Dalton Murray

INT 7223 Cybersecurity

Dr. Hany Othman

July 3, 2023

Chapter 16 - 18 Review

Question

16.1 What are the principal concerns with respect to inappropriate temperature and humidity?

The principal concerns to inappropriate temperature and humidity are that: the computer cannot adequately cool itself which may result in internal components being damaged, if it is too cold the components can suffer thermal shock when turned on and cause circuit boards and integrated circuits to crack, long-term expose to high humidity may also result in corrosion, condensation can also effect the internal components by causing short circuits, there may also be a galvanizing effect resulting in electroplating from connectors to each other and bond the two, low humidity can cause materials to change shape and reduce performance, static electricity can also cause concern when in the right degree which causes electric discharge which can permanently break components (Stallings & Brown, 2018. p. 511 - 512).

16.2 What are the direct and indirect threats posed by fire?

The direct and indirect threats posed by fire are: direct heat caused by fire can significantly break or destroy components and even melt them completely, it also causes a large amount of heat to come off, the release of toxic fumes, water damage from fire suppression, smoke itself can also cause damage to components, and fire can disrupt utilities such as electricity (Stallings & Brown, 2018. p. 512 - 513).

16.3 What are the threats posed by loss of electrical power?

There are three categories of problems which the loss of electrical power may cause, these categories are: undervoltage, overvoltage, and noise (Stallings & Brown, 2018. p. 515).

Undervoltage – If the equipment is receiving less voltage than required than the power supply will suffer from temporary dips in voltage all the way to full brownouts, which are prolonged undervoltage and can result in the system unexpectedly shutting down, and all the way to complete power outage (Stallings & Brown, 2018. p. 515). Generally slight undervoltage won't cause any harm as a power supply is built to take small dips in voltage, but once the dip is large enough it may cause damage by turning off components when they're not expecting it resulting in potential loss of data, corruption, to hardware damage (Stallings & Brown, 2018. p. 515).

Overvoltage – With overvoltage there is a sudden surge of voltage, with a significant enough overvoltage it can completely destroy components (Stallings & Brown, 2018. p. 515).

Noise – Noise is when a power line or something else is producing a random signal and will typically be filtered out by the power supply, but if the noise is significant enough it can cause errors with components (Stallings & Brown, 2018. p. 515).

16.4 List and describe some measures for dealing with inappropriate temperature and humidity

Some measures to deal with inappropriate temperature and humidity are to have environmental-control equipment with a capacity which is capable of dealing with the temperature and humidity (Stallings & Brown, 2018. p. 516). Some examples of this are having air conditioning and even heating in some cases, as well as having humidity control systems. Another thing to help deal with inappropriate temperature and humidity is having temperature and humidity sensors placed in various places which makes the most logical sense to have them in, and then have thresholds and alerts setup as well as have automations setup to handle when thresholds are met (Stallings & Brown, 2018. p. 516). Regular maintenance of parts can also significantly help with temperature and humidity (Stallings & Brown, 2018. p. 516).

17.1 What are the benefits of a security awareness, training, and education program for an organization?

There are four major benefits to organization to have security awareness, training, and education programs, these are: improving employee behavior, increasing the ability to hold employees accountable for their actions, mitigating liability of the organization for an employee's behavior, and complying with regulations and contractual obligations (Stallings & Brown, 2018. p. 529).

17.2 What is the difference between security awareness and security training?

There are a few critical differences between security awareness and security training in an organization.

Security awareness – With security awareness, it seeks to inform and focus the attention of an employee on issues related to security within the organization, it is also often required for all employees, there will typically be security basics and literacy elements, it helps employees be aware of their responsibilities for maintaining security as well as the restrictions placed on them, and it helps them understand the importance of security (Stallings & Brown, 2018. p. 531 - 532). Security awareness is also tailored for the organization with the target audience in mind (Stallings & Brown, 2018. p. 532).

Security training – With security training, it is designed to teach people the skills needed in order to perform their IT related tasks more securely, training teaches them what they should do and how they should do it, this is also extremely dependent on the users and department and levels of them, it can range from basic skills to advanced skills (Stallings & Brown, 2018. p. 534). Typically training will involve how to protect the physical area and equipment such as locking doors, and looking out for USBs and

ports, how to protect passwords if they're used, and how to use and protect other authentication data, it helps teach how and when to report security violations or incidents, and how to identify possible suspicious activity, but it can be more tailored for IT professionals, management, and executives (Stallings & Brown, 2018. p. 534).

17.3 What are some goals for a security awareness program?

There are generally 9 goals for a security awareness program, and these goals are as follows:

Goal 1: Raise staff awareness of information technology security issues in general.

Goal 2: Ensure that staff are aware of local, state, and federal laws and regulations governing confidentiality and security.

Goal 3: Explain organizational security policies and procedures.

Goal 4: Ensure that staff understand that security is a team effort and that each person has an important role to play in meeting security goals and objectives.

Goal 5: Train staff to meet the specific security responsibilities of their positions.

Goal 6: Inform staff that security activities will be monitored.

Goal 7: Remind staff that breaches in security carry consequences.

Goal 8: Assure staff that reporting of potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making behavior).

Goal 9: Communicate to staff that the goal of creating a trusted system is achievable."

(Stallings & Brown, 2018. p. 533).

18.2 List and briefly describe the elements of a security audit and alarms model

The elements of a security audit and alarms model are as follows: event discriminator, audit recorder, alarm processor, security audit trail, audit analyzer, audit archiver, archives, audit provider, audit trail examiner, and security reports (Stallings & Brown, 2018. p. 550 - 551).

Event discriminator – The event discriminator is logic which is embedded into the software of the system that monitors system activity, this detects security related events which it has been configured to detect (Stallings & Brown, 2018. p. 550).

Audit recorder – The audit recorder takes in information from the event discriminator and records/logs it (Stallings & Brown, 2018. p. 550 - 551).

Alarm processor – The alarm processor detects if an event triggers configurable alarm events and then performs an action based on the alarm, this is also an auditable event and gets sent to the audit recorder (Stallings & Brown, 2018. p. 551).

Security audit trail – The security audit trail takes in information from the audit recorder and creates a formatted event and stores it (Stallings & Brown, 2018. p. 551).

Audit analyzer – The audit analyzer gets information from the security audit trail and detects patterns of activity in order to define new auditable events which are sent to the audit recorder and may generate an alarm (Stallings & Brown, 2018. p. 551).

Audit archiver –The audit archiver is a software module which periodically gets records from the audit trail and creates a permanent archive (Stallings & Brown, 2018. p. 551).

Archives – The archives are a permanent store of security-related events (Stallings & Brown, 2018. p. 551).

Audit provider – The audit provider is an application which can have a user interface that allows people to interact to the audit trail (Stallings & Brown, 2018. p. 551).

Audit trail examiner – The audit trail examiner is an application or can be a user who examines the audit trail and the audit archives, they look at trends and perform analysis (Stallings & Brown, 2018. p. 551).

Security reports – Security reports has the audit trail examiner create and prepare human-readable security reports (Stallings & Brown, 2018. p. 551).

18.3 List and briefly describe the principal security auditing functions

The principal security auditing functions are: data generation, event selection, event storage, automatic response, audit analysis, and audit review (Stallings & Brown, 2018. p. 551 - 552).

Data generation – With data generation, it identifies the level of auditing and then enumerates the types of auditable events (Stallings & Brown, 2018. p. 551). After this, it identifies the minimum set of audit-related information provided, while doing this is has

to deal with conflicts between security and privacy as well as identify which events the identity of the user is associated with (Stallings & Brown, 2018. p. 552).

Event selection – In event selection, the inclusion or exclusion of events which are auditable are set, allowing the system to be set to different levels of granularity, or how detailed it is (Stallings & Brown, 2018. p. 552).

Event storage – In event storage, it creates and maintains the secure audit trail as well as provides availability to and prevent loss of data to the audit trail (Stallings & Brown, 2018. p. 552).

Automatic response – The automatic response creates reactions or steps taken by the system on detection of events (Stallings & Brown, 2018. p. 552).

Audit analysis – The audit analysis is provided by automated mechanisms, and analyzes system activity (Stallings & Brown, 2018. p. 552). It identifies the set of auditable events which indicates a potential security violation, and it performs an analysis to determine if a security violation has taken place (Stallings & Brown, 2018. p. 552).

Audit review – In the audit review, it is available only to authorized users who assist in audit data review, it also may include a selectable review function which provides the ability to perform searches which are based upon a single criteria or multiple criteria (Stallings & Brown, 2018. p. 552).

18.4 In what areas (categories of data) should audit data be collected?

The areas in which audit data should be collected are: related to the use of auditing software, events related to security mechanisms, any event that are collected for the use of various security detection and prevention mechanisms, events related to system management and operation, operating system access, application access for select applications, and remote access (Stallings & Brown, 2018. p. 555).

Problem

17.4 A colleague Lynsay recently left the company. However, you find Lynsay in the office late one Friday afternoon, logged into a company computer. What security objectives have likely not been met with respect to Lynsay's termination of employment?

To start off I would like to say that a large number of security objectives as well a privacy objectives have not been met in this situation. A large number of issues could take place as a result of this person's actions. The first big thing that should have taken place was their account credentials be suspended, they should not be able to log into any company computers or systems after they left the company, except in some situations leaving their email active for a few days is fine but should not be able to send outgoing emails or should be monitored. Secondly, at the same time of their computer and account credentials and profiles being suspended they should no longer have access to the building's doors or be in any way able to gain access to the interior of the building in private locations. It is clear that the persons termination did not get sent to the departments which needed to know such as IT and security. It is also possible that

this person had access to doors and locks which are not smart/connected to a smart badge system in which case the combinations and locks should have been changed and keys replaced. As this person was not authorized or was not supposed to be authorized to gain entry into the building and onto their company computer it is possible they broke a number of privacy and security rules such as copying data or sending information out to people who should not have it. An investigation should occur of every action which she performed which relates to this event of her gaining access to the building.

References

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. Pearson.

I have neither given nor received unauthorized aid in completing this work, nor have I presented someone else's work as my own.

Dalton Murray