

Overview

□ Are employees on the road issued standardized laptops or standardized mobile devices that meet corporate security requirements?

□ If the organization is supplying laptops or mobile devices to its employees, does the organization withhold administrator privileges from those employees, so that it can limit the applications installed on those laptops or devices?

Harder to Find

□ Does the organization arrange for its domain registrar to keep its identify and contact information confidential for any domains that are intended only for the organization's own private use?

□ Do any public-facing websites that are intended only for the organization's own private use omit any mention of the organization's identity and avoid including any information that could be used to deduce that identity?

□ If the organization is maintaining public-facing websites intended only for the organization's own private use, do these websites use internet protocol (IP) addresses that are not easily identifiable as belonging to the organization?

□ If the organization uses any dial-up modems for remote management or secure connections, do these have phone numbers that are unlisted and difficult to deduce?

Harder to Penetrate

Employee Laptops & Mobile Devices

□ Are employee laptops protected by anti-virus software?

□ Are all smart phones issued by the organization protected by anti-virus software if those devices are vulnerable to viruses?

□ Are the anti-virus signatures and definitions on employee laptops and smart phones updated as soon as new signatures are available?

□ Are employee laptops protected by internet-protection software that blocks access to dangerous websites or known hostile IP address ranges?

□ Are infrared, bluetooth, and wireless links on laptops and mobile devices disabled when not required for business functions?

□ Are remote log-in's from employee laptops required to use IP addresses that were used in the past or are consistent with the employee's expected geographical location?

□ Do remote log-in's from employee smart phones require geopositioning data from those devices that is consistent with the employee's expected geographical location?

□ Do corporate policies define security requirements for off-site wireless modems and wireless broadband connections?

□ If Voice over IP (VoIP) is employed for sensitive communications, are the transmissions encrypted?

Virtual Private Networks (VPN's)

□ Are telecommuters required to use virtual private network connections to obtain access to the corporate network?

□ If the organization uses virtual private networks, is two-factor authentication required?

□ If the organization uses a virtual private network to access highly-critical systems, are more stringent authentication mechanisms, such as tokens and biometrics, required?

□ If the organization uses virtual private networks, are the connecting computers first connected to a computer in an isolated network that runs a security check on the remote computer before it is granted access to the internal network?

□ If a web-based virtual private network is used, does it securely remove information about the session from the computer that initiated the session?

Dial-Up Modems

□ If the organization uses any dial-up modems for remote management or secure connections, do these devices have security features to verify authorized callers before connecting?

□ If the organization uses any dial-up modems for remote management or secure connections, do these devices have dial-back security features to ensure that only authorized callers are connected?

□ If the organization uses any dial-up modems for remote management or secure connections, do these devices have embedded authentication capabilities, such as pair-shared keys?

Temporary Connections Inside Facilities

□ Are there strict controls on any laptops, storage media, or other kinds of equipment that are periodically plugged into the corporate network to update software or perform other maintenance?

□ Does the organization scan all laptops that are temporarily connected to the corporate network by outside vendors and contractors to verify that they are free of viruses, worms, and other malware?

□ Are direct wireless connections to the corporate network protected by strong identification codes and strong passwords?

Harder to Co-opt

□ If smart phones and other small mobile devices are allowed, does the organization restrict sensitive information from being downloaded to these devices?

□ If a large portion of the activities carried out on an employee's laptop involve highly sensitive information, is the entire hard drive on that laptop encrypted?

□ If only a modest portion of the activities carried out on an employee's laptop involve sensitive information, are the documents and data files containing that information encrypted using encryption containers or single file encryption?

□ If sensitive information needs to be stored on laptops or other mobile devices only temporarily, is the tool for encrypting and decrypting that information extremely convenient to use?

□ Are internal microphones and cameras on laptops disabled within sensitive areas?

□ If employee e-mails contain sensitive information, are these e-mails encrypted during transmission?

□ If an employee laptop contains a CD drive that could be used for booting in an emergency, is the boot sequence of that laptop set so that it cannot be booted from a USB connection?

□ If an employee laptop contains information sensitive enough to require full disk encryption, is the boot sequence of that laptop set so that it can only be booted from its internal hard drive?

□ If a service application needs to be kept proprietary for competitive purposes, is it made web-accessible only to trusted personnel, rather than web-accessible to a wider population?

Harder to Conceal

□ If removable information devices are allowed, does the organization monitor the usage of such devices?

□ Is each employee assigned a different identification code and password for connecting to the wireless network, so that employee activities using this network can be readily tracked?

□ Are the activities carried out by laptops that are temporarily connected to the corporate network by outside vendors and contractors tracked and monitored?

□ If Voice over IP (VoIP) is employed for sensitive communications, are the transmissions randomly scanned to detect content consisting of data, rather than voice?

□ If the organization uses any dial-up modems for remote management or secure connections, do these devices provide an audit trail for authorized log-ins and activities such as "break in" attempts?

□ Is there extra monitoring of remote connection activities to compensate for the fact that they are less supervised in other respects?

□ Does the organization monitor its inbound internet traffic for signs of session hijacking (e.g. sequence numbers out of sequence)?

□ If there are indicators of session hijacking activity being carried out, are these cases investigated in a timely manner?

More Reversible

□ Does the organization provide employees with an efficient internal service for removing malware from their laptops and mobile devices if the employee believes that these may have been infected?

□ If an employee's entire laptop hard drive is encrypted, does that employee have a way of conducting essential business if the hard drive cannot be accessed?

PUBLIC AND E-COMMERCE CONNECTIONS

Overview

□ Are web portals for e-commerce constructed by specialists in website and e-commerce security?

□ Are web portals for e-commerce checked more frequently for security issues than other corporate information systems?

□ Does the organization register its domains using a well-established domain registrar?

Harder to Find

□ Has the organization disabled or modified the banners or strings that announce the name and version of the software products being used on public-facing web servers?

□ Are any names or logos that would identify the specific types of software incorporated into a website removed from the publicly accessible images and metadata?

□ Has the organization removed all software testing pages and scripts on public-facing web servers?

Harder to Penetrate

Account Management

□ Does the organization mandate that accounts used to manage domain registration use two-factor authentication?

□ Has the organization enabled security features, such as a registrar-lock, on its domain registrations, to prevent unauthorized modifications?

□ Does the organization require two-factor authentication for accounts used to manage high-profile social media accounts, such as Facebook and Twitter?

Transaction Processing

□ If business transactions are being carried out over the internet, is data being collected from the customer and from the customer's computer or mobile device that will help authenticate the transaction?

□ If the mobile device uses geopositioning information, is that information employed as one of the factors that will determine whether a transaction will be allowed?

□ Is a hashed time stamp transmitted with the transaction, so that an unexplained transmission delay can trigger a demand for further authentication?

□ Are customer verifications for e-commerce transactions protected from automated attacks by the display of a visual image or audio play-back that contains a pattern which only be recognized by a human being (CAPTCHA)?

□ Is there a mechanism that will automatically terminate an e-commerce session after a period of inactivity?

□ If internet business transactions are sufficiently large financially, are these transactions authenticated both by digital certificates and by other advanced authentication mechanisms?

□ Is there a mechanism that allows customers to verify that they are on a legitimate website of the organization with which they are intending to do business?

□ If digital certificates are utilized for e-commerce transactions, are these certificates issued by an industry approved certificate authority?

□ When digital certificates are utilized for e-commerce transactions, is there a mechanism for verifying that the business is actually being conducted from the system for which the certificate was issued?

Instructions from Customers

□ Are vulnerability scans and penetration tests regularly performed on all internet or customer facing systems and applications?

□ Is all user-supplied information that is included in database queries between the client application and the database properly sanitized (i.e., escaped) prior to it use?

□ Are all queries from a client application that are not written in a highly constrained form blocked from reaching any database containing sensitive information?

□ Are all file uploads coming from public-facing websites restricted to files of a specific type and size?

□ Are all uploaded files coming from public-facing websites automatically scanned for malicious content?

Harder to Co-opt

□ Does the organization make it a policy never to send links to its website in e-mails, except for the address of its home webpage?

□ Are customer log-in screens normally accessed from the organization's home webpage?

□ Has the organization purchased any available web addresses that could easily be mistaken for its own?

□ Are all transactions associated with an individual user session accompanied by a unique, unpredictable session code that is included to prevent the codes for establishing the session from being reused by an attacker?

□ Is sensitive customer information, such as credit card numbers and personal identifiers, handled by systems different from the one that handles the web transaction itself?

□ If a financial transaction or business order is considerably larger than the normal range, does the transaction automatically require extra verification?

□ Are the file names used for storing files uploaded from public-facing websites completely different from the names of the users who supplied the information?

□ If the organization allows customers to post reviews on its website, is care taken to make sure that these postings do not reveal the customers' e-mail addresses or log-in names?

□ If the organization uses a social media account, such as a Twitter, for communicating security warnings, are all matters that don't serve this purpose kept off of that account?

Harder to Conceal

□ Is there an alarm mechanism that warns if internet business transactions involve unusual combinations of customer identities, billing addresses, and shipping addresses?

□ Does the organization choose easily recognizable uniform resource locators (URL's) for its e-commerce web pages, so that customers will see that these URL's look authentic?

□ Does the organization regularly search the web for bogus websites that pretend to belong to the organization?

□ Does the organization regularly search the web for bogus smart phone applications that pretend to facilitate secure connections to the organization's websites?

□ Does the organization monitor its high-profile social media accounts, such as Facebook and Twitter, for signs of unauthorized access or use?

□ Has the organization implemented the Sender Policy Framework for all their mail servers, in order to detect and prevent e-mail spoofing?

□ Does the organization provide the public with contact channels, including both a phone number and e-mail address, that are to be used only for reporting possible security issues?

More Reversible

□ Are public-facing websites equipped with anti-tampering software, which will automatically restore each site to its proper condition if an attempt is made to deface it?

□ Is there a plan in place for working with the provider of a social media account to get the account rapidly shut down if it is compromised?

□ Is there a procedure for acting rapidly to get bogus social media posts that pretend to belong to the organization taken down?

□ Is there a procedure for acting rapidly to get bogus websites that pretend to belong to the organization taken down?

□ If the organization's website is defaced, is there a plan in place for getting the defaced copies of the website rapidly removed from the caches of the leading search engines?

□ Is the contact information periodically updated that the organization provides to its domain registrar?

□ Is the contact information periodically updated that the organization provides to the regional internet registrar that maintains its assigned internet protocol (IP) addresses?

ENCRYPTION SYSTEMS AND DIGITAL CERTIFICATES

Overview

Encryption Systems

□ Do corporate policies define what type of data communications should be encrypted and which encryption technologies should be employed?

□ Is encryption explicitly required for the storage and transmission of all information above a designated sensitivity level?

□ Are the people in the organization who are responsible for encryption policies made aware that the organization's own encryption mechanisms could potentially be used by cyber attackers to make the encrypted information permanently inaccessible?

□ Does the organization have multiple encryption options available, such as individual document encryption, encryption containers, and full disk encryption, so that the scale of encryption can be adjusted to the quantity of information on a given computer that needs to be encrypted?

□ If the organization will need to encrypt transmissions of data between distributed, local devices with limited resources for computing and memory, do the organization's encryption options include one that can be applied with those limited resources?

□ If the organization is handling extremely critical information, is there a separate encryption policy for the handling of that information?

□ If the organization is handling extremely critical information, does the organization have an appropriately advanced encryption tool available for encrypting that information?

□ If highly sensitive information is being handled using an advanced encryption tool, does that encryption tool require two-factor authentication for decryption?

Digital Certificates

□ Does the organization maintain a comprehensive list of the certificate of authorities and digital certificates used by their computer systems and applications?

□ Are digital certificates obtained only from well-established certificate issuers who investigate all the companies to which they issue certificates?

□ Are digital certificates used on any customer website to encrypt the connection and transactions with Secure Sockets Layer (SSL)?

□ Are digital certificates used for digitally signing applications under development?

□ Are digital certificates embedded in the firmware of hardware devices performing secure connections, which allow for trusted authentication between multiple systems?

□ Are digital certificates used for the organization's virtual private networks?

Harder to Find

□ Are the encrypted repositories that contain encryption keys made to look like something else?

Harder to Penetrate

□ Are encryption keys created in a secure manner, using approved industry methods?

□ Are encryption keys and digital certificates distributed in a secure manner that prevents theft?

□ Are encryption keys stored in a secure manner, using approved industry methods?

□ Are decryption procedures activated separately from ordinary log-in procedures and required to use different passwords?

□ Do systems that have certificates installed have adequate security measures that prevent the theft of the private keys of these certificates?

□ Are the repositories used to store copies of the root-certificates and code-signing certificates protected by strong encryption?

□ Is access to the repositories used to store copies of the root-certificates and code-signing certificates protected by two-factor authentication?

□ Is access to encrypted repositories for encryption keys restricted to the smallest number of administrators that will still allow access on short notice?

□ Is access to encrypted repositories for encryption keys organized so that no single administrator has access to multiple repositories?

□ Do the organization's encryption keys and digital certificates have expiration periods?

□ If a vulnerability has been discovered in the encryption software used for financial transactions, such as Secure Sockets Layer (SSL), is there a procedure to have that vulnerability patched within hours of when the patch first becomes available?

□ If a digital certificate is discovered to contain a vulnerable cryptographic component, are there procedures to have the certificate promptly re-issued by the certificate authority?

□ Are encryption keys destroyed in a secure manner, using approved industry methods?

□ Are computer systems and applications configured to verify digital certificates by automatically checking certificate revocation lists?

Harder to Co-opt

□ If private encryption keys are maintained, are they archived in a password protected and encrypted area to prevent tampering or theft?

□ Are encryption keys that are used for different tasks stored in different encrypted repositories?

□ Is there a reliable system for renewing digital certificates used on any customer website, so that customers will never have to ignore security warnings to proceed to the site?

Harder to Conceal

□ Is the generation of encryption keys logged in a tamper-proof file that records the generating employee's identity and the time?

□ Does the organization periodically review Secure Sockets Layer (SSL) traffic to identify locations which are inconsistent with normal business operations?

□ Does the organization periodically review Secure Sockets Layer (SSL) traffic to identify traffic that might be using a custom encryption scheme masquerading as legitimate SSL?

More Reversible

□ Are there regular and reliable procedures for the archiving of private encryption keys and the associated pass phrases for individual users?

□ Are copies of the private keys of digital certificates stored in a password protected and encrypted area that allows recovery and prevents theft?

□ Is there a quick and effective procedure for dealing with compromised encryption keys?

□ Is there a procedure in place that will allow compromised private keys of digital certificates to be rapidly revoked?

□ Are archives of private encryption keys and associated pass phrases keys maintained after they are no longer in active use, so previously encrypted files can be retrieved if necessary?

FIREWALLS, INTRUSION DETECTION SYSTEMS, & CONTENT FILTERS

Overview

□ Has the organization made lists of the traffic destinations and kinds of traffic, both inbound and outbound, that it wants to allow through its firewalls?

□ Does the organization require the lists of the traffic it allows through its firewalls to be periodically reviewed, so that they take account of changes in the organization's traffic needs?

Harder to Find

□ If the organization is utilizing unconventional port numbers for communications involving its own computers, are its firewalls configured to block communications that appear to come from its own computers, but utilize the conventional port numbers?

□ Is network address translation (NAT) employed to conceal internal internet protocol (IP) address information?

Harder to Penetrate

Firewalls

□ Has the organization configured its network firewalls to allow only the types of traffic on its approved lists?

□ Has the organization enabled anti-spoofing on its firewalls to block ranges of private internet protocol (IP) addresses (e.g., the RFC 1918 list) coming from the internet?

□ Are personal firewalls employed on individual employees' computers, in addition to the network firewalls?

□ Are there additional internal firewalls deployed to protect critical systems from unauthorized access by internal personnel?

Intrusion Detection and Prevention

□ Are intrusion detection and/or intrusion prevention systems used on the organization's network?

□ Are signatures regularly updated on intrusion detection and prevention systems?

□ Are the instruction sets for intrusion prevention systems immediately revised when abnormal patterns of activity suggest that new kinds of attacks are being attempted?

□ Are additional signatures being collected from malware that was captured and from other intelligence sources?

□ Is there a regular procedure for adding other signatures that have been identified as dangerous to the list of those that the intrusion detection and prevention systems are blocking?

□ Is an up-to-date list maintained of the additional signatures that the intrusion prevention system has been instructed to block?

□ Is the list of additional signatures to be blocked periodically compared with the list of access attempts that *were* blocked, in order to verify these procedures are producing some benefit?

Content Filters

□ Are all e-mails and e-mail attachments received by employees automatically scanned for possible malware?

□ Are all web links in e-mails received by employees automatically checked against lists of websites known to be dangerous?

□ Are all files downloaded from the internet by employees automatically scanned for possible malicious content?

□ Does the organization use content filtering to limit to receipt of Active X, JavaScript, and Java Applets?

□ Does the organization make a serious effort to filter out all executable e-mail attachments?

□ Does the organization block internet downloads by employees that do not correspond to their work roles?

□ Are the instruction sets for content filters immediately revised when abnormal patterns of activity suggest that new kinds of attacks are being attempted?

Harder to Co-opt

Firewalls

□ Does the organization have an approval process for any changes in the rule sets defining the traffic it will allow through its firewalls?

□ Is network access to the management interfaces of firewalls, intrusion prevention systems, and content filters restricted to only authorized internet protocol (IP) addresses?

Content Filters

□ Are all uploads to the internet by employees restricted by a content filter to information and files of specific types and below certain sizes?

□ Does the organization perform content filtering on all file attachments being sent through e-mail, so that any transmission of sensitive information by this means is either blocked or tracked?

□ Does the organization perform content filtering on all outbound file transfer protocol (FTP) or trivial file transfer protocol (TFTP) transmissions, so that any transmission of sensitive information by these means is either blocked or tracked?

□ Does the organization use content filtering to control instant messages that may contain sensitive information?

□ Are content filters set to block export of sensitive documents tagged with digital watermarks, unless special authorization has been provided to export them?

□ Are content filters employed to help prevent confidential information from being uploaded to third-party collaborative platforms, such as Google Docs or Dropbox?

□ Are content filters employed to help prevent confidential information from being uploaded to web-based e-mail applications?

□ Are content filters employed to help prevent the transmission of sensitive information through social media and electronic greeting card portals?

Harder to Conceal

Firewalls

□ Does the organization require periodic checks of its firewalls to verify that the rule sets have been accurately implemented with no ad hoc changes?

□ Are configuration modifications to firewalls logged?

□ Are security logs for firewalls maintained in a way that prevents them from being modified or deleted?

□ Are security logs for firewalls regularly reviewed to establish baselines for normal traffic patterns?

□ Are security logs for firewalls regularly reviewed for unauthorized traffic?

Intrusion Detection and Prevention

□ Are security alerts from intrusion detection systems continuously monitored?

□ Are configuration modifications to intrusion detection systems and intrusion prevention systems automatically logged?

□ Are security logs for intrusion detection and intrusion prevention systems maintained in a way that prevents them from being modified or deleted?

□ Are security logs for intrusion detection systems regularly reviewed to detect abnormal patterns of activity?

□ If an attempt is made to access the organization's internal network using the organization's own range of private internet protocol addresses, does this trigger a warning alarm?

□ If the organization is utilizing unconventional port numbers for communications involving its own computers, do communications that appear to come from its own computers, but utilize the conventional port numbers, trigger a warning alarm?

□ If abnormal patterns of activity are detected in the intrusion detection logs, are these immediately analyzed to determine what new types of attacks are potentially being attempted?

Content Filters

□ Are content filters regularly tested to make sure they are actually blocking what they are supposed to be blocking?

□ Does the organization have procedures for reviewing e-mail attachments that have been quarantined?

More Reversible

□ When restrictions implemented by content filters are relaxed or removed, are these changes automatically archived, so that the content filters could later be restored to their more restrictive condition?

□ If the reviews of the firewall and intrusion detection logs reveal unauthorized traffic, is this traffic immediately investigated to determine what steps might be taken to reduce its possible effects?

Area Four: Automation

AUTOMATED OPERATIONS AND PROCESSES

Overview

□ Is there an overall map that accurately identifies all the communication paths by which control systems are connected?

□ Does the map of control system connections identify all the places where the response time must be extremely short, so that no security measures are introduced that might cause dangerous response delays?

□ Have all computer controlled physical processes that could produce dangerous physical conditions been clearly identified?

□ Are software patches and updates for critical systems handled separately from patches and updates for other systems?

□ Are there additional verification and testing procedures for software patches that affect the safety or effectiveness of a critical device?

□ Is there a documented procedure which allows a system *not* to be patched or updated in cases where this might create a greater hazard than an unpatched system?

Harder to Find

□ Are all documents that provide maps of the logical access routes to control systems rigorously protected from unauthorized access?

□ Are vendors of control system programs and components contractually prevented from revealing publicly or to third parties what kinds of programs and components they have supplied?

□ Has care been taken to make sure that intruders are not presented with clearly labeled schematic diagrams of the individual physical processes and the systems for managing them?

□ Have the addresses and labels for control system components, such as remotely operated switches and valves, been assigned in such a way that their functions are not too easy to guess or deduce?

□ Have the command codes for control system components, such as remotely operated switches and valves, been customized, wherever this can be done without creating hazards, so that they do not follow the default industry formulas?

Harder to Penetrate

Control Networks

□ Are all control systems that do not need to be connected to the internet isolated from the internet?

□ Are all control systems that *do* need to be connected to the internet isolated by access control lists?

□ Are all connections between control systems and the internet periodically evaluated to see whether these connections are really necessary?

□ Are all control systems isolated from the corporate network whenever there is no compelling reason to connect them?

□ If a control system cannot be isolated from the corporate network, is the control system protected by highly restrictive firewalls and intrusion detection systems?

□ Are port numbers used by control systems blocked at the perimeter firewalls?

Control Devices

□ Do all new remote terminal units and other control devices being installed in the network have changeable passwords or other reprogrammable authentication mechanisms?

□ If remote terminal units and other control devices have the capability of employing passwords and the operational speed requirements allow this, are passwords being used?

□ Are the default passcodes for control systems changed before they are put into service?

□ Are status queries to remote terminal units and other control devices sent in a secure manner from a secure source?

□ Are updates to the operating systems of remote terminal units and other control devices sent in a secure manner from a secure source?

□ Do updates to the operating systems of remote terminal units and other control devices need to be digitally signed by the vendor before being applied?

□ Is the integrity of updates to the operating systems of remote terminal units and other control devices verified before these are applied?

Harder to Co-opt

Range of Action

□ Are the computers inside production facilities extremely limited in the software applications they contain?

□ Are the schematic diagrams and instructions for managing physical processes kept in a system that is separate from the system that is used for the command inputs controlling those processes?

□ Are there pre-set parameters for inputs governing critical processes, so that attempted inputs outside those parameters are either blocked or need confirmation from another source?

□ If control systems that manage highly critical processes, especially dangerous ones, are severely disrupted, do these processes automatically revert to a safe, stable state or go into a controlled shut-down?

□ Have the remote sensors been designed or modified to make it difficult for someone to cause them to report false data by manipulating them physically?

Transmission of Instructions

□ Are the computers in production facilities extremely limited in the kinds of information they can receive and send?

□ If the command codes for control system components have been customized to not use the default formulas, are the control systems configured to ignore any commands that *do* follow the default formulas?

□ Are all periodic automated transmissions of critical control data, where speed is not an issue, protected by encryption?

□ Is there a separate, second channel for putting highly critical processes, such as physically dangerous ones, into a safe, stable state or into a controlled shut-down?

□ If remote sensors communicate via cellular, satellite, or other wireless connections, have measures been taken to prevent information transmissions from being falsified?

Time Controls

□ Are all critical system components within the network synchronized, so that they are using the same time zone?

□ Are critical system components configured to regularly update their time from a secure time source?

□ Do especially critical system components periodically update their time from different time sources, so that any spoofing or corruption of the communications with one time source would be detected?

Harder to Conceal

□ Are there sufficient alarms to warn operators when any critical processes are in danger of moving outside the normal parameters of safe operation?

□ If a large portion of the schematic diagrams and instructions for managing physical processes are accessed in a short period of time, does this automatically trigger a warning alarm?

□ Are there provisions, such as remote alarms, which would warn that remote sensors are being physically manipulated on site to produce false readings?

□ Are there second sets of sensors that monitor critical processes with a different measuring technique, so that a false reading from the first set of sensors would be rapidly detected?

□ Are there regular procedures for checking adjustments and changes in control systems to make sure that the changes which should correlate do, in fact, correlate?

□ Are "honeypot" controls that appear to function, but don't actually do anything, employed to detect unauthorized explorations of the automated control systems?

□ Are the computers and systems that run quality control checks kept separate from the computers and systems that control production operations?

□ Are access procedures and codes for the computers and systems that run quality control checks considerably different from the access procedures and codes for the computers and systems that control production operations?

□ Are the details of the quality control test procedures known only to those employees who are actually carrying out those test procedures?

□ Are the records of production outputs that fail their quality control tests periodically examined to determine if those quality control problems could have been caused by cyber attacks?

More Reversible

□ If communications involving control settings are interrupted, do the controls automatically reset to normal or safe levels?

□ Are highly critical controls accessible by a secure secondary control channel, so that they can still be accessed if the first control channel fails?

□ Are there plans and procedures for dealing with the possibility of critical wireless links being jammed or disrupted?

PERIPHERAL DEVICES AND PHYSICAL EQUIPMENT

Overview

□ Are the security features of distributed, local devices taken into consideration before those devices are purchased?

□ Does the organization collect information on the resources of distributed, local devices, in order to determine what kinds of encryption and other security measures would be possible with those devices, given their limited resources?

□ Is the ability of the purchaser to customize the security settings on distributed, local devices treated as a significant factor in decisions about whether to purchase these devices?

□ Are the procedures for the secure updating of firmware treated as a significant factor in decisions about whether to purchase distributed, local devices?

□ Is there a list of the peripheral devices, such as printers, scanners, that are shared between multiple employee computers, along with additional lists of the computers sharing them?

□ Is there a list of the local computers that provide coordination between multiple local devices?

□ Is there a list of the local device computers that can connect to the internet, along with an identification of the paths by which they can do this?

□ Are records kept of all modifications of the firmware and software in distributed, local devices?

□ Is there document that accurately identifies all the kinds of data that are being collected from the distributed, local devices that the organization owns or that are located in its facilities?

□ Is data collected from distributed, local devices only when there is a clear benefit from collecting that data?

□ Is there a limit on how long any data collected from distributed, local devices is retained, based on when the retention of that data would deliver no further benefits?

Harder to Find

□ If distributed, local devices need to be located in public places, are they installed behind walls, in fixtures, or behind panels, so that their exact physical position and layout is not apparent?

□ If a local device, such as a piece of medical treatment equipment, performs a critical process, does the network name for that device conceal its true function?

Harder to Penetrate

□ If it is economically practical, are the cases or housings of distributed, local devices closed or locked in a way that would make it difficult to access the internal

electronic components without disabling the device? (E.g., are point-of-sale credit card readers designed so that it would be difficult to open them up without breaking a connection necessary for their operation?)

□ Are the default passcodes for wireless and bluetooth connected devices changed before they are put into service?

□ Are the infrared, bluetooth, and wireless links on printers and scanners disabled if they are not regularly required for business functions?

□ Is every device that could be used to do physical harm, such as medical treatment equipment, isolated from any network that is connected to the internet, unless there is a compelling reason to connect to the internet?

□ If there is a compelling reason to connect a potentially dangerous device to the internet, is this connection physically disabled (e.g., physically unplugged), except when the internet connection is needed?

Harder to Co-opt

□ Are the data storage components inside distributed, local devices installed in such a way that they cannot be easily removed from the device?

□ Whenever possible, is the data that is being transmitted between devices encrypted?

□ Whenever possible, is the data being transmitted between devices and the local computers coordinating their activities encrypted?

□ Are video feeds from drones and other autonomous or semi-autonomous devices encrypted?

□ Are different devices given different passcodes, so that they cannot all be accessed in the same way at the same time?

□ If peripheral devices used locally, such as printers and scanners, can hold large amounts of data, are these devices prevented from sending or receiving large amounts of data over the internet?

□ If a critically important device, such as a piece of medical treatment equipment, needs to be periodically recalibrated, is that recalibration carried out using a different computer than the one normally used to control the device?

□ If data collected from distributed, local devices could be used to deduce personal information, is that data stored only in an encrypted form?

Harder to Conceal

□ Are distributed, local devices equipped with tamper-proof seals that will reveal if their cases or housings have been opened?

□ If a local device that needs to be connected to the internet sends or receives data at unusual times, frequencies, or volumes, does this trigger an automatic warning alarm?

□ If there are indicators of unusual types or quantities of activity being carried out by local devices, are these cases investigated in a timely manner?

□ Is the traffic generated by local devices periodically scanned to determine if any data is being sent in clear text that should be encrypted?

□ If a local device, such as a piece of medical treatment equipment, contains customized settings that are highly important, are the most critical of these settings regularly checked to be verify that they have not been improperly changed?

More Reversible

□ If a local device, such as a piece of medical treatment equipment, contains customized settings that are highly important, is there a complete record or backup copy of these customized settings?

INFORMATION BACKUP DEVICES AND PROCESSES

Overview

□ Is there a comprehensive plan covering everything that needs to be backed up?

□ Are the operating systems, programs, and operating information backed up, as well as the data?

□ Is there a special automatic procedure for regularly backing up the contents of employee laptops and mobile devices?

□ Are the configurations of switches and routers backed up on a regular basis?

Harder to Find

□ If backup media containing sensitive information are being transported physically to another location, are the routes and means of transport kept secret?

□ Are the location and nature of the facility where backup media are stored kept secret?

Harder to Penetrate

□ Is the backup regularly transferred to a storage device that is isolated from the organization's primary network?

□ Does the backup procedure include checking the data for hostile code, such as viruses and trojan horses, prior to backing-up the information?

□ Are there sufficiently rigorous procedures to restrict unauthorized physical access to backup media?

□ If the backup copy is sent electronically to a remote system, is the information transmitted to that location through encrypted means or across a dedicated secure network?

□ If the backup copies are being transported physically to a remote location, are they handled by a secure means of transport?

□ Are all of the backup media protected from physical theft during storage, whether they are stored locally or remotely?

Harder to Co-opt

□ If the information being backed up is sensitive or proprietary in nature, is the information encrypted during the backup process, so that it is stored in an encrypted form?

□ Are any encryption keys used in backup stored in a secure location and rotated to ensure that the one compromised key does not expose all the data?

□ Are the encryption keys for the backups, along with a schedule of when and where they were used, stored in a secure form at another location?

□ Is the backup regularly transferred to a physically remote location?

□ If the loss of the backed-up information would jeopardize the enterprise, are there backups stored at more than one remote location?

□ When the backup storage media are no longer needed for backup purposes, are there secure procedures for destroying or reusing those media, whether they are stored locally or remotely?

Harder to Conceal

□ Are the backups regularly tested to ensure that they are readable and uncorrupted?

□ Are the backups randomly tested to ensure that the data has not been modified?

□ If the backup copies are being transported physically to a remote location, are they placed in tamper-proof containers and tracked in transit?

□ Are the protective cases for transporting backup media equipped with global position tracking devices?

□ Are all logs of activity that could have relevance for security backed up frequently and stored in a form that would prevent tampering?

□ Are the log files of application access regularly backed up to a secure location?

□ Are the log files of application access held for a long enough periods, so that any sources of gradual data corruption could be tracked down?

More Reversible

□ Is the data being backed up at a frequency appropriate to its economic value and the rate at which it is being changed?

□ Is there a plan for restoring and reloading the information that has been backed up, as well as for storing it?

□ Are there multiple backups, so that if one is lost or corrupted, the system could still be restored?

□ Are there procedures for dealing with backup data that has become corrupted, especially during a crisis?

□ Are there procedures for dealing with the loss or theft of unencrypted backup tapes that contain proprietary or sensitive information?

□ Is the backup data stored long enough so that there would still be an uncorrupted copy if the data was gradually being corrupted in a hard-to-detect manner over a long period of time?

□ Are crucial backups that have not yet been transferred to a remote location stored and tagged in such a way that they could be easily be taken along in the event of a physical evacuation?

Area Five: Human Users

INDIVIDUAL EMPLOYEE ACTIONS

Overview

Security Accountability

□ Is maintaining the security of the organization made part of each employee's job description?

□ Are all employees required to sign confidentiality and intellectual property agreements and told their practical implications?

□ Is each piece of information equipment the organization owns or leases the explicit responsibility of one designated employee?

□ Are there permanent tags or other identifying markings that make it easy for other employees to determine who "owns" a given piece of information equipment?

□ Is the employee who is responsible for a given piece of information equipment explicitly required to oversee the security of that equipment?

□ When employees are carrying or using their laptops or other portable information equipment outside the workplace, are they trained to keep those devices under watch or in secure places?

□ Do corporate policies define the proper use of e-mail, internet access, and instant messaging by employees?

□ Do corporate policies define the kinds of information about the corporation that can be posed on social media by employees and the kinds of information that should be treated as confidential or proprietary?

□ Are employees made strictly accountable for any actions they carry out on the corporate information system that are in violation of corporate security policies?

General Security Training

□ Are all employees given periodic training on the security policies that are important to the business with sufficient explanations of why these policies are important?

□ Are employees taught what sorts of information handled by the organization should be regarded as sensitive information?

□ Are employees taught how to create imaginary memory personae, so that they have a relatively easy way of remembering passwords and answers to challenge questions that cannot be discovered by researching them on the web?

□ Does the employees' training in security policies include practical exercises in which the employees act out some of the practical implications of these policies?

□ Are all employees periodically tested on their knowledge of security procedures, including their knowledge of newly emerging threats?

□ Are the employees' security behaviors regularly tested in practical ways that will not be easily recognized as tests?

□ When the employees' security behaviors are tested, are they given near-instantaneous feedback that will shape their future behavior? (E.g., does loud, comic music blare out from an employee's computer each time that employee clicks on a trojanized e-mail attachment that was sent as a test?)

Security Reporting

□ Are employees made aware that any time they install a new software application in a computer belonging to the organization, they must report this fact to the organization's cyber-security personnel?

□ Are employees given an easy way to report possible security vulnerabilities and rewarded for doing so?

□ Are employees given adequate incentives to report possible security breaches and bad security behavior, while simultaneously insulated from any blame or retribution for making such reports?

Harder to Find

□ Are employees contractually forbidden from posting information on the internet that would reveal which critical information systems they are able to access?

□ Are employees contractually forbidden from posting information on the internet that would reveal what security measures the organization has put in place?

□ Are employees made aware of the security risks they can incur by storing personal information, especially personal identification information, on their smart phones?

□ Are employees taught a variety of polite ways to say "no" to requests for information relevant to security, even when that information seems relatively innocuous?

Harder to Penetrate

□ Are employees prohibited from using personal identification devices, such as badges and proximity cards, to give other employees access to information facilities and systems?

□ Are employees trained to avoid using passwords constructed out of personal biographical facts that might be publicly accessible?

□ Have employees been trained in the methods for constructing non-dictionary and phrase-based passwords?

□ Are employees made aware of the hazards of storing passwords in insecure places, such as on post-it notes in their work area?

□ Are employees made aware how hazardous it is to plug electronic devices, such as iPods, Kindles, smart phones, and digital cameras, into work computers, even if this is only done to charge the batteries of these devices?

□ Have physical security personnel been taught that preventing unauthorized electronic equipment, including flash drives, from being plugged in inside the organization's facilities is just as important as preventing the theft or vandalism of equipment?

□ Are employees regularly reminded not to open e-mail attachments if the e-mail is generic, seems unlikely, or has unexplained features?

□ Are employees prohibited from installing any software on corporate computers that is personal, recreational, or simply unauthorized?

□ Are employees trained to be suspicious of any software that arrives in the mail, even though it may appear to be packaged and sent by trusted vendors?

□ Are employees made aware that they should never plug in an unlabeled or suspiciously labeled memory device to see what it contains?

□ Are employees regularly reminded not to download file types from the internet that could contain executable code?

□ Have employees been made aware of the fact that mass produced and mass distributed software could still contain targeted malware?

Harder to Co-opt

□ Have the employees been trained not to fall victim to social manipulations by telephone or over the internet that would led them to reveal security-related information?

□ Have the employees been trained never to type or dial specific sequences of numbers or characters when someone they do not know is requesting them to do this?

□ Does the organization restrict employee access to critical systems from unsupervised locations and at unsupervised times?

□ Are areas of responsibility distributed among employees in such a way that a single employee cannot carry out a critical operation without the knowledge of other employees?

□ If a given category of input is sufficiently critical, does the organization require a second employee to verify that input before it is processed?

□ Do extremely critical operations require the active, simultaneous participation of two or more employees?

□ Are information technology employees made aware of how dangerous it is to install network links, such as modems or wireless connections, that are undocumented and not authorized by security personnel, even though these links might be requested by senior executives?

□ Does the organization warn all employees who are leaving the organization that they need to respect the organization's intellectual property?

Harder to Conceal

Security Accountability

□ Are employees prohibited from letting other employees use their work computers?

□ Are employees prohibited from sharing passwords, even with other employees who are authorized to access the same systems?

Employee Monitoring

□ Is there a system for collecting and collating information on which physical facilities and information resources each employee is accessing?

□ Is video surveillance carried out on building maintenance personnel, such as janitors, even in areas that are only moderately sensitive?

□ Are the employees' physical and electronic access logs periodically reviewed to identify access patterns that are not motivated by normal work responsibilities?

□ Are employees prevented from accessing files that would reveal when their behavior is being monitored and whether it has attracted special attention?

□ Are employees required to take periodic vacations, so that ongoing activities they might otherwise be able to conceal would be noticed by their temporary replacements?

□ Are special web searches periodically carried out to discover if employees are improperly posting information that could be useful to cyber attackers?

□ Does the organization begin closely monitoring the data accessed by employees as soon as those employees give notice that they intend to leave the organization?

□ Does the organization review the data accessed by any employees during the ninety days prior to the date they give notice that they intend to leave the organization?

Security Reporting

□ Are various cyber-attack strategies described to employees in enough detail and with enough variations, so that the employees would have a good chance of recognizing the early signs of such attacks?

□ If employees use an internet link supplied to them by another employee or anyone else, are they taught always to check the uniform resource locator (URL) that appears in their browser window to make sure that has an appropriate domain and looks authentic?

□ Are employees provided with an easy way of reporting possible warning signs of a cyber attack and encouraged to do so, even when it seems likely that no actual attack is involved?

□ Are employees made aware that, even though they are expected to make a serious effort to avoid security lapses, occasional lapses are inevitable and can often be made harmless by prompt reporting?

□ Are employees provided with an easy way of reporting potentially bogus phone calls and other possible efforts to obtain information that might be useful in mounting a cyber attack?

More Reversible

□ Does the organization have a prescribed procedure for collecting forensic evidence on any attempts by employees to use the organization's computer systems for theft of information or to cause other harm?

ADMINISTRATIVE ACTIONS

Overview

Senior Management

□ Are the organization's senior managers regularly briefed on the status of the organization's cyber security and the possible consequences of emerging cyber threats?

□ Are the organization's senior managers made aware that good cyber security needs to take account of what the organization's information systems are used to accomplish in business and operational terms?

□ Are the organization's senior managers made aware that the most cost-effective way to deal with many cyber-security issues is not to add more cyber-security measures, but to make small changes in the way operations are carried out?

□ Are the organization's senior managers made aware that dealing with cyber-security issues is usually much easier and much less expensive if these issues are taken into account when new business operations and new information systems are first being planned?

□ Does the organization have a designated Chief Information Security Officer?

□ Is the organization's Chief Information Security Officer periodically required to brief the organization's Chief Financial Officer or its Chief Executive Officer without the presence of anyone else to whom the Chief Information Security Officer might otherwise report?

□ Is the organization constantly using news about the attacks being carried out against other organizations to update its cyber-security plans and programs?

□ Does the organization provide a regular channel through which cyber-security personnel can provide advice and warnings about the cyber-security implications of corporate strategies, policies, practices, and public relations?

□ Are the organization's cyber-security personnel actively rewarded for bringing cyber-security considerations to the attention of managers and other personnel outside the cyber-security department, as long as this is done in an appropriate manner?

Audits and Outside Reviews

□ Are the organization's information security policies and their implementation reviewed annually by an expert outside auditor?

□ Are the organization's information security policies and their implementation carefully checked to verify that the organization is compliant with the regulations and recognized standards for that industry?

□ Is the annual review of the organization's information security policies and their implementation broad enough in scope to uncover information vulnerabilities in the physical facilities?

□ Is the annual review of the organization's information security policies and their implementation broad enough in scope to uncover information vulnerabilities in employee behavior?

□ Are the audits and reviews of the organization's information security examined analytically to identify areas where different or additional counter-measures may be needed?

□ Are the successive audits and reviews of the organization's information security compared, so that senior managers can make sure that the organization's information security is improving, rather than deteriorating?

Security Administration

□ Is there a reliable system for keeping track of all the logs and other sources of information that the security team needs to review and for verifying that they are being dealt with on an appropriate schedule?

□ Is there a reliable, continuously updated system for listing and tracking all of the vulnerabilities noticed by employees, discovered by audits, reported by vendors, or covered in the media?

□ Does the system for tracking vulnerabilities allow security personnel to determine quickly which vulnerabilities are still in need of attention, which vulnerabilities are currently being dealt with, and which vulnerabilities have already been remedied?

□ Are vulnerabilities assigned a priority level, so that more critical vulnerabilities are dealt with more quickly?

□ Does the priority level assigned to vulnerabilities take into account the nature of the business or production operations that are supported by the information systems in which those vulnerabilities occur?

□ Is the system for tracking vulnerabilities co-ordinated with the system for tracking software patches and updates, so that effort is not wasted dealing with the same issues more than once?

□ If an important vulnerability is going to be dealt with by a software patch or update, but not for some time, are temporary measures to reduce the effect of that vulnerability put into place in the meantime?

□ Is there a single designated security manager who is continually checking to make sure that the vulnerabilities are being dealt with in a timely manner and in an order that takes account of their relative priority?

□ Does the Chief Information Security Officer review the security programs and procedures on a monthly basis to make sure that these are staying ahead of security needs, rather than falling behind?

□ Does the work schedule of the security team set aside a significant amount of time for putting new security measures in place and renovating old ones, rather than allowing all the team's time to be taken up with patching vulnerabilities and responding to attacks?

Harder to Find

□ Is the organization's publicity and public relations department made aware that its activities could have a significant impact on the organization's cyber security?

□ Does the organization refrain from publishing advertising and publicity materials that would draw attention to the organization's exact role in critical supply chains, unless there is a compelling business reason to do so?

□ Does the organization refrain from publishing advertising and publicity materials that would reveal the extent of the organization's dependence on key information systems?

□ Does the organization avoid making public statements that would be regarded as provocations by the hacker community, drawing attention to the organization as a possible target?

□ If the organization is an extremely high profile target, do advertisements and notices used for recruiting cyber-security personnel avoid revealing the organization's identity?

Harder to Penetrate

□ Are background checks carried out on employees with higher levels of information access, even though their salaries and job titles might not indicate this level of access?

□ If an employee is promoted to a considerably higher level of responsibility and access, is a new background check carried out?

□ Is background screening carried out for building maintenance personnel with extensive physical access to information system components, such as janitors?

□ If there is a noticeable change in the personal or financial behavior of an employee with access to critical systems, is there a procedure for unobtrusively carrying out a new background check, covering such things as rapid changes in credit ratings or signs of unexplained wealth?

□ If an employee is going through a period of great difficulties in his or her personal life, is there a policy for temporarily reducing that employee's responsibilities for critical systems and access to critical systems?

Harder to Co-opt

□ Are employees monitoring critical systems that seldom change given something to do that will make their jobs less boring?

□ Does the organization make fairness and good faith in the treatment of employees a higher priority than seizing every opportunity to gain a short-term competitive edge?

□ Does the organization make a point of acknowledging, at meetings attended by many other employees, any individual employee working with information systems who has done work that is especially reliable, skillful, or innovative?

□ Does the organization provide a channel through which employees can anonymously nominate other employees or themselves for special recognition, based on work with information systems that is unusually reliable, skillful, or innovative?

□ Does the organization provide adequate mechanisms for employees to express their grievances without penalty and for them to see those grievances being conscientiously addressed?

□ Does the organization handle down-sizings in a manner that minimizes hostile feelings on the part of former employees?

Harder to Conceal

□ Does the organization offer a procedure which would allow employees to report attempts by outsiders to extort their cooperation in circumventing security, without having the basis for that extortion widely revealed or made part of that employee's permanent record?

□ Is an effort made to track the current whereabouts of former employees who were deeply acquainted with critical systems and procedures?

More Reversible

□ If employees with access to competitively important information leave the organization, does the organization check for signs that they are improperly using that information in their new jobs?

SECURITY INCIDENT HANDLING

Overview

□ Does the organization have detailed plans for dealing with security incidents, both while they are underway and immediately after?

□ Do the organization's detailed plans for dealing with security incidents specify the points at which senior managers outside the cyber-security team should be notified?

□ Do employees know where they should turn for operational guidance during a continuing series of cyber attacks?

□ Are exercises periodically conducted in which key employees go through the motions of responding to a cyber attack in a reasonably realistic manner?

□ Have the key personnel been given opportunities to practice their emergency responses in actual simulations?

□ Are both real incidents and exercises followed by after-action discussions directed at identifying the lessons learned?

□ Is the organization constantly using news about the attacks being carried out against other organizations to update its response plans for the attacks it might suffer?

Harder to Find

□ Are the organization's detailed plans for dealing with security incidents kept highly confidential?

□ Are the after-action reports on the organization's security exercises and simulations kept highly confidential?

Harder to Penetrate

□ Do employees know how to quickly interrupt or shut down any channel of communication that is apparently being utilized by a cyber attack?

□ If a particular account is being utilized by the attack, are the account administrators ready to quickly force a log-out of that account and disable that account across the organization's networks?

Harder to Co-opt

□ If there is reason to believe a major cyber attack may be immanent, is there a plan for temporarily cutting back on vulnerable activities and shutting down dispensable communication channels, in order to limit the effects of that attack?

□ If a serious attack has occurred, are there procedures that can be implemented very rapidly that will isolate or quarantine any system that may have been contaminated with malware or false information *without* shutting it down?

□ Are there procedures that can be rapidly employed to *manually* isolate or quarantine each system if there is reason to distrust the computerized procedures for accomplishing this?

□ Are any cables that should be physically unplugged in the event of an attack clearly labeled?

□ Do employees know which cables to unplug in the event of an attack and what events should trigger this response?

□ If an attack is causing data to be deleted or encrypted on a local computer, have employees been authorized to immediately shut off that computer?

□ Are there procedures for rapidly modularizing or compartmentalizing operations and systems beyond those likely to have been affected by the attack, as a further precaution?

□ Are there separate systems or procedures for monitoring each of the systems that has been isolated or quarantined?

□ After the affected systems have been isolated or quarantined, do the procedures for dealing with a serious or sustained cyber attack require the cyber-security team to pause and consider what the attack is probably trying to accomplish before taking further steps to deal with it?

□ Does the procedure for responding to a cyber attack remind the cyber-security team that the observable attack might be intended to cover or distract from another attack?

□ Do employees know how to switch over to alternative channels of communication in the event of normal channels being compromised?

□ Is there a procedure for moving the quarantine lines when better information about the possible contamination becomes available?

Harder to Conceal

□ Do employees know whom they should notify if they are observing symptoms of an apparent cyber attack?

□ Do employees know what additional symptoms or developments should prompt further notifications?

□ Is it standard procedure, in the event of a significant cyber attack, to verify the nature and extent of the attack's effects by direct human communication, rather than relying entirely on automated reports?

□ Are employees with access to highly critical systems or facilities provided with special access codes that would signal that they are acting under duress?

□ Are automated detection systems in place that would raise silent, remote alarms if the duress codes are used?

□ Do the key response personnel know how to collect and preserve the evidence necessary for proper forensic investigations and legal prosecutions?

More Reversible

□ Does the security team know the names, e-mail addresses, and phone numbers of the people outside the organization that the team may need to contact in order to deal with an attack and its effects?

□ If important information systems are shut down as a result of a cyber attack, is it standard procedure to inform employees immediately how long they should plan on operating without those systems?

□ If the automatic procedures for saving documents and data to remote locations will be disrupted as a result of the attack, are employees warned to save these documents and data locally?

□ If there are other information systems that could substitute for the systems that have been shut down or made unreliable as a result of the attack, do employees know how to switch over to them?

□ Do employees know how to go about restoring compromised information systems to their last known good state?

□ Is there a mechanism for retrieving "last known good state" when that state is a considerable time into the past?

□ Are employees trained to handle storage media and by-products securely in the special circumstances produced by disaster recovery?

□ If a potential cyber attack would affect people outside the organization, is the organization's publicity and public relations department prepared to deal with this?

□ If the organization is supplying urgently needed services to regular customers, is there an ordered list of which customers are the highest priority for the restoration of services?

Area Six: Suppliers

PROCEDURES FOR DEVELOPING NEW SOFTWARE

Overview

□ Does the organization have a written policy detailing the steps and procedures for the internal development of software?

□ Does the organization require in-house software developers to have periodic training in secure coding techniques?

□ Does the organization have clear policies regarding the use of open-source software libraries and third-party components in the software it develops?

□ Does the organization maintain an inventory of all open-source or third-party software components it has incorporated into the software it has developed, along with the details of exactly where and how those components were used?

□ Does the organization periodically check whether upgrades or patches are needed to correct bugs or security flaws in the open-source and third-party software components it has incorporated into its software?

□ Does the organization have a system for tracking the upgrades and patches that might be needed for the software it has developed in house, logging all reports of software issues that might need attention, the decisions about the actions to be taken, the dates by which any necessary patches or upgrades were completed, and the dates and methods by which these patches or upgrades were distributed?

Harder to Find

□ Do advertisements for recruiting software developers and programmers avoid revealing the specific nature of the software being developed?

□ If software developers are using websites where developers trade help, do they refrain from revealing their true identify, the organization they are working for, and the intended use of the program they are working on?

□ If developers post pieces of code on websites where developers trade help, do they take care to make sure that the piece of code being posted does not contain any labels or annotations that would reveal the organization it belongs to or its intended operational functions?

□ If developers let other users of websites where developers trade help critique their work or offer suggestions for solving problems they have encountered, are the pieces of program being presented for discussion sufficiently short that shaping their functions will not shape the functions of the larger program being developed?

Harder to Penetrate

□ Do corporate security policies require contractor personnel working on software development to meet minimum security requirements if the software is going to be used for critical processes or highly sensitive information?

□ Are software developers given background checks that are more thorough than those for other employees?

□ Does the organization have procedures for the orderly insertion of code during software production, so that no one has an opportunity to alter a line of code other than the programmer recorded as responsible for it?

□ If software components from third parties are going to be incorporated into libraries or applications under development, are these components examined for vulnerabilities before being accepted?

□ If software components or files from third parties are going to be installed with the program under development, but not actually incorporated into it, is the authenticity of those components and files verified before they are deployed?

□ Are changes to the source code library controlled and monitored, so that the source control module cannot be bypassed by someone with administrator privileges?

□ Is access to the software development tools that utilize code-signing digital certificates limited to authorized developers?

□ Are any user accounts employed for software testing systematically removed before the software is actually put into service?

Harder to Co-opt

□ Does the organization have pre-approved code modules that can be inserted into new software to accomplish standard security functions, such as authentication and encryption?

□ Does the organization have pre-approved code modules for managing file transfers and other communication functions?

□ Does the organization provide developers with dummy data, so that the applications under development do not have to be tried out on private, sensitive, or proprietary information?

□ Are all dummy data used for software testing systematically removed before the software is actually put into service?

□ Are the applications under development tried out in test bed environments that are completely isolated from the actual production environments?

□ If there are embedded comments by developers on the source code that survive the development process, are these comments manually removed before the program is deployed?

Harder to Conceal

□ Does the organization have a system for tracking exactly which employee or outside contributor wrote each line of code for any software produced internally?

□ Are all the programmers working on each software application made aware that records are being kept of exactly who wrote each line of code?

□ Is the use of digital certificates for code-signing of applications under development regularly audited?

□ Does the organization have software vulnerability specialists conduct reviews and tests of the software it has developed, regardless of whether it was outsourced or produced in-house?

□ Do the reviews and tests run on the newly developed software include a search for possible “back doors”?

□ Is stress testing been conducted against the software ports utilized by applications under development to make sure that they are not susceptible to buffer overflows at the software port level?

□ If the application under development is mission critical, is it required to undergo a source code review by an independent third-party**?**

More Reversible

□ Are annotations maintained on each section code as it is being written, so that other developers and security specialists can rapidly understand what a given section is designed to do?

□ Are successive versions of software under development archived, so that it will be possible to return to a last known good version, even if corrupt code was inserted and went undetected for a considerable period of time?

FEATURES TO BUILD INTO NEW SOFTWARE

Overview

□ Are proposed software designs, including plans for the modification or extension of existing software, evaluated from the standpoint of information security by experienced security specialists before the initial versions of that software are created?

□ Are the potential security issues in the software designs evaluated in relation to the software's ease of use and its business functions?

□ Is consideration explicitly given to the possibilities for incorporating security features into the software itself, rather than leaving the relevant security measures to be dealt with after the software is ready to install?

□ Are the software designs approved by the cyber-security team, as well as the software developers and the business managers, before the new software program is actually written?

Harder to Find

□ If the application under development is designed to carry out critical operations, are the functions of the individual program components masked or obfuscated, wherever possible?

□ Are the banners or strings that announce the name and version of the software application designed to be altered or removed when the application is put in service?

□ Is the application under development designed not to expose any unencrypted user or account ID's in the uniform resource locator (URL)?

Harder to Penetrate

Authentication Features

□ Is the application under development designed to require passwords for access that have a minimum and maximum number of characters?

□ Is the application under development designed to require passwords for access that include a mixture of character types and characters chosen from large character sets?

□ Does the application under development automatically reject weak password choices, such as those on the list of commonly used passwords?

□ Is the application under development designed to store only the hashed value of a user's password?

□ If the application under development is sufficiently critical, is it designed to require advanced authentication mechanisms, such as biometrics or two-factor tokens?

Data Management

□ If input fields are being built into the application, are those input fields designed to accept only data written in the appropriate characters?

□ If the application under development will receive data streams from other applications, are the characters accepted in those data streams limited to the ones needed for that type of data, so that other characters that could be used to write executable commands are excluded?

□ If a critically important program is going to call on supplementary files and separate components that are to be installed with the program, is there a mechanism that will automatically check the authenticity of those files and components each time they are used?

□ Is the application under development designed with appropriate buffer bound checking, which disregards any input that is too long?

□ Is the application under development designed to restrict direct memory access, so that buffer lengths can be controlled and enforced?

□ Is the application under development designed to protect sensitive data in memory, such as passwords and cryptographic keys, by locking memory and overwriting the memory location once the sensitive data has been used?

Harder to Co-opt

General Functions

□ Is the application under development designed to request and release resources in a systematic way?

□ Is the application under development designed to limit the demands its operations make on system resources, so that these are not overloaded?

□ If a process within the application under development receives or retrieves information that is not in the form on which the process is designed to operate, is the process given an alternative operation to perform, so that it does not crash?

□ If the application under development is intended to control highly critical or dangerous processes, is it written in a programming language that was designed to avoid type errors, buffer overflows, and other software vulnerabilities, such as Ada or its dialect Spark, rather than a programming language where these problems are chronic, such as C, C++, or Objective-C?

General Privilege Management

□ Is the application under development designed to use the concept of least privilege when executing instructions?

□ Is the application under development designed to have privilege separation during operations?

□ Is the application under development designed to set appropriate permissions on all resident files installed with the application?

□ Is the application under development designed to set appropriate permissions on temporary files?

Data Management

□ Is the application under development designed to create new, random file names for each operation, rather than reuse file names?

□ Is the application under development designed to verify that file writes are only allowed on files using an absolute path to the same disk location**?**

□ Is the application under development designed to write to a directory location that can only be accessed by that application, rather than to a standard temporary directory location (e.g., /tmp)?

□ Is the application under development designed to verify that commands to delete data are only allowed to file and folders using an absolute path to the same disk location**?**

□ Is the application under development designed to erase thoroughly any data generated during intermediate steps in the execution of the program (good garbage collection)?

□ Is the application under development designed to encrypt sensitive information that it stores in a file or database?

□ Is the application under development designed to encrypt sensitive information that it writes to cookies?

Harder to Conceal

□ Is the application under development designed to report to a log file all failed log-in attempts and to send an alert if the number of attempts surpasses a specific threshold?

□ Is the application under development designed to report to a log file all attempts to insert executable commands into input files that should not contain such commands?

□ Is the application under development designed to report to a log file all requests to modify permissions and also to send an alert when these modifications are outside normal parameters?

□ Is the application under development designed to report to a log file all cases where data streams from other applications that include characters that are not normal part of such data?

□ Is the application under development designed to report to a log file all cases in which a supplementary file or separate component installed with the program fails an authenticity test?

More Reversible

□ Is the application under development designed to automatically reinstall supplementary files and separate components from a trusted repository if the authenticity of the current ones cannot be verified?

□ Is the application under development designed to place special items (terminator canaries) in its buffer areas that will trigger an alarm if they are overwritten?

EXTERNAL VENDORS

Overview

□ Does the organization have a written policy detailing the steps and procedures for interacting with software vendors and outside developers?

□ Are all outside vendors or contract personnel contractually required to adhere to the security policies at least as stringent as those maintained by the client organization?

□ Are all outside vendors or contract personnel required to have briefings or training in the security policies of the client organization?

□ Do corporate policies require vendor personnel to sign non-disclosure agreements?

Harder to Find

□ Does the organization contractually require its vendors to abstain from advertising or publishing the fact that the organization is a customer?

□ Does the organization contractually require its vendors to abstain from revealing, even in private settings, exactly which products and services those vendors are supplying?

□ Does the organization periodically verify that its vendors are not advertising or publishing the fact that the organization is a customer?

Harder to Penetrate

□ Do the service agreements require vendors to conduct background checks on their personnel before they are assigned to the corporate account?

□ If a software application was supplied by a third-party vendor, can the vendor demonstrate that precautions were taken to make sure that the application does not have backdoors that allow third-party access?

□ Are physical shipments from external vendors protected by tamper-resistant packaging?

□ Is there a regular procedure for verifying over the internet or by telephone that any physical shipment from the vendor is an authentic one?

□ Are there trusted channels for receiving updates from each software vendor?

□ Are there appropriate limitations and an expiry date on the access rights that the vendors need in order to install the software and updates?

□ Does the organization have processes in place to restrict internal information access by outside vendors or contractors?

□ Does the organization have processes established to identify and terminate vendor, contractor, and other outsourced personnel access when no longer required?

Harder to Co-opt

□ Are prospective software vendors and outside developers limited to those who can be verified to meet industry standards for information security?

□ Are software vendors required to keep records of which employee or outside contributor wrote each line of code for any software being purchased?

□ Are software vendors required to certify that their code has undergone a rigorous and thorough security inspection before it is delivered for deployment?

□ Do vendors provide physical shipments with packaging and labels that are difficult to counterfeit or tamper with?

□ If a vendor is sending out software, updates, or patches, does it post hashes of these software products on its website, so that the integrity of these products can be verified?

□ When software updates need to be applied, is there a guarantee that those updates were adequately tested in the relevant kind of software environment before being installed?

□ Are there procedures for verifying that copies of proprietary information were destroyed after the vendors delivered the contracted software?

Harder to Conceal

□ Are the vendors' physical comings and goings inside the organization's facilities logged and monitored?

□ Does the organization scan all laptops that are temporarily connected to the corporate network by outside vendors and contractors to verify that they are free of standard hacking tools?

□ Does the organization have processes established to monitor electronic activities carried out by outside vendors or contractors from *inside* the organization's facilities?

□ Does the organization have processes established to monitor electronic activities carried out by outside vendors or contractors from *outside* the organization's facilities?

□ Are steps regularly taken to verify that access rights for past vendors and contractors were, in fact, eliminated as soon as they were no longer necessary?

□ Are the actions of former vendors or contractors who handled critical information or critical systems monitored for non-compliances with non-disclosure agreements?

More Reversible

□ Are software vendors required to make escrow arrangements for the preservation and protection of the source code used in the applications being purchased or licensed?