**CHAPTER 8**

**INFORMATION SYSTEM CONTROLS for SYSTEMS RELIABILITY**

**Part 1: Information Security**

 **SUGGESTED ANSWERS TO DISCUSSION QUESTIONS**

**8.1 Explain why an organization would want to use all of the following information security controls: firewalls, intrusion prevention systems, intrusion detection systems, and a CIRT.**

 Using this combination of controls provides defense-in-depth. Firewalls and intrusion prevention systems are preventive controls. Intrusion detection systems are used to identify problems and incidents. The purpose of a Computer Incident Response Team (CIRT) is to respond to and mediate problems and incidents. According to the time-based model of security, information security is adequate if the firewalls and intrusion prevention systems can delay attacks from succeeding longer than the time it takes the intrusion detection system to identify that an attack is in progress and for the CIRT to respond.

**8.2 What are the advantages and disadvantages of having the person responsible for information security report directly to the chief information officer (CIO), who has overall responsibility for all aspects of the organization’s information systems?**

It is important for the person responsible for security (the CISO) to report to senior management. Having the person responsible for information security report to a member of the executive committee such as the CIO, formalizes information security as a top management issue.

One potential disadvantage is that the CIO may not always react favorably to reports indicating that shortcuts have been taken with regard to security, especially in situations where following the recommendations for increased security spending could result in failure to meet budgeted goals. Therefore, just as the effectiveness of the internal audit function is improved by having it report to someone other than the CFO, the security function may also be more effective if it reports to someone who does not have responsibility for information systems operations.

**8.3**  **Reliability is often included in service level agreements (SLAs) when outsourcing. The toughest thing is to decide how much reliability is enough. Consider an application like e-mail. If an organization outsources its e-mail to a cloud provider, what is the difference between 95%, 99%, 99.99%, and 99.9999% reliability?**

The differences in promised reliability levels over the course of a year in terms of days when the e-mail system may not work are:

 95% reliability = 18.25 days

 99% reliability = 3.65 days

 99.99% reliability = .0365 days or approximately 52.56 minutes

 99.9999% reliability = .000365 days or less than one minute

**8.4** **What is the difference between authentication and authorization?**

Authentication and authorization are two related controls designed to restrict access to an organization’s information systems and resources.

 The objective of authentication is to verify the claimed identity of someone attempting to obtain access.

 The objective of authorization is to limit what an authenticated user can do once they have been given access.

**8.5** **What are the limitations, if any, of relying on the results of penetration tests to assess the overall level of security?**

Penetration testing provides a rigorous way to test the effectiveness of an organization’s computer security by attempting to break into the organization’s information system. Internal audit and external security consulting team perform penetration tests in which they try to compromise a company’s system. Some outside consultants claim that they can get into 90 percent or more of the companies they attack. This is not surprising, given that it is impossible to achieve 100% security. Thus, one limitation of penetration testing is that it almost always shows that there are ways to break into the system.

The more important analysis, however, is evaluating how difficult it was to break in and the cost-effectiveness of alternative methods for increasing that level of difficulty.

Another limitation is that failure to break in may be due to lack of skill by the tester.

Finally, penetration testing typically focuses on unauthorized access by outsiders; thus, it does not test for security breaches from internal sources.

**8.6** **Security awareness training is necessary to teach employees “safe computing” practices. The key to effectiveness, however, is that it changes employee behavior. How can organizations maximize the effectiveness of their security awareness training programs?**

Top management support is always essential for the success of any program an entity undertakes. Thus, top management support and participation in security awareness training is essential to maximize its impact on the employees and managers of the firm.

Effective instruction and hands-on active learning techniques help to maximize training. “Real life” example should be used throughout the training so that employees can view or at least visualize the exposures and threats they face as well as the controls in place to address the exposures and threats. Role-playing has been shown to be an effective method to maximize security awareness training especially with regard to social engineering attack training.

Training must also be repeated periodically, at least several times each year, to reinforce concepts and update employees about new threats.

It is also important to test the effectiveness of such training.

Including security practices and behaviors as part of an employee’s performance evaluation is also helpful as it reinforces the importance of security.

**8.7 What is the relationship between COSO, COBIT, and the AICPA’s Trust Services frameworks?**

COSO is a broad framework that describes the various components of internal control. It does not, however, provide any details about IT controls.

COBIT is a framework for IT governance and control.

The AICPA’s Trust Services framework is narrower in scope than COBIT, focusing only on those IT controls (security, confidentiality, privacy, processing integrity, and availability) that relate directly to systems reliability.

 **SUGGESTED SOLUTIONS TO THE PROBLEMS**

**8.1 Match the following terms with their definitions:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| \_\_d\_\_ 1. Vulnerability | 1. Code that corrects a flaw in a program.
 |
| \_\_s\_\_ 2. Exploit | 1. Verification of claimed identity.
 |
| \_\_b\_\_ 3. Authentication | 1. The firewall technique that filters traffic by comparing the information in packet headers to a table of established connections.
 |
| \_\_m\_\_ 4. Authorization | 1. A flaw or weakness in a program.
 |
| \_\_f\_\_ 5. Demilitarized zone (DMZ) | 1. A test to determine the time it takes to compromise a system.
 |
| \_\_t\_\_ 6. Deep packet inspection | 1. A subnetwork that is accessible from the Internet but separate from the organization’s internal network.
 |
| \_\_o\_\_ 7. router | 1. The device that connects the organization to the Internet.
 |
| \_\_j\_\_ 8. social engineering | 1. The rules (protocol) that govern routing of packets across networks.
 |
| \_\_k\_\_ 9. firewall | 1. The rules (protocol) that govern the division of a large file into packets and subsequent reassembly of the file from those packets.
 |
| \_\_n\_\_ 10. hardening | 1. An attack that involves deception to obtain access.
 |
| \_\_l\_\_ 11. CIRT | 1. A device that provides perimeter security by filtering packets.
 |
| \_\_a\_\_ 12. patch | 1. The set of employees assigned responsibility for resolving problems and incidents.
 |
| \_\_\_u\_ 13. virtualization | 1. Restricting the actions that a user is permitted to perform.
 |
| \_\_i\_\_ 14. Transmission Control Protocol (TCP) | 1. Improving security by removal or disabling of unnecessary programs and features.
 |
| \_q\_\_\_ 15. static packet filtering | 1. A device that uses the Internet Protocol (IP) to send packets across networks.
 |
| \_\_g\_\_ 16. border router | 1. A detective control that identifies weaknesses in devices or software.
 |
| \_\_p\_\_ 17. vulnerability scan | 1. A firewall technique that filters traffic by examining the packet header of a single packet in isolation.
 |
| \_\_e\_\_ 18. penetration test | 1. The process of applying code supplied by a vendor to fix a problem in that vendor’s software.
 |
| \_r\_\_\_ s. patch management | 1. Software code that can be used to take advantage of a flaw and compromise a system.
 |
| \_v\_\_\_ t. cloud computing | 1. A firewall technique that filters traffic by examining not just packet header information but also the contents of a packet.
 |
|  | 1. The process of running multiple machines on one physical server.
 |
|  | 1. An arrangement whereby a user remotely accesses software, hardware, or other resources via a browser.
 |

**8.2**  **Install and run the latest version of the Microsoft Baseline Security Analyzer on your home computer or laptop. Write a report explaining the weaknesses identified by the tool and how to best correct them. Attach a copy of the MBSA output to your report.**

 **Solution:** will vary for each student. Examples of what to expect (from a computer running Windows 7 follow:

1. The first section should identify the computer (not shown below) and the status of security updates:

1. Next is a section about user accounts and Windows settings:

1. **Then there is a section about other system information**

**8.3 The following table lists the actions that various employees are permitted to perform:**

|  |  |
| --- | --- |
| **Employee** | **Permitted actions** |
| Able | Check customer account balancesCheck inventory availability |
| Baker | Change customer credit limits |
| Charley | Update inventory records for sales and purchases |
| Denise | Add new customersDelete customers whose accounts have been written off as uncollectibleAdd new inventory itemsRemove discontinued inventory items |
| Ellen | Review audit logs of employee actions |

Complete the following access control matrix so that it enables each employee to perform those specific activities:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Employee | CustomerMaster file | Inventory Master File | Payroll Master File | System Log Files |
| Able | 1 | 1 | 0 | 0 |
| Baker | 2 | 0 | 0 | 0 |
| Charley | 0 | 2 | 0 | 0 |
| Denise | 3 | 3 | 0 | 0 |
| Ellen | 0 | 0 | 0 | 1 |

Use the following codes:

0 = no access

1 = read only access

2 = read and modify records

3= read, modify, create, and delete records

**8.4 Which preventive, detective, and/or corrective controls would best mitigate the following threats?**

1. **An employee’s laptop was stolen at the airport. The laptop contained personally identifying information about the company’s customers that could potentially be used to commit identity theft.**

**Preventive:** Policies against storing sensitive information on laptops and requiring that if any such information must exist on the laptop that it be encrypted.

Training on how to protect laptops while travelling to minimize the risk of theft.

**Corrective**: Installation of “phone home” software might help the organization either recover the laptop or remotely erase the information it contains.

1. **A salesperson successfully logged into the payroll system by guessing the payroll supervisor’s password.**

**Preventive**: Strong password requirements such as at least an 8 character length, use of multiple character types, random characters, and require that passwords be changed frequently.

**Detective:** Locking out accounts after 3-5 unsuccessful login attempts; since this was a “guessing” attack, it may have taken more than a few attempts to login.

1. **A criminal remotely accessed a sensitive database using the authentication credentials (user ID and strong password) of an IT manager. At the time the attack occurred, the IT manager was logged into the system at his workstation at company headquarters.**

**Preventive:** Integrate physical and logical security. In this case, the system should reject any user attempts remotely log into the system if that same user is already logged in from a physical workstation.

**Detective**: Having the system notify appropriate security staff about such an incident.

1. **An employee received an email purporting to be from her boss informing her of an important new attendance policy. When she clicked on a link embedded in the email to view the new policy, she infected her laptop with a keystroke logger.**

 **Preventive:** Security awareness training is the best way to prevent such problems. Employees should be taught that this is a common example of a sophisticated phishing scam.

**Detective and corrective**: Anti-spyware software that automatically checks and cleans all detected spyware on an employee's computer as part of the logon process for accessing a company's information system.

1. **A company’s programming staff wrote custom code for the shopping cart feature on its web site. The code contained a buffer overflow vulnerability that could be exploited when the customer typed in the ship-to address.**

**Preventive:** Teach programmers secure programming practices, including the need to carefully check all user input.

Management must support the commitment to secure coding practices, even if that means a delay in completing, testing, and deploying new programs.

**Detective:** Make sure programs are thoroughly tested before being put into use

Have internal auditors routinely test in-house developed software.

1. **A company purchased the leading “off-the-shelf” e-commerce software for linking its electronic storefront to its inventory database. A customer discovered a way to directly access the back-end database by entering appropriate SQL code.**

 **Preventive:** Insist on secure code as part of the specifications for purchasing any 3rd party software.

Thoroughly test the software prior to use.

Employ a patch management program so that any vendor provided fixes and patches are immediately implemented.

1. **Attackers broke into the company’s information system through a wireless access point located in one of its retail stores. The wireless access point had been purchased and installed by the store manager without informing central IT or security.**

**Preventive:** Enact a policy that forbids installation of unauthorized wireless access points.

**Detective**: Conduct routine audits for unauthorized or rogue wireless access points.

**Corrective:** Sanction employees who violate policy and install rogue wireless access points.

1. **An employee picked up a USB drive in the parking lot and plugged it into their laptop to “see what was on it,” which resulted in a keystroke logger being installed on that laptop.**

**Preventive:** Security awareness training. Teach employees to never insert USB drives unless they are absolutely certain of their source.

Anti-spyware software that automatically checks and cleans all detected spyware on an employee's computer as part of the logon process.

1. **Once an attack on the company’s website was discovered, it took more than 30 minutes to determine who to contact to initiate response actions.**

**Preventive:** Document all members of the CIRT and their contact information.

Practice the incident response plan.

1. **To facilitate working from home, an employee installed a modem on his office workstation. An attacker successfully penetrated the company’s system by dialing into that modem.**

**Preventive:** Routinely check for unauthorized or rogue modems by dialing all telephone numbers assigned to the company and identifying those connected to modems.

1. **An attacker gained access to the company’s internal network by installing a wireless access point in a wiring closet located next to the elevators on the fourth floor of a high-rise office building that the company shared with seven other companies.**

 **Preventive:** Secure or lock all wiring closets.

Require strong authentication of all attempts to log into the system from a wireless client.

Employ an intrusion detection system.

**8.5 What are the advantages and disadvantages of the three types of authentication credentials (something you know, something you have, and something you are)?**

|  |  |  |
| --- | --- | --- |
| **Type of Credential** | **Advantages** | **Disadvantages** |
| Something you know | + Easy to use+ Universal - no special hardware required+ Revocable – can cancel and create new credential if compromised | + Easy to forget or guess + Hard to verify who is presenting the credential+ May not notice compromise immediately |
| Something you have | + Easy to use+ Revocable – can cancel and reissue new credential if compromised+ Quickly notice if lost or stolen | + May require special hardware if not a USB token (i.e., if a smart card, need a card reader)+ Hard to verify who is presenting the credential |
| Something you are (biometric) | + Strong proof who is presenting the credential+ Hard to copy/mimic+ Cannot be lost, forgotten, or stolen | + Cost+ Requires special hardware, so not universally applicable+ User resistance. Some people may object to use of fingerprints; some culture groups may refuse face recognition, etc.+ May create threat to privacy. For example, retina scans may reveal health conditions.+ False rejection due to change in biometric characteristic (e.g., voice recognition may fail if have a cold).+ Not revocable. If the biometric template is compromised, it cannot be re-issued (e.g., you cannot assign someone a new fingerprint).  |

**8.6** a**. Apply the following data to evaluate the time-based model of security for the XYZ Company. Does the XYZ Company satisfy the requirements of the time-based model of security? Why?**

* **Estimated time for attacker to successfully penetrate system = 25 minutes**
* **Estimated time to detect an attack in progress and notify appropriate information security staff = 5 minutes (best case) to 10 minutes (worst case)**
* **Estimated time to implement corrective actions = 6 minutes (best case) to 20 minutes (worst case)**

 **Solution:** XYZ Company is secure under their best case scenario but they do not meet security requirements under their worst case scenario.

P = 25 Minutes

 D = 5 Minutes (Best Case) 10 Minutes (Worst Case)

 C = 6 Minutes (Best Case), 20 minutes (Worst Case)

 Time-base model: P > D + C

 Best Case Scenario P is greater than D + C (25 > 5 + 6)

 Worst Case Scenario P is less than D + C (25 < 10 + 20)

1. **Which of the following security investments to you recommend? Why?**
2. **Invest $50,000 to increase the estimated time to penetrate the system by 4 minutes**
3. **Invest $50,000 to reduce the time to detect an attack to between 2 minutes (best case) and 6 minutes (worst case)**
4. **Invest $50,000 to reduce the time required to implement corrective actions to between 4 minutes (best case) and 14 minutes (worst case).**

**Solution:** Option 3 is the best choice because it is the only one that satisfies the time-based model of security under the worst case conditions:

|  |  |  |  |
| --- | --- | --- | --- |
| Option | P (worst case) | D (worst case) | C (worst case) |
| 1 | 29 | 10 | 20 |
| 2 | 25 | 6 | 20 |
| 3 | 25 | 10 | 14 |

**8.7** **Explain how the following items individually and collectively affect the overall level of security provided by using a password as an authentication credential.**

 **a**. **Length** – interacts with complexity to determine how hard it is to “guess” a password or discover it by trial-and-error testing of every combination. Of the two factors, length is more important because it has the biggest impact on the number of possible passwords.

To understand this, consider that the number of possible passwords = xy, where x = the number of possible characters that can be used and y = the length. As the following table shows, increasing the length increases the number of possibilities much more than does the same proportionate increase in complexity:

|  |  |  |  |
| --- | --- | --- | --- |
| **Complexity (types of characters allowed)** | **Number of characters** | **Length** | **Number of possible passwords** |
| Numeric | 10 (0-9) | 4 | 104 = 10,000 |
| Alphabetic, not case sensitive | 26 (a-z) | 8 | 268 = 2.088+E11 |
| Alphabetic, case sensitive | 52 (a-z, A-Z) | 8 | 528 = 5.346+E13 |
| Alphanumeric, case sensitive | 62 (0-9, a-z, A-Z) | 8 | 628 = 2.183+E14 |
| Alphanumeric, case sensitive,  |  | 12 | 6212 = 3.226+E21 |
| Alphanumeric, case sensitive, plus special characters | 95 (0-9, a-z, A-Z, and $, !, #, etc.) | 8 | 958 = 6.634+E15 |
| Alphanumeric, case sensitive, plus special characters | 95 (0-9, a-z, A-Z, and $, !, #, etc.) | 12 | 9512 = 5.404+E23 |

**b**. **Complexity requirements (which types of characters are required to be used: numbers, alphabetic, case-sensitivity of alphabetic, special symbols like $ or !)** - interacts with complexity to determine how hard it is to “guess” a password or discover it by trial-and-error testing of every combination.

**c**. **Maximum password age (how often password must be changed)** – shorter means more frequent changes which increases security

**d**. **Minimum password age (how long a password must be used before it can be changed)** – this combined with history prevents someone from just keeping their same password, because it prevents repeatedly changing passwords until the system allows use of the same password once again.

**e**. **Maintenance of password history (how many prior passwords does system remember to prevent reselection of the same password when required to change passwords)** – the larger this is, the longer the time before someone can reuse a password. For example, a password history of 12 combined with a minimum age of 1 month means that the same password cannot be used until after a year. Note that this requires setting a minimum age. Otherwise, if the minimum age is zero, someone could repeatedly change their password as many times as the system’s history setting, and then change it one more time, this last time setting it to be the current password.

**f**. **Account lockout threshold (how many failed login attempts before the account is locked)** – this is designed to stop guessing attacks. However, it needs to account for typos, accidentally hitting the CAPS LOCK key, etc. to prevent locking out legitimate users. Its effect also depends on the next variable, time frame.

**g**. **Time frame during which account lockout threshold is applied (i.e., if lockout threshold is five failed login attempts, time frame is whether those 5 failures must occur within 15 minutes, 1 hour, 1 day, etc.).** – Shorter time frames defeat attempts to guess.

**h**. **Account lockout duration (how long the account remains locked after exceeding the maximum allowable number of failed login attempts)** – longer lockouts defeat attempts to guess. Too short a value on this parameter may enable an attacker to try to guess x times, get locked out for only a few minutes, and then start guessing again.

**8.8** **The chapter briefly discussed the following three common attacks against applications**

**a. Buffer overflows**

**b. SQL injection**

**c. Cross-site scripting**

**Required**

**Research each of these three attacks and write a report that explains in detail how each attack actually works and that describes suggested controls for reducing the risks that these attacks will be successful.**

**Solution**: Reports will vary from student to student; however, the reports should contain at least some of the following basic facts gathered from the text, cgisecurity.net, and Wikipedia:

**a. Buffer overflows**

One of the more common input-related vulnerabilities is what is referred to as a buffer overflow attack, in which an attacker sends a program more data than it can handle. Buffer overflows may cause the system to crash or, even worse, may provide a command prompt, thereby giving the attacker full administrative privileges, and control, of the device. Because buffer overflows are so common, it is instructive to understand how they work.

Most programs are loaded into RAM when they run. Oftentimes a program may need to temporarily pause and call another program to perform a specific function. Information about the current state of the suspended program, such as the values of any variables and the address in RAM of the instruction to execute next when resuming the program, must be stored in RAM. The address to go to find the next instruction when the subprogram has finished its task is written to an area of RAM called the stack. The other information is written into an adjoining area of RAM called a buffer. A buffer overflow occurs when too much data is sent to the buffer, so that the instruction address in the stack is overwritten. The program will then return control to the address pointed to in the stack. In a buffer overflow attack, the input is designed so that the instruction address in the stack points back to a memory address in the buffer itself. Since the buffer has been filled with data sent by the attacker, this location contains commands that enable the attacker to take control of the system.

Note that buffer overflows can only occur if the programmer failed to include a check on the amount of data being input. Thus, sound programming practices can prevent buffer overflow attacks. Therefore, internal auditors should routinely test all applications developed in-house to be sure that they are not vulnerable to buffer overflow attacks.

**b. SQL injection**

Many web pages receive an input or a request from web users and then, to address the input or the request, they create a Structured Query Language (SQL) query for the database that is accessed by the webpage. For example, when a user logs into a webpage, the user name and password will be used to query the database to determine if they are a valid user. With SQL injection, a user inputs a specially crafted SQL command that is passed to the database and executed, thereby bypassing the authentication controls and effectively gaining access to the database. This can allow a hacker to not only steal data from the database, but also modify and delete data or the entire database.

To prevent SQL injection attacks, the web server should be reprogrammed so that user input is not directly used to create queries sent to the database.

**c. Cross-site scripting**

Cross site scripting (also known as XSS) occurs whenever a web application sends user input back to the browser without scrubbing it. The problem is that if the input is a script, the browser will execute it. The attack requires tricking a user into clicking on a hyperlink to a trusted website that is vulnerable to cross site scripting. The hyperlink will take the victim to that website, but it also contains a script. When the user’s browser visits the trusted website, it sends the input (the embedded script in the hyperlink) back to the browser. The browser then executes that script and sends information, often cookies that may contain authentication credentials, back to the attacker.

The best protection is that web sites should never replay user input verbatim back to the browser, but should always convert it to harmless HTML code first.

**8.9 Physical security is extremely important. Read the article “19 Ways to Build Physical Security into a Data Center,” which appeared in the CSO Magazine November 2005. (You can find the article at**

**www.csoonline.com/read/110105/datacenter.html).**

**Which methods would you expect to find used by almost any major corporation?**

**Which might likely only be justified at a financial institution?**

**Solution**:

Depending on the sensitivity and value of the data processed and stored at a data center, all of the 19 methods could be used by a corporation. For example, IBM is extremely concerned about the loss of data and trade secrets due to disasters and corporate espionage and employs all 19 methods.

However, most corporations do not employ all 19 methods. Thus, the following solution is an approximation of the methods that a typical corporation may employ and the more extensive methods that a financial institution would choose.

The methods that any corporation would use can also be employed at financial institutions, but are not checked to more clearly highlight the differences.

|  |  |  |
| --- | --- | --- |
| Method | Any Corporation  | Extra methods justified at a Financial Institution |
| 1. Build on the right spot | X |  |
| 2. Have redundant utilities | X |  |
| 3. Pay attention to walls |  | X |
| 4. Avoid windows | X |  |
| 5. Use landscaping for protection | X |  |
| 6. Keep a 100-foot buffer zone around the site |  | X |
| 7. Use retractable crash barriers at vehicle entry points |  | X |
| 8. Plan for bomb detection |  | X |
| 9. Limit entry points | X |  |
| 10. Make fire doors exit only | X |  |
| 11. Use plenty of cameras | X |  |
| 12. Protect the buildings machinery | X |  |
| 13. Plan for secure air handling |  | X |
| 14. Ensure nothing can hide in the walls and ceilings |  | X |
| 15. Use two-factor authentication | X |  |
| 16. Harden the core with security layers | X |  |
| 17. Watch the exits too | X |  |
| 18. Prohibit food in the computer rooms | X |  |
| 19. Install visitor restrooms | X |  |

**SUGGESTED SOLUTIONS TO THE CASES**

**Case 8.1 Costs of Preventive Security**

**Firewalls are one of the most fundamental and important security tools. You are likely familiar with the software-based host firewall that you use on your laptop or desktop. Such firewalls should also be installed on every computer in an organization. However, organizations also need corporate-grade firewalls, which are usually, but not always, dedicated special-purpose hardware devices. Conduct some research to identify three different brands of such corporate-grade firewalls and write a report that addresses the following points:**

* **Cost**
* **Technique (deep packet inspection, static packet filtering, or stateful packet filtering)**
* **Ease of configuration and use**

Specifics of the solution will differ depending upon the brand identified. The instructor may wish to require students to turn in copies of their source materials. At a minimum, solution should clearly demonstrate that students understand the different types of firewalls and have read and understood the review of a product’s ease of configuration and ease of use.

**Case 8.2 Developing an Information Security Checklist**

**Obtain a copy of COBIT (available at** [**www.isaca.org**](http://www.isaca.org)**) and read section DS5.**

**Design a checklist for assessing each of the 11 detailed information security control objectives. The checklist should contain questions to which a Yes response represents a control strength, a No response represents a control weakness, plus a possible N/A response.**

**Provide a brief reason for asking each question. Organize your checklist as follows:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **Yes** | **No** | **N/A** | **Reason for asking** |
| **1. Is there regular security awareness training?** |  |  |  | **Training is one of the most important preventive controls because many security incidents happen due to either human error or social engineering.** |
|  |  |  |  |  |
|  |  |  |  |  |

Suggested solution (answers will vary, key is to address each objective)

|  |  |
| --- | --- |
| **COBIT Control Objective** | **Possible questions** |
| DS5.1 | * Does the person responsible for information security report to the C-suite?
* Is information security a topic at meetings of the Board of Directors?
 |
| DS5.2 | * Does an information security plan exist?
* Do information security policies and procedures exist?
* Are information security policies and procedures communicated periodically to all employees?
 |
| DS5.3 | * Do all employees have unique user IDs?
* Are all employees required to use passwords?
* Are there policies to ensure that passwords are sufficiently strong?
* Are access rights assigned by employee role?
* Are access rights approved by management?
 |
| DS5.4 | * Are there procedures for closing user accounts when an employee leaves the company?
* Do employees who need administrative access have two accounts – one that is a limited account and the other with administrative rights?
* Do employees routinely use only their limited user accounts when surfing the Internet?
 |
| DS5.5 | * Are there periodic vulnerability assessments?
* Are there periodic penetration tests?
* Is logging enabled?
* Are logs regularly reviewed?
 |
| DS5.6 | * Is there a computer incident response team (CIRT)?
* Does membership of the CIRT include all appropriate functions?
* Is there a written incident response plan?
* Has the plan been practiced this year?
 |
| DS5.7 | * Is documentation related to firewalls and IPS stored securely and with restricted access?
* Are firewalls and other security devices protected with appropriate logical and physical access controls?
 |
| DS5.8 | * Is sensitive information encrypted?
* Are there procedures for issuing and revoking encryption keys?
 |
| DS5.9 | * Do all computers run up-to-date anti-malware?
* Are patches applied on a timely basis?
 |
| DS5.10 | * Are firewalls and IPS used to protect the perimeter?
* Are firewalls used to segregate functions within the corporate network?
* Are intrusion detection systems used?
 |
| DS5.11 | * Is sensitive information encrypted prior to transmission over the Internet?
 |