

Dalton Murray

INT 7223 Cybersecurity

Dr. Hany Othman

June 26, 2023

Chapter 13 - 15 Review

Question

13.1 Define cloud computing

Cloud computing is defined as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [...] that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models (Stallings & Brown, 2018. p. 424). In other words, this means that cloud computing is a service that someone can pay for and use in order to have computing capabilities from anywhere in the world which can be easily scalable.

13.2 List and briefly define three cloud service models

Three cloud service models are as follows: Software as a Service, Platform as a Service, and Infrastructure as a Service (Stallings & Brown, 2018. p. 426).

SaaS – With software as a service the hoster is providing a software to the customer which they pay for, such as application software, which will run on their servers and be accessible anywhere they choose (Stallings & Brown, 2018. p. 426). With SaaS the biggest benefit is the customer doesn't have to setup any software on their own, they pay for the use of the software and that's what they get, such as Google Workspace, or Microsoft 365 (Stallings & Brown, 2018. p. 426).

PaaS – With Platform as a Service the hoster provides a platform to the customer which they can use to setup anything on such as deploying their own software or bought software, it basically allows them to pay for the entire operating system and use how they want (Stallings & Brown, 2018. p. 426).

IaaS – With Infrastructure as a Service the hoster provides the infrastructure itself to the customer, do note though that the customer does not manage or control the resource of the underlying cloud infrastructure but has control over the entire operating system, and in a sense has control over other things such as a firewall or virtual machine (Stallings & Brown, 2018. p. 426 - 427). It allows the customer to select processors they use as well as storage and network capabilities (Stallings & Brown, 2018. p. 427).

13.3 What is the cloud computing reference architecture?

Cloud computing reference architecture is defined as follows "The NIST cloud computing reference architecture focuses on the requirements of "what" cloud services provide, not a "how to" design solution and implementation. The reference architecture

is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference” (Stallings & Brown, 2018. p. 429). In other words, this means that NIST, or the National Institute of Standards and Technology defines cloud computing reference architecture as what cloud service provide, helps people understand the cloud computing operates, and is a tool to describe, discuss, and develop system-specific architecture which uses a common framework for reference (Stallings & Brown, 2018. p. 429). Cloud computing reference architecture is there to act as an illustration to understand cloud services, to use as a technical reference, and to help with analysis of standards such as security (Stallings & Brown, 2018. p. 429 - 430).

13.4 Describe some of the main cloud-specific security threats?

The main cloud-specific security threats are as follows: abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, account or service hijacking, and unknown risk profiles (Stallings & Brown, 2018. p. 435).

Abuse and nefarious use of cloud computing – It is typically easy for someone to freely sign up to a cloud service provider’s services, because of this it enables attackers to get inside of the cloud to conduct different attacks (Stallings & Brown, 2018. p. 436).

Insecure interfaces and APIs – Cloud service providers have a large amount of interfaces open to registered users as well as APIs, because of this it is important to make sure that these are very secure (Stallings & Brown, 2018. p. 436).

Malicious insiders – With cloud services the customer will typically give up some level of security, because of this it is important that the provider has a high level of security as the customer puts a large amount of trust into them, and as a result of this its employees must be extremely trustworthy and have security policies in place (Stallings & Brown, 2018. p. 436).

Shared technology issues – With cloud service providers many customers will often be sharing hardware and because of this it is important to keep them separated and not allow access to each other's resources (Stallings & Brown, 2018. p. 436 - 437).

Data loss or leakage – Data loss or leakage is very important in security as the provider must have a high level of security to prevent data loss and leakage (Stallings & Brown, 2018. p. 437).

Account or service hijacking – This will typically occur with stolen credentials, with stolen credentials anyone can access the account and will break confidentiality and security (Stallings & Brown, 2018. p. 437).

Unknown risk profile – The customer gives up a large amount of privacy and security to the provider and gives the customer an unknown level of risk (Stallings & Brown, 2018. p. 437).

14.1 Define IT security management

IT security management is defined as “the formal process used to develop and maintain appropriate levels of computer security for an organization’s assets, by preserving their confidentiality, integrity, availability, accountability, authenticity, and reliability” (Stallings & Brown, 2018. p. 460). In other words, this means that IT security management is the process in which an organization uses to protect their assets by using computer/cybersecurity.

14.2 List the three fundamental questions IT security management tries to address

The three fundamental questions IT security management tries to address are as follows: what assets do we need to protect, how are those assets threatened, and what can we do to counter those threats? (Stallings & Brown, 2018. p. 459).

14.3 List the steps in the process used to address the three fundamental questions

The steps in the process used to address the three fundamental questions are the same steps in the IT security management process, and these are as follows:

Determine the organization’s IT security objectives, strategies, and policies

Perform an IT security risk assessment

Select suitable controls

Write plans and procedures to implement controls

Implement the controls

Monitor the operations

Detect and react to incidents (Stallings & Brown, 2018. p. 460 - 461).

15.1 Define security control or safeguard

A security control, safeguard, or countermeasure are defined as “an action, device, procedure, or other measure that reduces risk by eliminating or preventing a security violation, by minimizing the harm it can cause, or by discovering and reporting it to enable corrective action” (Stallings & Brown, 2018. p. 490). In other words, this means that a security control, also interchangeably used as a safeguard and countermeasure are an action, device, procedure, or any other measure which is being taken by someone or something which reduces risk by a number of different ways such as preventing security violations.

15.2 List and briefly define the three broad classes of controls and the three categories each can include

Three broad classes of controls are as follows: management controls, operational controls, and technical controls (Stallings & Brown, 2018. p. 490). The three categories each of these controls can have are as follows: supportive controls, preventative controls, and detection and recovery controls (Stallings & Brown, 2018. p. 491).

Management Controls – Management controls focus on security policies, planning, guidelines, and the standards which influence the selection of operational and technical controls (Stallings & Brown, 2018. p. 490). In general, management controls are the controls which refer to the issues that management needs to address (Stallings & Brown, 2018. p. 490).

Operational Controls – Operational controls relate to addressing the correct implementation and the use of security policies and standards (Stallings & Brown, 2018. p. 490). Operational controls ensure that the security operations and correcting identified operational deficiencies are consistent (Stallings & Brown, 2018. p. 491). Operational controls, will in general, relate to mechanisms and procedures in which they are primarily implemented by people rather than systems (Stallings & Brown, 2018. p. 491).

Technical Controls – Technical controls focus on the correct use of hardware and software security capabilities (Stallings & Brown, 2018. p. 491).

Supportive Controls – With supportive controls they are pervasive, generic, underlying technical IT security capabilities which are also interrelated with other controls (Stallings & Brown, 2018. p. 491).

Preventative Controls – Preventative controls will typically focus on preventing security breaches from occurring in the first place, and they do this by inhibiting, or preventing, attempts that violate security policies or can exploit vulnerabilities (Stallings & Brown, 2018. p. 491).

Detection and Recovery Controls – Detection and Recovery tools also focus on the response to a security breach, such as warning people of violations or attempts at violating security policies, they also provide means to restore the resulting lost computing resources (Stallings & Brown, 2018. p. 491).

15.8 What checks does the organizational security officer need to perform as the plan is being implemented?

The organizational security officer needs to check that: the implementation costs and resources are within the identified bounds, the controls are correctly being implemented how they have been specified in the plan to achieve the identified reduction in risk level, and the controls are being operated and administered as needed (Stallings & Brown, 2018. p. 499).

Problem

14.1 Research the IT security policy used by your university or by some other organization you are associated with. Identify which of the topics listed in Section 14.2 this policy addresses. If possible, identify any legal or regulatory requirements that apply to the organization. Do you believe the policy appropriately addresses all relevant issues? Are there any topics the policy should address but does not?

I have elected to use the IT security policies used by my current work. The topics listed in Section 14.2 are as follows:

“The scope and purpose of the policy

The relationship of the security objectives to the organization’s legal and regulatory obligations, and its business objectives

IT security requirements in terms of confidentiality, integrity, availability, accountability, authenticity, and reliability, particularly with regard to the views of the asset owners

The assignment of responsibilities relating to the management of IT security and the organizational infrastructure

The risk management approach adopted by the organization

How security awareness and training is to be handled

General personnel issues, especially for those in positions of trust

Any legal sanctions that may be imposed on staff, and the conditions under which such penalties apply

Integration of security into systems development and procurement

Definition of the information classification scheme used across the organization

Contingency and business continuity planning

Incident detection and handling processes

How and when this policy should be reviewed

The method for controlling changes to this policy”

(Stallings & Brown, 2018. p. 463 - 464).

Upon reviewing my work's IT security policy, it does in fact address all of these topics listed as well as quite a few more. Given my work there are quite a few legal and regulatory requirements which apply to the organization. A majority of the legal and regulatory requirements involve the privacy of the customers, who can access the data, how they access the data, and how long and what data can be stored. We are also required to comply with multiple international guidelines such as the EU's General Data Protection Regulation, also known as GDPR. Continuing, we are required to have and follow standards for disclosing information such as if a breach were to happen or a vulnerability found. I believe our current policy appropriately addresses all relevant issues and that it has no missing topics that it should address.

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