ISA Assessment of an Organization’s IT systems.

Kennith Thurman

School or Institution Name (University at Place or Town, State)

**ISA Assessment of an Organization’s IT Systems**

**Introduction:**

Information technology and communication systems play an important role in modern business. Advancements made in information and communication technologies over the years have changed the way people do business. Almost all of the modern enterprise or even small to medium-sized businesses rely on information technology equipment. Information technology is used to achieve business goals and embedded in business processes. All modern businesses harnessing the power of information technology, utilize the state of the art technologies for data processing (Englbrecht, Meier, & Pernul, 2019). The data being processed by modern businesses often contain personally identifiable information of customers collected through various sources. It also includes direct business processes that rely on such data for service delivery. Exponential penetration of information technology systems into modern businesses have also made them a potential target of cybercriminals.

 Where every organization claim to be the best in protecting their customer's data, the headlines are always filled with successful news of data breaches on such organizations. Increased reliance on businesses has shifted the attention of cybercriminals from targeting individual users to enterprise businesses. Cybercrime is developing as an industry and real businesses are facing challenges in securing their critical infrastructure from cyber-attacks. Cybercriminals are always trying to devise new and improved methods of breaching the available defense mechanisms of enterprise information systems (Wood & Vickers, 2018). There are various frameworks in place to help organizations in securing critical information technology infrastructure. The basic goal of all of the frameworks is to ensure the confidentiality, integrity, availability, and non-repudiation of data systems. Most organizations fail due to inefficient system configurations or lack of investments for appropriate infrastructure developments. It is hard for security managers to impress and convince higher management to invest in secondary systems to protect primary installations.

 To overcome these and various other challenges faced by organizations in securing critical information infrastructure, information security assurance capability maturity model has been developed. It is also known as ISA-CMM framework. The framework requires organizations to build security into the business process. Information security must be a part of the business plan and it must be built into the business goals. Information security strategy must align with the business goals. Capability maturity model for information security assurance helps organizations to evaluate their existing infrastructure for compliance with the framework. The case study explains the assessment of an organizations data storage systems based on ISA-CMM framework version 3.2. During the study, various vulnerabilities and risks were discovered in the data storage systems and mitigation strategies were formed as per the capability maturity framework.

**Discussion:**

The most valuable and critical asset of any modern organization is the data storage system of the organization. Modern businesses rely on extensive data processing. Cloud computing paradigm has shifted the data storage from local storage systems to cloud ones. But the shift in storage system paradigm has not resolved the problem of targeted attacks and data breaches. Although virtualization and cloud computing solutions have solved the problem to some extent in the broader picture the risks have increased as well (Yu, 2018). Most of the businesses are not ready for migration to cloud servers due to privacy concerns and lack of regulation in this regard. An assessment of an organization's local data storage systems has been made based on the ISA-CMM framework. The organization provides data analytics services to global clients by employing state of the art data analytics technology. Data is received, processed, and stored into storage systems continuously. Data streams related to market analysis also contain personally identifiable information of clients. Securing such information storage and processing systems is the responsibility of the organization. The organization claims to be the best in protecting data storage systems but the assessment results suggest otherwise.

 Local data storage systems consist of twenty servers interconnected with the internal network of the organization. Some servers and their communication topologies further divided into smaller networks for redundancy purposes. Most of the services offered by these data storage servers are accessible from external networks as well. A single server was configured to perform authentication and authorization services for the entire fleet of data storage systems in the organizational network (Jacobs, 2015). Authentication requires the identification of the person requesting access to the resources. Authorization deals with the access restrictions at the second step of the authentication. Meaning that it controls that the host will have access to what resources after successful authentication. The basic line of defense against any remotely accessed service is to use strong authentication and authorization systems.

 During the assessment, it was discovered that the authentication server was configured to use password-based authentication system without any additional password policies making the system potentially vulnerable to hacking attempts. Simple password-based authentication systems can be compromised by password sniffing or packet sniffing attacks along with man in the middle type of attacks. Once an attacker is able to compromise the authentication system then all of the other logical measures for data security can also be breached. Although the organization has not experienced any attack bypassing their authentication system but lack of basic password policies made the system highly vulnerable (Wahlgren, Fedotova, Musaeva, & Kowalski, 2016). The severity of the vulnerability was rated as critical and there was a high likelihood of the breach as per the capability maturity model of information security assurance. As the mitigation steps, it was recommended to implement a password policy as soon as possible. When designing security infrastructure, the most difficult aspect is to find the best balance of security and usability. For example, a most secure system will be one that is not connected to anything such as not even connected to power source. And then buried into the earth inside a concrete block. The system is no doubt the most secure system in the world as it cannot be accessed or breached by anyone. However, on the other hand, the same system will be the most useless system on earth as well as it cannot be used at all.

 Therefore, implementing security means finding the optimal balance between security and usability of the system. The goal of information security assurance capability maturity model is to help organizations to minimize the security and usability tradeoff. In the current situation of the organization a password policy that requires the users to use complex passwords can be implemented. But the policy will kill the usability of the system as well because it will be hard for the employees and service users to remember a bunch of complex passphrases. As a result, people will tend to write down the passcodes as hand notes making the system even more vulnerable (Le & Hoang, 2017). Thus an incorrectly configured security policy will make the system more vulnerable instead of increasing security. The basic goal of information security assurance is to create the culture of secure practices used by the employees without compromising the security and usability of the system. A good password policy will require users and employees to use a strong password that must be eight characters long. Along with the length requirement, the policy must state that the user is required to use a combination of lowercase letters, uppercase letters, numerical values, and special characters. Use of all these characteristics will make the password secure enough to survive dictionary attacks.

 Dictionary attacks are a type of attack in which criminals try to bypass the authentication system using all of the password combinations found in a dictionary. Therefore, it is highly recommended not to use dictionary words as passphrases for critical information systems. Moreover, a policy can implement that the password must be changed after a predefined interval such as after six months. It will ensure the password re-use conditions as the users are tempted to use a single password for multiple services they use. Password rotation is compulsory and it is never recommended to use the same password for multiple accounts. Given all of the password hardening policies and requirements, the authentication system cannot be considered as reliably secure against sophisticated attacks (Doss, Tesiero, Gokaraju, Mc Elreath, & Goza, 2017). Stated password policy can work for end users but may not be enough for the employees working with sensitive personal information of clients. The solution is the implementation of the two-factor authentication system. A two-factor authentication system will provide an extra layer of security making the system more complex for criminals to breach the defenses.

 Multiple systems are available for two-factor or multifactor authentication such as one-time password based logins, facial recognition, and fingerprint scanners. All of these authentication systems are based on something the user has, something the user remembers, and something that belongs to the actuals user for identification purpose. Something the user has can be a credit card, something the user remember is the password, and something that belongs to the user is the biometric verification through a fingerprint. The most secure factor is something that belongs to the user such as biometrics as they cannot be duplicated with ease. However, there are certain cases in which researchers were able to bypass fingerprint validation systems. But the probability of such attacks is very low and close to zero for enterprise systems. A layered approach to security of the system will increase the capacity of the system to defend against the digital dark arts.

 Authorization system of the organization was also vulnerable due to the poor segregation of data systems inside the network. The organization was not maintaining the recommended level of data segregation for different departments. For example, data related to the finance department was easily accessible to the customer support department. The organization was informed about the vulnerabilities and steps to mitigate the risks of data breaches due to poor segregation of confidential data. All of the data storage servers were accessible from external networks even the system perceived to be only internal due to poor configuration of firewall rules. Network level firewall was installed but not configured to close unused ports on the network allowing hackers to exploit the firewall defenses. To mitigate the risk the firewall was configured to drop all incoming traffic on any port for internal servers of the organization making them invisible from external networks (Bloomfield, Bishop, Butler, & Netkachova, 2017). Data storage server’s segregation was achieved by the implementation of virtual local area networks on switch level. Network switches were configured to block the access of one department for the data of other departments. Along with network-based firewall it was recommended to use host-based firewalls as well because a host-based firewall will protect the internal network of the organization from being compromised. It will also help in the isolation of an infected host from the network.

 The organization was informed about the benefits and appropriate configuration of network intrusion detection systems that will protect any attempt to compromise the network. It must be configured at a point with the network firewall so, that the traffic from all of the internal network nodes can be monitored. It was also discovered that the organization was storing logs of network activity and access requests on different servers. There was no mechanism of analyzing the logs and central management of the logs as well making it extremely difficult for the organization to reconstruct the attack events in case of successful breach of the defenses. The risk was mitigated by the installation of central log storage and analysis system secured by a reverse proxy configuration. It was necessary as targeted attacks and advanced persistent attacks try to wipe out the log files to obscure the forensic investigation paths for researchers.

**Conclusion:**

It is of vital importance for organizations to secure their information technology infrastructure from cyber-crimes. There are many frameworks available to organizations for securing infrastructure with legal implications and regulations. Information security assurance based on capability maturity model is the best framework for most of the organizations to align their information security infrastructure to their business goals. It requires organizations to implement security into processes at the domain level. The case study of the organization revealed many vulnerabilities including some critical risks. All of the risks were mitigated as per the ISA-CMM framework and assigned appropriate recommendations along with comprehensive suggestions for strategic security policy implementation.

**References**

Bloomfield, R., Bishop, P., Butler, E., & Netkachova, K. (2017). Using an assurance case framework to develop security strategy and policies. *International Conference on Computer Safety, Reliability, and Security*, 27–38. Springer.

Doss, D. A., Tesiero, R., Gokaraju, B., Mc Elreath, D., & Goza, R. (2017). Proposed derivation of the Integrated Capability Maturity Model as an environmental management maturity model. *Energy Environ. Eng*, *5*, 67–73.

Englbrecht, L., Meier, S., & Pernul, G. (2019). Toward a Capability Maturity Model for Digital Forensic Readiness. In *Innovative Computing Trends and Applications* (pp. 87–97). Springer.

Jacobs, S. (2015). *Engineering information security: The application of systems engineering concepts to achieve information assurance*. John Wiley & Sons.

Le, N. T., & Hoang, D. B. (2017). Capability Maturity Model and Metrics Framework for Cyber Cloud Security. *Scalable Computing: Practice and Experience*, *18*(4), 277–290.

Wahlgren, G., Fedotova, A., Musaeva, A., & Kowalski, S. (2016). IT Security Incidents Escalation in the Swedish Financial Sector: A Maturity Model Study. *HAISA*, 45–55.

Wood, P. B., & Vickers, D. (2018). Anticipated impact of the capability maturity model integration (CMMI®) V2. 0 on aerospace systems safety and security. *2018 IEEE Aerospace Conference*, 1–11. IEEE.

Yu, D. (2018). *Method Study on Information Safety Capability Evaluation of Internet Finance Enterprise*.