

# The US-CCU Cyber-Security Check List

By

**John Bumgarner and Scott Borg**

**FINAL VERSION**

**2007**



© 2006-2007 U.S. Cyber Consequences Unit

This cyber-security check list is being made available for free, but it is copyrighted, and it may not be sold nor resold in another form without the express permission of the U.S. Cyber Consequences Unit, a non-profit research institute.

Those using this list should note that no cyber-security check list is completely foolproof, and that the defensive measures enumerated in this check list could, in principle, be circumvented. The U.S. Cyber Consequences Unit cannot accept responsibility for the consequences of implementing this check list, nor for any errors that the check list might contain.

It is the intention of the U.S. Cyber Consequences Unit to update this check list annually. Suggestions for improvements would be very welcome and should be addressed to: [checklist\\_comments@usccu.us](mailto:checklist_comments@usccu.us)

To those who have offered suggestions after reviewing earlier draft versions, the authors are profoundly grateful.

## THE US-CCU CYBER-SECURITY CHECK LIST

BY JOHN BUMGARNER AND SCOTT BORG

This check list is intended as a comprehensive survey of the steps that corporations and other organizations should take to reduce their vulnerability to cyber-attacks. The basis for this list is the large number of real-life cyber-security vulnerabilities uncovered in the course of their work by John Bumgarner, the Research Director for Security Technology at the U.S. Cyber Consequences Unit, and Scott Borg, the Director of the U.S. Cyber Consequences Unit. It was only after this list was beginning to approach its present length that the authors consulted previous cyber-security check lists to make sure that all the more relevant topics on those lists were being encompassed by the new effort. Preliminary drafts of the new check list were then circulated among large numbers of cyber-security professionals, and hundreds of comments were collected. By incorporating all of the more practical suggestions that emerged into one comprehensive document, the authors have tried to provide a fairly complete map of the existing cyber-attack avenues and the measures needed to protect them.

To make the check list's organization as clear and intuitive as possible, the vulnerabilities and counter-measures have been sorted according to six easy-to-distinguish categories of information system components: 1) hardware, 2) software, 3) networks, 4) automation, 5) humans, and 6) suppliers.

A few further points should help make clear how these categories are applied. Software vulnerabilities are really software *access* vulnerabilities, since after software has been produced, verified, and installed, it needs to be accessed by someone to become a security hazard. Software supply vulnerabilities need to be treated as an integral part of an information system's vulnerabilities, since software suppliers are regularly interacting with information systems long after the initial sale or licensing of the software. Other kinds of suppliers do not generally need to be treated as information system vulnerabilities, since they are not really an ongoing participant in the information system's operations. Automation vulnerabilities encompass not just all of the systems that mediate between information processes and physical processes, but also *any* automatic processes that produce physical products. Since virtually every information system produces at least one physical product—its own backup media—automation vulnerabilities are important not just for physical industries, but for all information systems.

Each of the main areas in which cyber-attacks could take place has been subdivided further into two or more attack avenues. These narrower attack avenues are organized according to the activities that need to be carried out or overseen in order to maintain the security of those information system components. This leads to sixteen avenues, organized according to the following chart.

<b>OVERVIEW OF MAJOR CYBER-ATTACK AVENUES</b>
<b>Area One: Hardware Vulnerabilities</b>
Avenue 1: Physical Equipment
Avenue 2: Physical Environment
Avenue 3: Physical By-Products
<b>Area Two: Software Access Vulnerabilities</b>
Avenue 4: Identity Authentication
Avenue 5: Application Privileges
Avenue 6: Input Validation
Avenue 7: Appropriate Behavior Patterns
<b>Area Three: Network Vulnerabilities</b>
Avenue 8: Permanent Network Connections
Avenue 9: Intermittent Network Connections
Avenue 10: Network Maintenance
<b>Area Four: Automation Vulnerabilities</b>
Avenue 11: Remote Sensors and Control Systems
Avenue 12: Backup Procedures
<b>Area Five: Human Operator Vulnerabilities</b>
Avenue 13: Human Maintenance of Security Procedures
Avenue 14: Intentional Actions Threatening Security
<b>Area Six: Software Supply Vulnerabilities</b>
Avenue 15: Internal Policies for Software Development
Avenue 16: Policies for Dealing with External Vendors

Within the sixteen avenues, there are further headings that group the counter-measures used to protect those attack avenues. All of the individual vulnerabilities in the check list are described in terms of the counter-measures that should be taken to eliminate or minimize them. A question format has been used, so that an auditor checking the item will know that the appropriate measures have been taken if the answer to the question is “yes.” The words in some of the questions that might sound imprecise, such as “strict,” “rigorous,” “adequate,” and “sufficient,” actually have fairly precise meanings in the contexts where they are applied. In most cases, to interpret these terms properly, it is only necessary to ask “what is this counter-measure intended to accomplish?” and then to see whether the measures taken are adequate for accomplishing that purpose.

Great care has been taken to avoid the currently fashionable catch phrases and to keep technical jargon to a minimum. Instead, every effort has been made to say what is meant as clearly and plainly as is consistent with brevity. If someone is looking for a cyber-security issue identified by some currently trendy buzz-words, it will almost always be here, but the buzz words themselves will not be.

Many questions about “corporate policies” and “verifications” have been intentionally omitted from this check list on the grounds that these points should usually be taken for granted. *Every* security measure included in this check list should be carried out as a matter of corporate policy. *Every* security measure included in this check list should be subjected to some kind of verification. The point is to make sure that the security measures on the check list are actually being carried out. Policies and verifications are merely auxiliary devices for achieving this. Where the check list *does* explicitly mention “corporate policies” or “verifications,” the issue in question is one where special procedures need to be instituted. Ordinarily, the basic principles of good management will imply the necessary policies and verifications.

The administrative and organizational arrangements necessary for implementing good cyber-security practices have also been largely omitted from this check list. This is because these arrangements involve the effective deployment of roles, responsibilities, incentives, and chains of command, all of which are general management practices, not practices specific to cyber-security. Some principles and guidelines for the administration of cyber-security policies have been laid out in other documents produced by the U.S. Cyber Consequences Unit. But there are actually many different administrative arrangements that can be employed to implement the same cyber-security measures.

Although the document refers throughout to “corporations” and to “business,” these terms should be interpreted very broadly. Any organization that has a budget and

information systems and attempts to carry out practical activities can be treated as a “corporation” for purposes of cyber-security. That includes government departments and agencies, non-profit corporations, and most other non-governmental organizations as well. The “business” these organizations carry out could be any activities that create or deliver value, regardless of whether this value is ever assessed or described in monetary terms. The reason for choosing the term “corporation” is simply that the greatest portion of the nation’s information systems are owned and managed by corporations.

Many corporations will find that not all of the questions in the check list apply to their information systems. Some corporations, for example, will not be operating the sorts of remote sensors and control systems that are the focus of most of the questions listed under Avenue 11. Other corporations will find that it isn’t practical for them to maintain the kind of physically separate data center mentioned in many of the questions. Still other corporations will find that they have no systems that are so extremely critical as to warrant the most elaborate security measures described in the check list. Before declaring an item “non-applicable,” however, a corporation should make sure that the item is not pointing to an over-looked vulnerability. Features of an information system that are not conspicuous in a particular industry can still represent a major security vulnerability for that industry.

The counter-measures marked with an asterisk \* are currently very difficult or very expensive to implement with the products and technologies routinely available from commercial vendors. This means that, for the time being at least, they require special initiatives, ranging from improvised hardware to the commissioning of custom programming. Security vendors, government agencies, and institutions funding security R&D should take special note of these asterisked items. They are all places where new product features or new services for improving information security are urgently needed.

In situations where this US-CCU check list is used as a standard for information security compliance, the asterisked items should be treated as optional. Over the coming months and years, as new technologies, products, and services become available and the check list is periodically updated, many of the asterisks will undoubtedly be removed, and items that are currently optional will gradually become part of standard security practices. In the meantime, it is not practical to expect corporations to tackle security issues where standard solutions are not routinely on offer, even though these issues may be very important ones.

Some of the check list items that are *not* marked with an asterisk may sound difficult or expensive to implement, but in most cases this is an illusion. It is true that there are some very expensive ways to go about tackling these vulnerabilities and some very expensive products on offer for dealing with them. But for virtually all of the items

without an asterisk, there are also relatively inexpensive ways to go about satisfying that security requirement.

If cyber-security is described in terms of a “risk triangle,” where the three corners are threats, consequences, and vulnerabilities, this check list deals only with vulnerabilities. To apply this check list in a cost-effective manner, it is necessary to take account of the *other* corners of the risk triangle. This means understanding the threats enough to have some idea of what kinds of attacks to expect over a given period of time. Even more important, it means understanding the consequences enough to know how critical the various software applications are, how sensitive the various kinds of information are, and what sort of security expenditures are justifiable to protect each of these. Although these subjects are outside the scope of the cyber-security check list itself, they are explained at some length in the main text of Scott Borg’s (forthcoming) book-length report *Cyber-Attacks: A Handbook for Understanding the Economic and Strategic Risks*.

This US-CCU Cyber-Security Check List is *not* intended to replace all previous vulnerability check lists or to make other lists unnecessary. In fact, to implement this overview list, it will generally be necessary to employ additional, specialized check lists that provide more detail on specific security problems, on the latest technical developments, and on the special requirements of individual industries. It is hoped, however, that this US-CCU list will help draw attention to many vulnerabilities that might otherwise be overlooked.

## **Area One: Hardware Vulnerabilities**

### **Avenue 1: Physical Equipment**

#### **Tracking Physical Equipment**

- 1.01. Does the corporation maintain an accurate inventory of the electronic equipment housed in each room at each physical location?
- 1.02. Is there a quick and easy procedure for updating this inventory, whenever an employee with responsibility for a piece of equipment authorizes it to be moved?
- 1.03. Is each piece of electronic equipment labeled with a bar code or other identifier for easy tracking?
- 1.04. If information equipment is sufficiently sensitive, is it tagged with radio frequency identification (RFID) chips, so that its movements can be traced almost in real time? \*

- 1.05. Is there an explicit policy specifying what kinds of equipment can be taken off the corporate premises and what authorizations are required to remove it?
- 1.06. If electronic equipment needs to be taken off the corporate premises, is there an efficient procedure for tracking the movement of that equipment?
- 1.07. Are unannounced spot checks periodically carried out to verify that the electronic equipment is present at the locations designated in the equipment inventory?

### **Guarding Physical Equipment**

- 1.08. Are especially important pieces of electronic equipment consolidated into data centers for easier protection?
- 1.09. Are there physical security barriers established to protect electronic equipment from theft or malicious damage?
- 1.10. If external hard drives and other external data storage devices contain sensitive information and would be easy to carry off, are they anchored down as an extra security precaution? \*
- 1.11. Are wiring closets securely locked at all times?
- 1.12. Are the data center and wiring closets equipped with intrusion alarms?
- 1.13. Are the intrusion alarms for the data center and wiring closets monitored offsite?
- 1.14. Is physical access to the console interfaces of security appliances, such those used to manage firewalls and intrusion detection systems, restricted to authorized users?
- 1.15. 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?

### **Protecting Electronic Access Ports**

- 1.16. Are unused network access ports physically disabled by network switches or physical security barriers to prevent unauthorized access?
- 1.17. Where the network ports are not actually disabled, are there procedures to monitor for unauthorized access to these ports?
- 1.18. Are there physical security barriers, such as locked covers or plugs, established to protect all of the system's media access points (e.g., USB ports, CD drives, etc.)? \*
- 1.19. Where the media ports are not actually disabled, are there procedures to monitor for unauthorized access to these ports? \*

- 1.20. Is the physical access to all unused ports on network switches disabled, especially the Switched Port Analyzer (SPAN) port?
- 1.21. Is the physical access to all console and auxiliary ports on routers protected?

**Protecting Communication Lines**

- 1.22. Are physical security barriers established to protect the network cables running to and from the system, so that they cannot be easily severed or damaged?
- 1.23. Are the critical communication cables and cable harnesses inside the corporation's facilities laid out in a way that makes it difficult to access them physically for the purpose of intercepting transmissions?
- 1.24. Is there physical protection at the demarc point where telephone and data cables enter the building?
- 1.25. Does the corporation investigate the physical security practices of internet service providers and other communication companies before choosing which companies to buy services from?

**Controlling How Equipment Is Physically Accessed**

- 1.26. Is the data center securely locked at all times, with doors at ingress points kept closed?
- 1.27. Does the data center have "restricted area" signs on the ingress doors?
- 1.28. Is access to the data center controlled with technologies such as scannable badges, smart cards, proximity cards, biometrics, or locks requiring personal combinations?
- 1.29. Are the logs for the access control mechanisms (e.g., key cards and video surveillance logs) reviewed on a regular basis?
- 1.30. Does this review include an analysis of failed physical access attempts?
- 1.31. Is video surveillance used to monitor ingress portals for data centers and other areas housing information processing equipment?
- 1.32. If there is video surveillance of the data centers, is it monitored off-site?
- 1.33. If there is video surveillance of the data centers, is the video recorded in a permanent medium that prevents tampering?
- 1.34. If there is video surveillance of the data centers, 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?
- 1.35. If security cameras, especially wireless ones, are used for monitoring, are they protected from jamming, unauthorized viewing, and the spoofing of images? \*

- 1.36. Is access to the management consoles of security components, such as firewalls and IDS, physically restricted to authorized users?
- 1.37. Is physical access to all wireless and infrared uplinks controlled and monitored?
- 1.38. Are fax machines that receive and print sensitive information protected against unauthorized access?

### **Controlling Which Personnel Have Physical Access**

- 1.39. Are there controls on who goes in and out of the larger physical facility in which the information systems operate?
- 1.40. Are there clear and rigorously enforced restrictions on which employees have access to the data center?
- 1.41. Are there clear rules and strict controls on access to the wiring closets?
- 1.42. Are there strict controls to modify physical access privileges when an employee's role changes?
- 1.43. Are physical access privileges and devices such as badges immediately deactivated when an employee is terminated, leaves, or retires?
- 1.44. Are there strict controls on vendor access to the data center, so that only properly authorized vendor personnel are admitted?
- 1.45. Does the data center have a sign-in procedure that is used to log non-employees into the restricted space?
- 1.46. Are physical access privileges and devices for vendors frequently reviewed and promptly deactivated when there are changes in the status of vendor personnel?
- 1.47. Are there strict policies outlining the procedures for after hours access to the data center by personnel such as custodians?
- 1.48. Do corporate security policies outline emergency access to the data center?

## **Avenue 2: Physical Environment**

### **Environmental Controls**

- 2.01. Do environmental controls exist, such as heating and cooling systems, which can maintain a consistent operating temperature for the electronic equipment?
- 2.02. Is the electronic equipment protected from moisture or excessive humidity?
- 2.03. If the environmental controls can be managed remotely, are these controls adequately protected from unauthorized access?
- 2.04. Do environmental controls exist that can protect the system from elements other than temperature and humidity, such as smoke, dust, and chemical fumes?
- 2.05. Are there environmental sensors, especially for temperature, smoke, and moisture, in the data center and in the wiring closets?

- 2.06. Are the areas where electronic equipment is housed equipped with a fire suppression system appropriate for electrical equipment?
- 2.07. Are there fire suppression systems that can control fire outbreaks in the areas adjoining those that house the electronic equipment?

### **Power Supply**

- 2.08. Are emergency power shut-off switches conspicuously labeled, monitored by video, and covered by safety panels to prevent the electric power from being inappropriately interrupted?
- 2.09. 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?
- 2.10. Have measures been taken to prevent the connecting power cables farther away from the data center from passing through readily identifiable, insecure locations?
- 2.11. Are electrical supply components, such as power panels and breaker boxes, protected from unauthorized access?
- 2.12. If uninterrupted power supplies (UPS's) are being utilized, are these protected from authorized remote access?
- 2.13. If the systems are sufficiently critical, are they connected to electric power by two different connection routes?
- 2.14. Are back-up generators protected with security devices, such as locks, alarms, and fences with barbed wire?
- 2.15. Is there an adequate backup power supply, especially for any system critical to the business's overall survivability?
- 2.16. Does the backup power supply have ample fuel for a fairly long interruption in fuel supply chain?
- 2.17. Is the backup power supply regularly tested under a full load and run for long enough periods to verify that everything is in working order?
- 2.18. Is the backup power supply in a location that is not susceptible to flooding?
- 2.19. Is there protection against extreme power surges of the sort that could be produced by lightning or, possibly, by artificial means.

### **Physical Defense**

- 2.20. 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?

- 2.21. Are the critical computer and communication facilities a sufficient distance from public parking places, streets, and other locations where a bomb could be easily detonated?
- 2.22. Is critical computer and communication equipment kept away from ordinary windows, which could provide a channel for thrown or projectile bombs, gunfire, or microwave weaponry?
- 2.23. Are backup generators a sufficient distance from public parking places, streets, and other locations where a bomb could be easily detonated?
- 2.24. 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 non-nuclear electro-magnetic pulse attacks? \*
- 2.25. 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?
- 2.26. 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?

### **Avenue 3: Physical By-Products**

- 3.01. Are documents that contain sensitive information protected from printing if there is no operational need for those documents to be printed? \*
- 3.02. Are there sufficiently rigorous procedures to restrict unauthorized access to paper printouts that contain sensitive information?
- 3.03. Do corporate security policies define the type of storage containers that can be used to house paper printouts that contain sensitive information?
- 3.04. Are there sufficiently rigorous procedures for the secure destruction of paper printouts?
- 3.05. Has care been taken to make sure that paper re-use and recycling programs do not undermine other secure handling of paper printouts?
- 3.06. Are there sufficiently rigorous policies and procedures governing the use of removable magnetic media, such as universal serial bus (USB) devices?
- 3.07. Are there sufficiently rigorous procedures to restrict unauthorized access to backup media?
- 3.08. Are there sufficiently rigorous procedures for properly inventorying CD-ROM disks and removable magnetic media that store sensitive information?
- 3.09. Is there a set procedure for documenting the removal of items from the inventory of storage media, so that the employees responsible verify first that the

media have been removed for disposal, second that they have been properly destroyed or sanitized, and third that the physical remnants have been physically released?

- 3.10. Are there sufficiently rigorous procedures for properly shipping any removable data storage devices that need to be moved to offsite locations?
- 3.11. Are there regular procedures to make sure that memory media, such as hard drives, tapes, flash drives, and zip disks, are thoroughly overwritten before they are reassigned to different business uses?
- 3.12. Are there sufficiently rigorous procedures for the secure destruction or sanitation of memory media, such as hard drives, tapes, flash drives, and zip disks, when they are taken out of business service?
- 3.13. Are there sufficiently rigorous procedures for sanitizing memory media being returned for warranty replacement, publicly sold, or donated for charitable use?
- 3.14. Are used CD-ROM disks containing sensitive information adequately destroyed (not just broken) prior to disposal?

## **Area Two: Software Access Vulnerabilities**

### **Avenue 4: Identity Authentication**

#### **Authentication Policies**

- 4.01. Are information systems protected with basic authentication mechanisms, such as username and password?
- 4.02. Is each user's access to applications on the system restricted to those applications that are necessary and appropriate for that user?
- 4.03. If an application allows access to sensitive information, does it require an additional user authentication?
- 4.04. 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?
- 4.05. 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?
- 4.06. If a critical system can be accessed remotely via one or more of these authentication mechanisms, is the link itself dedicated or encrypted?
- 4.07. If advanced authentication is used as an access mechanism, is this technology applied in a consistent and effective way throughout the enterprise?

- 4.08. Is there a procedure for rapidly revoking the privileges for two-factor tokens and smart cards, if they become compromised?
- 4.09. 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? \*
- 4.10. If biometrics are employed, is a pin number also required to verify identity?
- 4.11. If biometrics are employed, are live-scans or other measurements taken to help verify that the readings are being taken from a live person? \*
- 4.12. If it becomes necessary, does the corporation have a way of accessing data and applications ordinarily protected by personal two factor authentications, such as biometric authentication? \*

#### **Monitoring of Access and Access Attempts**

- 4.13. Do corporate policies require that all access attempts be logged, regardless of whether they are successful or unsuccessful, especially for applications that perform critical functions or store sensitive information?
- 4.14. Are all changes that a systems administrator makes to passwords logged and reviewed?
- 4.15. Are all increases in access privileges logged and reviewed?
- 4.16. Is there an alarm mechanism that would warn if the general root-level or administrator-level (e.g., domain administrator) account is utilized?
- 4.17. Are all access logs written to a non-rewriteable disk or other permanent medium where even the systems administrator cannot tamper with them? \*
- 4.18. Are successful authentications reviewed to make sure that the access was proper and appropriate?
- 4.19. Is an effort made to identify and investigate successful access attempts that are carried out at unusual hours of the day or night?
- 4.20. Are multiple failed attempts to access applications reviewed in a timely manner?
- 4.21. Are there automatic alarms and defensive actions designed to counter brute force attacks against the log-in mechanisms, and triggered by multiple log-in attempts, even if distributed across time or across user ID's?

#### **Management of Passwords and Biometrics**

- 4.22. Do corporate policies require secure procedures for issuing passwords?
- 4.23. Do corporate policies define minimum password length requirements, taking account of the user's role and what length passwords the systems in question will support?

- 4.24. Are applications developed within the organization protected with passwords that have a minimum and maximum number of characters?
- 4.25. Do corporate policies mandate password complexity requirements, requiring a mixture of character types or characters chosen from large character sets?
- 4.26. Is care taken to be sure that passwords are not transmitted in clear text through e-mail or instant messaging?
- 4.27. Are employees required to change their passwords on a routine schedule mandated by corporate policy?
- 4.28. Are employees prevented from using previous passwords when a scheduled password change is required?
- 4.29. Do corporate policies mandate adequate password requirements for networking equipment, such as routers and switches?
- 4.30. Have measures been taken to prevent someone from obtaining passwords by theft of an encrypted or unencrypted file in which they are stored?
- 4.31. Is there an alarm mechanism that would warn of the theft of a file in which passwords are stored? \*
- 4.32. Is there a procedure for rapidly and securely changing passwords if there is any reason to believe they may have been compromised?
- 4.33. Do corporate security policies mandate the immediate deactivation of passwords when an employee is terminated, leaves, or retires?
- 4.34. Are servers and work station applications periodically audited 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?
- 4.35. 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?
- 4.36. Once a user's biometric information is captured, is it stored in a secure location that prevents tampering or theft?
- 4.37. Does the corporation and its vendors have a plan for replacing compromised biometric information with alternative information? \*
- 4.38. Do corporate policies define the procedures for dealing with the destruction of biometric information when no longer required?

#### **Management of Encryption Keys and Digital Certificates**

- 4.39. Are encryption keys created in a secure manner, using approved industry methods?
- 4.40. Are decryption procedures activated separately from log-in procedures and required to use different passwords?

- 4.41. Is the generation of encryption keys logged in a tamper-proof file that records the generating employee's identity and the time?
- 4.42. Are encryption keys and digital certificates distributed in a secure manner that prevents theft?
- 4.43. Are encryption keys stored in a secure manner, using approved industry methods?
- 4.44. Are encryption keys destroyed in a secure manner, using approved industry methods?
- 4.45. Is there a quick and effective procedure for dealing with compromised encryption keys?
- 4.46. Are there regular and reliable procedures for the archiving of private encryption keys and associated pass phrases for individual users?
- 4.47. If private encryption keys are maintained, are they archived in a password protected and encrypted area to prevent tampering or theft?
- 4.48. Are archives of private encryption and associated pass phrases keys maintained after they are no longer in active use, so previously encrypted files can be retrieved if necessary?
- 4.49. Do corporate policies define the procedures for deploying digital certificate-based authentication mechanisms?
- 4.50. Are copies of the private keys of digital certificates stored in a password protected and encrypted area that allows recovery and prevents theft?
- 4.51. Do systems that have certificates installed have adequate security measures that prevent the theft of the private keys of these certificates?
- 4.52. Is there a procedure in place that will allow compromised private keys of digital certificates to be rapidly revoked?
- 4.53. Do encryption keys and digital certificates have expiration periods?

**Management of Document Authenticity**

- 4.54. Are documents that present the corporation's works or positions converted into formats that cannot be easily modified, before they are circulated electronically outside the corporation?
- 4.55. Are documents digitally signed when they are converted into formats that cannot be easily modified?
- 4.56. Are the digital signatures on important documents regularly checked to verify that the documents were actually created by the person they appear to be from?

- 4.57. Are important e-mails sent using an application that hashes their contents and adds a digital signature, so that the e-mails' contents and their sender's identity cannot easily be falsified?
- 4.58. Are receipts for important e-mails collected and stored to provide a record verifying that they reached the addressees?

## **Avenue 5: Application Privileges**

### **Customizing of Privileges**

- 5.01. Are the default security settings changed on software and hardware devices before these devices are put into operation?
- 5.02. Has the corporation formally assigned criticality classifications to its more important or more widely used software applications?
- 5.03. Is access to critical applications restricted to those users within the corporation who actually need to use those applications?
- 5.04. Has the corporation formally assigned sensitivity classifications to its information files?
- 5.05. Is access to sensitive data restricted to those users within the corporation who actually need to use that data?
- 5.06. Is the ability to alter or input data into documents or data bases restricted to those employees who would have a valid need to do so in the course of their normal work?
- 5.07. 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?
- 5.08. Are root-level and administrator-level privileges restricted to those who actually have need for those privileges?
- 5.09. Are root-level and administrator-level privileges controlled and audited?
- 5.10. Is there a documented approval process for giving people access to virtual private networks?
- 5.11. Is there a documented approval process for giving people remote access to modems?
- 5.12. Is there a procedure for documenting and tracking which privileges are active for each individual employee?
- 5.13. Are the software application privileges for individual employees reviewed and revised whenever there is a substantial change in their work assignments?
- 5.14. Is there a procedure for removing and verifying the removal of privileges when they are no longer needed?

### **General Control of Privileges**

- 5.15. Are employees prevented from saving sensitive information to local storage devices, such as floppies, CD-ROM's, or USB drives, except in cases where business needs require this? \*
- 5.16. Are applications monitored to determine if sensitive information is being printed, saved, or downloaded without due cause? \*
- 5.17. Are locally stored critical data files normally kept in an encrypted form when not in use? \*
- 5.18. Can a valid user improperly upload or download sensitive data files from the system to another system?
- 5.19. Are all uploads of sensitive data files monitored and logged?
- 5.20. Are all uploads of encrypted data files monitored and logged?
- 5.21. Are there provisions to prevent valid users from downloading executable files to their system without these files first being scanned for malware?
- 5.22. If employees can save sensitive information to a local drive, is this action monitored and logged? \*
- 5.23. Can a valid user access restricted resources on other systems without additional passwords and/or validation by IP address?
- 5.24. 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 the general public?

### **Avenue 6: Input Validation**

- 6.01. Are the characters typed into password fields masked, so that they can't be read by bystanders?
- 6.02. Is there a program checking passwords when they are created to make sure that they meet the requirements for passwords specified in the corporate security policies?
- 6.03. Are all input fields in an application restricted to the appropriate characters and expressions? (E.g., a Social Security Number field should not allow anything but numerals and dashes.)
- 6.04. Are all input fields in an application restricted to an appropriate minimum and maximum length? (E.g., a Social Security Number field should only allow nine numerals.)
- 6.05. Are the limitations on what can be written into the input fields sufficiently restrictive, so that these fields will not accept executable instructions?

- 6.06. Are there limitations on the data fields for the data base that correspond to the limitations in the fields on the user interface, so that improper data and executable instructions are not inserted directly into the data base?
- 6.07. Are data fields that would rarely need to be changed made “read only” as soon as the data entry is verified as correct?
- 6.08. 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?
- 6.09. Have the error messages been properly designed, so that they do not reveal information about the internal design and configuration of the software?
- 6.10. Have debugging features been disabled, so that they do not provide an avenue for obtaining information about the internal design and configuration of the software?
- 6.11. Are the service ports for critical applications configured to filter out data that is outside the proper operating parameters for those applications? \*
- 6.12. Has stress testing been conducted against the service ports that are utilized by critical applications to make sure that they are not susceptible to buffer overflows at the service port level?
- 6.13. 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? \*

#### **Avenue 7: Appropriate Behavior Patterns**

- 7.01. 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? \*
- 7.02. 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? \*
- 7.03. Is there an alarm mechanism that warns if internet business transactions involve unusual combinations of customer identities, billing addresses, and shipping addresses? \*
- 7.04. 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? \*
- 7.05. Is an effort made to identify and investigate successful access attempts that are carried out at unusual hours of the day or night, when computers could carry out unauthorized processes unobserved? \*

- 7.06. Is there any provision for detecting situations in which bogus data or instructions are being inserted without detectable intrusions? \*
- 7.07. Is the data base designed so that sensitive information cannot be over-written, without successive, time-stamped revisions being securely archived? \*
- 7.08. Is there a mechanism for monitoring and logging all changes to critical data bases?
- 7.09. Is the log of changes made to critical data bases regularly analyzed for unusual access patterns, including unusual access times and frequencies? \*
- 7.10. If logging of data change has been implemented, is the log regularly analyzed for any unusual alteration patterns in data bases? \*
- 7.11. Are system and security logs maintained in a way that prevents them from being modified or deleted after they have been stored?
- 7.12. Does the system contain honey tokens, consisting of fake documents or fake accounts with mechanisms for logging whether and when they are accessed? \*
- 7.13. Is there an automatic process for monitoring systems for signs that false information may have been inserted? \*
- 7.14. Is there an automatic mechanism that quarantines systems which may have been contaminated with false information without shutting them down? \*

### **Area Three: Network Vulnerabilities**

#### **Avenue 8: Permanent Network Connections**

##### **Network Connection Integrity**

- 8.01. Is the network itself secured by authentication procedures in addition to the securing of systems on the network?
- 8.02. Have measures been taken to prevent unauthorized systems from being easily connected to the network?
- 8.03. Is the network traffic regularly monitored to establish normal usage patterns?
- 8.04. Is the network traffic regularly monitored for covert communication channels?
- 8.05. 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?
- 8.06. Do critical systems have redundant communication connections?
- 8.07. Do any networks that are extremely critical have redundancy in the switching fabric?

- 8.08. If sensitive information is transmitted across the network, into the network, or out of the network, are the transmissions protected from eavesdropping or modification during transit by encryption?
- 8.09. Do corporate policies define what type of data communications should be encrypted and which encryption technologies should be employed?
- 8.10. Are virtual private network connections being utilized to provide secure communications with partner networks?
- 8.11. Have security requirements been established for non-encrypted network connections to outside partner networks?
- 8.12. If wired or wireless Voice over IP (VoIP) is employed for highly sensitive communications, is the transmission encrypted?

### **Network Component Integrity**

- 8.13. 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?
- 8.14. 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? \*
- 8.15. Have legitimate systems that do not require wider network connectivity been kept off the wider networks?
- 8.16. Is the network regularly checked for unauthorized systems?
- 8.17. If software-based Voice over IP phones are used for sensitive communications, are the systems secure from voice loggers? \*
- 8.18. 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?
- 8.19. Is there a mechanism to automatically restart critical components, such as web server applications, whenever other applications are repeatedly unable to connect with them and to inform the system operator that this was done?
- 8.20. Do critical systems use redundant domain name system (DNS) servers to lessen the affect due to interruptions of that service from one source?
- 8.21. Are measures taken to monitor domain name system (DNS) servers for attacks that reroute requests to unauthorized locations?
- 8.22. Are vulnerability scans or penetration tests performed on critical systems before they are connected to the corporate networks?

- 8.23. Are vulnerability scans or penetration tests regularly performed on critical systems inside the corporate networks?
- 8.24. Are vulnerability scans or penetration tests performed on all internet facing or customer facing systems and applications before they are placed on the network?
- 8.25. Are vulnerability scans or penetration tests regularly performed on all internet facing or customer facing systems and applications that are connected to the network?

### **Wireless Connections and Modems**

- 8.26. Are there clear and rigorously enforced rules for establishing and using wireless connections to the internal networks?
- 8.27. Is a wireless analyzer periodically run to identify any unauthorized wireless devices that may have been connected to the network?
- 8.28. Are infrared, Bluetooth, and wireless links on printers disabled when not required for business functions?
- 8.29. If a wireless technology, such as a wireless local access network (LAN), Bluetooth, or wireless USB, is used for sensitive information; do the connections provided employ strong encryption technologies?
- 8.30. Are the default PIN's for Bluetooth devices changed before they are put into service?
- 8.31. If wireless technology is used for a sensitive network, is the beacon that would broadcast the network's presence disabled?
- 8.32. If wireless network technology is used, are the shared encryption keys rotated regularly?
- 8.33. If wireless network technology is utilized, is access to the wireless connections limited to authorized devices?
- 8.34. Do corporate policies mandate procedures for deploying modems within the corporate infrastructure?
- 8.35. Are authorized modems accessed using security measures, such as dial-back and call forwarding detection?
- 8.36. Are internal war-dialing campaigns periodically carried out to identify unauthorized modems that can be reached by dialing in?
- 8.37. Are corporate phone exchanges periodically checked to detect outside attempts at finding unauthorized modems by war-dialing campaigns?

**Firewalls and Intrusion Detection and Prevention Systems**

- 8.38. Has the corporation made lists of the traffic destinations and kinds of traffic, both inbound and outbound, that it wants to allow through its firewalls?
- 8.39. Has the corporation configured its firewalls to allow only the traffic on its approved lists?
- 8.40. Does the corporation have an approval process for any changes in the rule sets defining the traffic it will allow through its firewalls?
- 8.41. Does the corporation require the lists of the traffic it allows through its firewalls to be periodically reviewed, so that they take account of changes in the corporation's traffic needs?
- 8.42. Does the corporation require periodic checks of its firewalls to verify that the rule sets have been accurately implemented with no ad hoc changes?
- 8.43. Are security logs for firewalls maintained in a way that prevents them from being modified or deleted?
- 8.44. Are security logs for firewalls regularly reviewed for unauthorized traffic?
- 8.45. Are there firewalls deployed to protect critical systems from unauthorized access from internal personnel?
- 8.46. Does the corporation maintain comprehensive access control lists for its routers, including the internet protocol addresses and port numbers being utilized?
- 8.47. Does the corporation require periodic checks of its routers to verify that the access control lists have been accurately implemented?
- 8.48. Does the corporation require that the access control lists for its routers be periodically reviewed, so that they take account of changes in the corporation's traffic needs?
- 8.49. Are intrusion detection and/or intrusion prevention systems used on the network?
- 8.50. Are security alerts from intrusion detection systems continuously monitored?
- 8.51. Are signatures regularly updated on intrusion detection and prevention systems?
- 8.52. Are security logs for intrusion detection systems and intrusion prevention systems regularly reviewed for abnormal patterns of activity?
- 8.53. Are security logs for intrusion detection and intrusion prevention systems maintained in a way that prevents them from being modified or deleted?

### **Filtering**

- 8.54. Are web filters used to restrict confidential information from being uploaded to web-based e-mail applications? \*
- 8.55. Are web filters used to restrict the upload of sensitive information to online storage portals and contact directory portals? \*
- 8.56. Are web filters used to restrict the transmission of sensitive information through electronic greeting card portals? \*
- 8.57. Does the corporation filter out internet downloads by employees, based on their work roles? \*
- 8.58. Does the corporation use content filtering to control hostile Active X, JavaScript, and Java Applets?
- 8.59. Does the organization perform content filtering on all file attachments being sent through e-mail, so that any transmission of sensitive information is either blocked or tracked? \*
- 8.60. Does the organization filter out all executable e-mail attachments?
- 8.61. Are e-mail filters used to restrict confidential information from being transmitted to outside parties, unless authorized and encrypted? \*
- 8.62. Does the corporation use content filtering to control instant messages (IM) that may contain sensitive information? \*
- 8.63. Does the corporation tag sensitive documents with digital watermarks, so that content filters can more easily identify them? \*
- 8.64. Does the organization perform content filtering on outbound file transfer protocol (FTP) or trivial file transfer protocol (TFTP) transmissions, so that any transmission of sensitive information is either blocked or tracked?
- 8.65. Does the corporation restrict Simple Network Management Protocol (SNMP) requests at the internet gateway?
- 8.66. Does the corporation restrict internal SNMP requests from unauthorized systems to critical servers and networking devices?
- 8.67. Does the corporation use ingress and egress filtering at their internet gateways?
- 8.68. Does the corporation use ingress and egress filtering on perimeter routers to prevent impersonation with spoofed IP addresses?
- 8.69. Does the corporation use ingress and egress filtering between partner network connections?
- 8.70. Do firewall or router rules prevent unauthorized outbound connections from public facing systems, such as web servers?

## **Avenue 9: Intermittent Network Connections**

### **Telecommunication Issues**

- 9.01. Do employees working from home utilize computers with the firewalls, virus protection, security patches, virtual private network software, and other security that the corporation deems appropriate?
- 9.02. Are employees on the road issued standardized computer equipment that incorporates security measures to protect sensitive data if the computer is lost or stolen, in addition to the meeting the other corporate security requirements?
- 9.03. Do corporate policies define security requirements for dial-up connections to the corporate network or virtual private network?
- 9.04. Do corporate policies define security requirements for off-site wireless modems and wireless broadband connections?
- 9.05. Do telecommuters use two-factor authentication to access the corporate network?
- 9.06. Are telecommuters required to use virtual private network connections to obtain access to the corporate network?
- 9.07. If a web-based virtual private network is used, does it securely remove information about the session from the computer that initiated the session?
- 9.08. Is there extra monitoring of remote connection activities to compensate for the fact that they are less supervised in other respects?

### **Irregular Connections by Employees and Partners**

- 9.09. Are there strict controls on any laptops, storage media, or other kinds of equipment that are periodically plugged into the network to perform maintenance?
- 9.10. Are there strict controls on any laptops, storage media, or other kinds of equipment that are periodically plugged into the network to update software?
- 9.11. Are infrared, Bluetooth and wireless links on laptops and portable digital assistant's disabled when not required for business functions?
- 9.12. Are internal microphones and cameras on laptops disabled within sensitive areas?
- 9.13. If sensitive information needs to be stored on laptops, is this information encrypted?
- 9.14. Does the corporation 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?
- 9.15. Are the activities carried out by laptops that are temporarily connected to the corporate network by outside vendors and contractors tracked?

- 9.16. Do corporate policies define security requirements for portable digital assistants, smart phones, USB drives, iPods, digital cameras, and other devices that could be connected to the corporate network?
- 9.17. If removable information devices are allowed, does the organization monitor the usage of such devices? \*
- 9.18. If portable digital assistants or smart phones are allowed, does the organization restrict sensitive information from being downloaded to these devices?
- 9.19. If sensitive information needs to be temporarily stored on portable digital assistants or smart phones, is this information encrypted?
- 9.20. If portable digital assistants or smart phones are allowed, are anti-virus applications installed on these devices?
- 9.21. If anti-virus software is used on portable digital assistants or smart phones, are the definition files updated on a regular basis?

#### **E-Commerce Connections**

- 9.22. If business transactions are being carried out over the internet, is data being collected from the customer and from the customer's computer that will help authenticate the transaction?
- 9.23. Is there a mechanism that allows customers to verify that they are on a legitimate website of the company with which they are intending to do business? \*
- 9.24. Are customer verification's for e-commerce transactions protected from automated attacks by the display of a picture or audio play-back that contains a pattern which only be recognized by a human being? \*
- 9.25. If internet business transactions are sufficiently large financially, are these transactions authenticated by digital certificates, two-factor tokens, or additional authentication mechanisms?
- 9.26. If digital certificates are utilized for e-commerce transactions, are these certificates issued by an industry approved certificate authority?
- 9.27. 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? \*
- 9.28. Are there mechanisms established to prevent the alteration of the orders or instructions in business transactions conducted over the internet?
- 9.29. Is there a mechanism that will automatically terminate an e-commerce session after a period of inactivity?

- 9.30. 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?
- 9.31. Are customer websites equipped with anti-tampering software, which will automatically restore each site to its proper condition if an attempt is made to deface it?
- 9.32. Are web portals for e-commerce checked more frequently for security issues than other corporate information systems?

## **Avenue 10: Network Maintenance**

### **Network Documentation**

- 10.01. Do detailed network topology diagrams exist of the corporate network, so that all the connection routes can be traced?
- 10.02. If these network topology diagrams exist, do they list service paths and protocol being used?
- 10.03. 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?
- 10.04. Is there a floor plan or geographical map that shows exactly where the network cables have been laid?
- 10.05. Are all documents diagramming network topologies and physical layouts rigorously protected from unauthorized access?
- 10.06. Have all the cables and equipment been physically labeled in wiring closets and at other locations where they might need to be reconfigured?
- 10.07. Are there labels for equipment on both the front and rear of the equipment housings, to reduce the risk of equipment being improperly reconfigured?

### **Security Guidelines and Standards**

- 10.08. Is there a system for tracking software patches and updates that logs the news that they are needed, the announced release dates, and the dates on which they are actually received?
- 10.09. Are the relevant people within the organization alerted to any new 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?
- 10.10. Are there procedures for implementing software patches and updates in a manner that minimizes the risks of malfunctions by prior testing, carefully chosen

- installation times, and emergency procedures for returning rapidly to the last known good state?
- 10.11 Are security settings and configurations rechecked after patches and upgrades have been installed to make sure that they have not been inadvertently reset to less secure or default settings?
  - 10.12. 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?
  - 10.13. Are vendor default security settings changed on systems before those systems are placed on the network?
  - 10.14. Are there policies for limiting and monitoring the use of remote management tools that would allow systems to be controlled from outside the corporate network?
  - 10.15. Does the organization have agreements with vendors in which they guarantee a specified level of network reliability and service?
  - 10.16. Are there procedures for rate-limiting traffic so that the network is not incapacitated by excessive loads on the services affected?
  - 10.17. 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?
  - 10.18. Do corporate policies prohibit the use of unencrypted protocols, such as Telnet, FTP, and SNMP, for system management, unless the system requires these protocols?
  - 10.19. If the systems require unencrypted protocols for their management, are the corresponding connections set to shut down after a limited period of time?
  - 10.20. Are all server and work stations configured to a specified security standard?
  - 10.21. Are all network components, such as routers and switches, configured to a specified security standard?
  - 10.22. Are all firewalls and intrusion detection systems configured to a specified security standard?
  - 10.23. Is the remote management of routers, switches, and other network components restricted to only authorized Internet Protocol addresses?
  - 10.24. Is logical access to the management interfaces of security components (e.g. firewall, IDS, etc.) restricted to only authorized systems or Internet Protocol addresses?

### **System and Security Logging**

- 10.25. Are configuration modifications to all critical servers logged?
- 10.26. Are configuration modifications to routers and switches logged?
- 10.27. Are configuration modifications to firewalls and intrusion detection systems logged?
- 10.28. Is syslog enabled on critical servers and the information logged to a remote system?
- 10.29. Is syslog enabled on routers and switches and the information logged to a remote system?
- 10.30. Is syslog enabled on the wireless access points and information logged to a remote system?

## **Area Four: Automation Vulnerabilities**

### **Avenue 11: Remote Sensors and Control Systems**

- 11.01. Is there an overall map that accurately identifies all the communication paths by which control systems are connected?
- 11.02. Are all documents mapping the logical access routes to control systems rigorously protected from unauthorized access?
- 11.03. Are all control systems which do not need to be connected to the internet isolated from the internet?
- 11.04. Are all connections between control systems and the internet periodically evaluated to see whether they are really necessary?
- 11.05. Are all control systems isolated from the corporate network whenever there is no compelling reason to connect them?
- 11.06. If a control system cannot be isolated from the corporate network, is the control system protected by highly restrictive firewalls and intrusion detection systems?
- 11.07. Has care been taken to make sure that intruders are not presented with clearly labeled schematic diagrams of the physical processes and the systems for managing them?
- 11.08. Have the addresses and command codes for control system components, such as remotely operated switches and valves, been assigned or reassigned in such a way that they are not too easy to guess or deduce? \*
- 11.09. Are there provisions, such as remote alarms, which would warn that remote sensors are being physically manipulated on site to produce false readings?

- 11.10. 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? \*
- 11.11. Are highly critical controls accessible by a second control channel, so that they can still be accessed if the first channel fails?
- 11.12. 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? \*
- 11.13. If remote sensors communicate via cellular, satellite, or other wireless connections, have measures been taken to prevent information transmissions from being falsified? \*
- 11.14. Are there plans and procedures for dealing with the possibility of critical wireless links being jammed?
- 11.15. If remote terminal units have the capability of employing passwords or encryption and the operational speed requirements allow this, are these security measures being used?
- 11.16. Do all new remote terminal units and other control devices being installed in the network have changeable passwords or other reprogrammable authentication mechanisms?
- 11.17. Are all periodic automated transmissions of critical control data, where speed is not an issue, protected by encryption?
- 11.18. Are critical system components configured to regularly update their time from a secure time source?
- 11.19. Are all components within the network synchronized, so that they are using the same time, time zone, and date?
- 11.20. 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? \*
- 11.21. Are there sufficient alarms to warn operators when any critical processes are in danger of moving outside the normal parameters of safe operation? \*
- 11.22. Are updates to the operating systems of remote terminal units sent in a secure manner from a secure source?
- 11.23. Are status queries to remote terminal units sent in a secure manner from a secure source?

## **Avenue 12: Backup Procedures**

### **Backup Strategy**

- 12.01. Are the operating systems, programs, and operating information backed up, as well as the data?
- 12.02. Is the data being backed up at a frequency appropriate to its economic value and the rate at which it is being changed?
- 12.03. 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?
- 12.04. Are all logs of activity that could have relevance for security backed up frequently and stored in a form that would prevent tampering?
- 12.05. Are the configurations of switches and routers backed up on a regular basis?
- 12.06. Are the log files of application access regularly backed up to a secure location?
- 12.07. 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?
- 12.08. Are there multiple backups, so that if one is lost or corrupted, the system could still be restored?
- 12.09. Are the backups regularly tested to ensure that they are readable and uncorrupted?
- 12.10. Are there procedures for dealing with backup data that has become corrupted, especially during a crisis? \*
- 12.11. Is the backup regularly transferred to a storage device that is isolated from the network?
- 12.12. Is the backup regularly transferred to a physically remote location?
- 12.13. 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?
- 12.14. If the loss of the backed-up information would jeopardize the enterprise, are there backups stored at more than one remote location?

### **Backup Security**

- 12.15. Are there procedures for dealing with the loss or theft of unencrypted backup tapes that contain proprietary or sensitive information?
- 12.16. Does the backup procedure include checking the data for hostile code such as viruses and Trojan horses prior to backing-up the information? \*

- 12.17. 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? \*
- 12.18. 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? \*
- 12.19. 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? \*
- 12.20. If the backup copies are being transported physically to a remote location, are they placed in tamper-proof containers, handled by a secure means of transport, and tracked in transit? \*
- 12.21. Are all of the backup media protected from physical theft during storage, whether they are stored locally or remotely?
- 12.22. 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?
- 12.23. 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?

## **Area Five: Human Operator Vulnerabilities**

### **Avenue 13: Human Maintenance of Security Procedures**

#### **Security Training**

- 13.01. 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?
- 13.02. Are employees trained to keep their laptops and other portable information equipment under watch or in secure places when carrying or using them outside the workplace?
- 13.03. Are employees trained not to choose passwords constructed out of personal biographical facts that might be publicly accessible?
- 13.04. Are employees made aware of the hazards of storing passwords in insecure places, such as on post-it notes in their work area?
- 13.05. Are employees taught what sorts of information handled by the corporation should be regarded as sensitive information?
- 13.06. 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?

- 13.07. Have the employees been trained not to fall victims to social manipulations by telephone or over the internet that would led them to reveal private information or to type or dial specific sequences of numbers or characters?
- 13.08. Are employees regularly reminded not to download file types that could contain executable code, not to open suspicious e-mails, and not to install personal software on corporate systems?
- 13.09. Are employees made aware of the security risks they can incur by storing personal information, especially personal identification information, on their cell phones?
- 13.10. Have employees been made aware of the fact that mass produced and mass distributed software could still contain targeted malware?
- 13.11. Are employees made aware of how dangerous it is to install network links that are undocumented and not authorized by security personnel, even though these links might be requested by senior executives?
- 13.12. Are all employees periodically tested on their knowledge of security procedures, including their knowledge of newly emerging threats?

#### **Security Accountability**

- 13.13. Is maintaining the security of the corporation made part of each employee's job description?
- 13.14. Are all employees required to sign confidentiality and intellectual property agreements?
- 13.15. Are all outside contractors, facility managers, couriers, and maintenance companies explicitly informed of the corporate security policies and standards that apply to their activities?
- 13.16. Are all outside contractors, facility managers, couriers, and maintenance companies contractually committed to maintaining security policies and standards at least as stringent as those maintained by the corporation itself?
- 13.17. Are legal notices posted on log-in and authentication screens, warning that unauthorized access or use constitutes an illegal intrusion?
- 13.18. Are employees prohibited from installing any software on corporate machines that is personal, recreational, or simply unauthorized?
- 13.19. Do corporate policies define the proper use of e-mail, internet access, and instant messaging by employees?
- 13.20. Are employees prohibited from letting other employees use their personal computers?
- 13.21. Are employees prohibited from sharing passwords?

- 13.22. Are employees prohibited from using personal identification devices, such as badges and proximity cards, to give other employees access to information facilities and systems?
- 13.23. Is each piece of information equipment the corporation owns or leases the explicit responsibility of one designated employee?
- 13.24. Is the employee who is responsible for a given piece of information equipment required to oversee the general security of that equipment?
- 13.25. 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?
- 13.26. Are employees given adequate incentives to report security breaches and bad security practices, while simultaneously insulated from any blame or retribution for making such reports?
- 13.27. Are employees made strictly accountable for any actions they carry out on the corporate information system that are in violation of corporate security policies?

#### **Security Reviews**

- 13.28. Are the corporation’s information security policies and their implementation reviewed annually by an expert outside auditor?
- 13.29. Is the annual review of the corporation’s information security policies and their implementation broad enough in scope to uncover information vulnerabilities in the physical facilities and in employee behavior?
- 13.30. Are the corporation’s information security policies and their implementation carefully checked to verify that the corporation is compliant with the regulations and recognized standards for that industry?
- 13.31. Are the audits and reviews of the corporation’s information security examined analytically to identify areas where different or additional counter-measures may be needed?
- 13.32. Is there a reliable system for listing and tracking all of the vulnerabilities noticed by employees, discovered by audits, reported by vendors, or covered in the media, so security personnel can quickly and regularly access an up-to-date list, showing which vulnerabilities have already been remedied and which are still in need of remedies?
- 13.33. Are remedial actions constantly undertaken in a timely manner to deal with all the more significant vulnerabilities uncovered or reported?

- 13.34. Are remedial programs to deal with recently uncovered vulnerabilities monitored on a monthly basis, to make sure that there is rapid and steady progress in those areas?
- 13.35. Are the successive audits and reviews of the corporation's information security compared, so that senior managers can make sure that the corporation's information security is improving, rather than deteriorating?

#### **Incident Handling and Response**

- 13.36. 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 and promptly reporting them?
- 13.37. Do employees know whom they should notify, both inside and outside the corporation, in the event of an apparent attack?
- 13.38. Are employees with access to highly critical systems or facilities provided with special access codes that would signal that they are acting under duress? \*
- 13.39. Are automated detection systems in place that would raise silent, remote alarms if the duress codes are used? \*
- 13.40. Are there alternative channels of communication that can be utilized in the event of normal channels being compromised?
- 13.41. Do employees know how to isolate the systems that have been compromised by removing them from the network?
- 13.42. Are there plans for manually quarantining and monitoring systems that may have been contaminated with false information without shutting them down?
- 13.43. Is there a procedure for moving the quarantine lines as better information about the possible contamination becomes available?
- 13.44. Do employees know how to go about restoring compromised information systems to their last known good state?
- 13.45. Is there a mechanism for retrieving "last known good state" when that state is a considerable time into the past?
- 13.46. If there are other 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?
- 13.47. Do employees know where they should turn for additional information and guidance during a continuing series of attacks?
- 13.48. If the corporation 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?

- 13.49. Do the key response personnel know how to collect and preserve the evidence necessary for proper forensic investigations and legal prosecutions?
- 13.50. Are exercises periodically conducted in which key employees go through the motions of responding to a cyber-attack in a reasonably realistic manner?
- 13.51. Are employees trained to handle storage media and by-products securely in the special circumstances produced by disaster recovery?
- 13.52. Have the key personnel been given opportunities to practice their emergency responses in actual simulations? \*
- 13.53. Are both real incidents and exercises followed by after-action discussions directed at identifying the lessons learned?

#### **Avenue 14: Intentional Actions Threatening Security**

##### **Background Checks**

- 14.01. 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?
- 14.02. If an employee is promoted to a considerably higher level of responsibility and access, is a new background check carried out?
- 14.03. Is background screening carried out for building maintenance personnel, such as janitors?
- 14.04. 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? \*
- 14.05. Is an effort made to track the current whereabouts of former employees who were deeply acquainted with critical systems and procedures?

##### **Behavior Checks**

- 14.06. Is information generally disseminated throughout the corporation on a need-to-know basis, while still recognizing the need for cross-disciplinary information sharing and the importance of employees' understanding the reasons for what they are doing?
- 14.07. If a given category of input is sufficiently critical, does the corporation require a second employee to verify that input before it is processed?
- 14.08. 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?

- 14.09. Does the corporation restrict employee access to critical systems from unsupervised locations and at unsupervised times?
- 14.10. Are building maintenance personnel, such as janitors, prevented from entering highly sensitive areas unless directly supervised by security personnel?
- 14.11. Is video surveillance carried out on building maintenance personnel, such as janitors, even in areas that are only moderately sensitive?
- 14.12. Are the employee's physical and electronic access logs periodically reviewed to identify access patterns that are not motivated by normal work responsibilities?
- 14.13. Does the corporation systematically check for multiple failed log-in attempts carried out by its own employees?
- 14.14. Are employees prevented from accessing files that would reveal when their behavior is being monitored and whether it has attracted special attention?
- 14.15. 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?
- 14.16. Are there measures to prevent employees from leaving the business premises with sensitive information carried on floppies or USB devices? \*

#### **Employee Relations**

- 14.17. Does the corporation make fairness and good faith in the treatment of employees a higher priority than seizing every opportunity to gain a short-term competitive edge?
- 14.18. Does the corporation provide adequate mechanisms for employees to express their grievances without penalty and for them to see those grievances being conscientiously addressed?
- 14.19. Does the corporation handle down-sizings in a manner that minimizes hostile feelings on the part of former employees?
- 14.20. Does the corporation 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?
- 14.21. 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?

## **Area Six: Software Supply Vulnerabilities**

### **Avenue 15: Internal Policies for Software Development**

#### **Secure Procedures for Developing New Software**

- 15.01. Does the corporation have a written policy detailing the steps and procedures for the internal development of software?
- 15.02. Does the software development cycle follow guidelines based on industry best practices concerning security?
- 15.03. Do corporate security policies require all vendor and contractor personnel working on software development to meet minimum security requirements?
- 15.04. Are the proposed software designs evaluated from the standpoint of information security by security specialists before the alpha versions are created?
- 15.05. Does the corporation have a system for tracking exactly which employee or outside contributor wrote each line of code for any software produced internally?
- 15.06. Are all the programmers working on each software application made aware that records are being kept of exactly who wrote each line of code?
- 15.07. Does the corporation 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 programmer recorded as responsible for it? \*
- 15.08. Are changes to the source code library controlled and monitored, so that the source control module cannot be bypassed by someone with administrator privileges? \*
- 15.09. Are commentaries 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?
- 15.10. Does the corporation have pre-approved code modules that can be inserted into new software to accomplish standard security functions, such as authentication and encryption?
- 15.11. Does the corporation provide developers with dummy data, so that the applications under development do not have to be tried out on private, sensitive, or proprietary information?
- 15.12. Are the applications under development tried out in test bed environments that are completely isolated from the actual production environments?

### **Security Features to Build into New Software**

- 15.13. Is the application being developed designed to encrypt sensitive information that it stores in a file or database?
- 15.14. Is the application being developed designed to encrypt sensitive information that it writes to the local system registry?
- 15.15. Is the application being developed designed to encrypt sensitive information that it writes to volatile memory?
- 15.16. Is the application being developed designed to encrypt sensitive information that it transmits to another system?
- 15.17. Is the application being developed designed to encrypt sensitive information that it writes to cookies?
- 15.18. Is the application under development designed to prevent excessively predictable authentication and encryption codes?
- 15.19. Is the application under development designed to use the concept of least privilege when executing instructions?
- 15.20. Whenever possible, is the meaning of code components masked or obfuscated in the applications under development that are designed to carry out critical operations?
- 15.21. Are critical applications under development designed to authenticate sub-components, such as dynamic link libraries, to ensure their authenticity before they are utilized? \*

### **Security Testing of New Software**

- 15.22. Is the software that the corporation has developed subjected to a code review from a security standpoint, regardless of whether it was outsourced or produced in-house, before the final version is readied for deployment? \*
- 15.23. Are any user accounts employed for software testing systematically removed before the software is actually put into service?
- 15.24. 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?
- 15.25. Does the corporation have information security professionals conduct vulnerability tests of the software it has developed, regardless of whether it was outsourced or produced in-house?
- 15.26. Does the organization have information security specialists conduct regular vulnerability testing against applications after they are deployed?

## **Avenue 16: Policies for Dealing with External Vendors**

### **Establishing Appropriate Relationships with Vendors**

- 16.01. Does the corporation have a written policy detailing the steps and procedures for dealing with software vendors and outside developers?
- 16.02. Are prospective vendors and outside developers limited to those who can be verified to meet industry standards for information security?
- 16.03. Are vendors or contract personnel required to have briefings or training in the security policies of the client corporation?
- 16.04. Are the vendors or contract personnel contractually required to adhere to the security policies of the client corporation?
- 16.05. Do corporate policies require vendor personnel to sign non-disclosure agreements?
- 16.06. Do the service agreements require vendors to conduct background checks on their personnel before they are assigned to the corporate account?
- 16.07. If the 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?
- 16.08. Are software vendors required to certify that their code has undergone a rigorous and thorough security inspection before it is delivered for deployment?
- 16.09. 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?

### **Managing Ongoing Relationships with Vendors**

- 16.10. Are there trusted channels for receiving updates from each software vendor?
- 16.11. Is there a regular procedure for verifying over the internet or by telephone that any physical shipment from the vendor is an authentic one?
- 16.12. Do vendors provide physical shipments with packaging and labels that are difficult to counterfeit or tamper with?
- 16.13. 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?
- 16.14. Are there appropriate limitations and an expiry date on the access rights that the vendors need in order to install the software and updates?
- 16.15. 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?

- 16.16. Are there provisions to maintain the system's performance during the update process and to restore the system to its last known good state if an update fails?
- 16.17. Does the organization have processes established to restrict, control, or monitor internal information access by outside vendors or contractors? \*
- 16.18. Does the organization have processes established to identify and terminate vendor, contractor, and other outsourced personnel access when no longer required?
- 16.19. Are the vendors' comings and goings logged and monitored, whether electronic or physical?
- 16.20. Are there procedures for verifying that copies of proprietary information were destroyed after the vendors delivered the contracted software?
- 16.21. Are the actions of former vendors or contractors who handled critical information or critical systems monitored for non-compliances with non-disclosure agreements?

### **Permission to Use US-CCU Cyber-Security Check List**

The US-CCU Cyber-Security Check List, which is copyrighted by the US-CCU, may be incorporated into other documents, formats, and software for free, but only under the following conditions:

- 1) The US-CCU is provided in advance with an example of the proposed publication, and the US-CCU confirms in writing that the publication is in compliance with these US-CCU guidelines.
- 2) This present notice is reproduced in a conspicuous place in the introduction, organizational credits, or explanatory materials that are incorporated into the publication.
- 3) If other cyber-security questions are incorporated into the publication, the ones from the US-CCU Cyber-Security Check List are presented in boldface, italics, or some other typographical form that clearly distinguishes them from the other material.
- 4) All of the US-CCU Cyber-Security Check List questions are included in the publication, with none omitted.
- 5) The original wording of the US-CCU cyber-security questions is retained without alternation.
- 6) The US-CCU copyright is acknowledged and authorship credit for the US-CCU Check List questions is clearly given to John Bumgarner and Scott Borg on those parts of the publication that function as the title page and cover.
- 7) The date of the specific edition of the US-CCU Cyber-Security Check List that was used is clearly noted on those parts of the publication that function as the title page and cover.
- 8) Users of the publication are hereby informed that the US-CCU Cyber-Security Check List is available to the public for free, directly from the US-CCU.