**How information security maturity model helps organizations to improve information assurance.**

Kennith Thurman

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

# Introduction:

Information technology plays the role of utility in modern business. It is hard to imagine any modern business without the implementation of information technology. Exponential penetration of information technology is subject to the reduction in price and size of information and communication technology equipment. Most of the modern business involve processing of personally identifiable information to ensure business continuity. When businesses have to deal with personal information then most critical asset of the organization is the data that the organization use to earn revenues. When data is the critical asset for the business then security of the data is the obligation of the organization as well. As cyber-attacks are increasing both in numbers and complexity as well, it is inevitable to ensure confidentiality, integrity, availability and no-repudiation of the data. Information assurance is the concept that deals with these aspects. The paper describes and evaluates that how information security maturity model helps organizations to ensure confidentiality, integrity availability and non-repudiation of data.

# Literature Review:

Miniaturization of microprocessors and price cuts in information and computer technology has enabled organizations to include information technology solutions in their business plans. Modern business relies on information technology equipment. All of the information technologies incorporated into businesses processes deals with the critical information related to the business (Jacobs, 2015a). The information processed by organizations often contain personally identifiable information. As more businesses have incorporated information and computer technologies into their operations the more the risks are now associated with these technologies.

When customers are trusting the organizations with their information then it is the responsibility of the organization to protect that information from all possible threats. Most valuable asset in any organization is the data they hold in their information systems. Protection of such data involves ensuring the confidentiality of the data. Confidentiality of data means that the data is only accessible by the authorized persons. For example, the data related to finance and accounting must only be accessible by the finance or accounts department of the organization and no one else should ever be able to breach that information (Duncan & Whittington, 2014). Ensuring the integrity of data means that the information has not been forged in any way. For example, the data related to finance has not be modified by an employee from another department. It may be an attacker who can make unwanted changes to the information. Therefore, integrity deals with the modification or forging of available information (Bozkus Kahyaoglu & Caliyurt, 2018). Ensuring availability of data means that the data and information must be available to the authorized persons whenever they need that information. For example, if an accountant has to generate payroll and he is unable to access the data related to accounts. In such conditions the possible cause may be a system downtime or a cyber attack in progress.

Traditionally information security is considered to be the achievement of confidentiality, integrity, availability, and non-repudiation of data. However, in modern businesses when cyber criminals use sophisticated attack methods ensuring the primary goals is not considered to be effective information assurance plan. Effective information assurance plan and implementation is to prevent all types of attacks instead of post attack investigations and restoration(W Krag Brotby & Hinson, 2016) . Organizations all across the world suffered targeted attacks by the criminals due to the weak information assurance strategies implementations. Target corporation is an example of such attack, when they suffered from one of the largest data breach in history. Hackers were able to compromise their point of sale network and captured millions of records of personally identifiable information from their systems. The attack was successful due to the poor segregation of confidential and ordinary data in their local database systems. Most interesting thing that is revealed during the post attack investigations is that the organization has implemented an information security program but the system administrators has turned off the essential features to prevent such type of attack. The situation was considered to be the result of isolation between security officers and other departments for intelligence sharing.

# Discussion:

 For organizations to ensure security of the most critical asset of the organization to implement security in planning phase of the business as well. Information security maturity model is not linked to responding cyber attacks but to create a security architecture that can prevent the attacks as well. Security related operations of the organization will only be carried out effectively if the processes are built with security infrastructure in mind as well as the future developments in the system (Abraham, Dutta, Mandal, Bhattacharya, & Dutta, 2018). Various factors affect the information security efforts at an organization such as governance, system architecture, culture of the organization and delivery of services to the customer. An effective way of assessing the information security maturity of the organization is information security maturity model. Information security maturity model helps the organizations to achieve their goals against digital darks.

A domain-oriented approach is recommended to implement information assurance and security. Any model developed by using the domain-oriented approach will be effective if the culture of the organization allows the system to perform. If the model is developed without understanding the culture of the particular organization, then the model will not be able to achieve intended benefits for the organization. In domain-oriented model development for information assurance, the senior management of the organization must become more literate in information technology to effectively craft business strategy. In information assurance implementation, people, systems, information, and networks affect each other. These are the four factors that are considered to be the dynamic links between all of the interconnections at an organization. All these four domains there are several processes that are used to measure, identify, and control the risks. All these factors must be considered while developing an information assurance plan or strategy for an organization because the success of the plan or strategy at the end will depend on the in-house information technology capability and reliance on the outsourcing.

**Information Security Maturity model:**

Information security is not about responding to attacks and investigations of security incidents. Instead information assurance is related to prevention of information assets against attacks. Information security is about achieving of organizational goals despite the security accidents if any. Most of the time these security objectives are not achieved because they are viewed in isolation as compared to the other organizational goals. It is due to the financial expenditures that the organization has to made on security equipment and control of the processes. Some efforts of security may not result in intended benefits due to the lack of financial support by senior managers of the organizations (Cambou, Flikkema, Palmer, Telesca, & Philabaum, 2018). It is hard for security managers to convince higher management to make investments on a new system to protect an existing system and the system is not visibly expected to add value to the business products.

 Only way of harvesting maximum benefits out of security investments is to build security in business processes. It can be achieved by making security strategies a part of planning and designing phase of business plan. Adding security layers at a later stage may not be fruitful and it would be difficult to convince higher managers for considerable investments on secondary systems. Mangers of the organizations must be literate in security so that they can make an informed decision about the security needs of processes (Chapple, Stewart, & Gibson, 2018). A domain-based approach will also help in development of effective security strategies. Security processes divided into domains will help organizations achieve goals of confidentiality, integrity, availability, and non-repudiation of data. Concept of information assurance maturity is being applied to the organizational processes to assess the capabilities of existing system as well as to determine the need of new systems. It is based on the levels of compliance for existing systems.

**No-Compliance:**

 Compliance levels are based on the time slots during which a system is exposed to security threats. It is also known as the vulnerability window. A system having vulnerabilities either in hardware infrastructure or software is like a house having a locked door but with a window left opened for attackers. A vulnerability plays the role of that window in the locked home. No compliance state is state of the system during which the system. In this state there eist vulnerabilities in the system that are already exploited by the criminals and the organization has zero days left to fix these vulnerabilities.

**Initial level of Compliance:**

At initial level of compliance, the vulnerabilities in application or hardware systems are not fully patched. Some of the systems have no security holes at all and some of the systems have no security patch installed. It is also known as the state of partial compliance. In which some of the systems comply with the organizational security policy and some are not compliant at all.

 The vulnerability is considered to be an open window for an attacker in a locked room. The lock at the door of the room will be useless if the window is left open. Therefore, it is critical for security operations teams of the organizations to close such windows immediately as soon as the vulnerability is discovered. Security operations team may need to install security patches for software products or harden the security policies according to the latest signature of the discovered vulnerability in the system. Information assurance and security maturity model deals with minimization of the vulnerability window. Vulnerability window is the time frame during which the vulnerability exists in the system to be attacked by the criminals. Minimizing this window to the possible limit is the actual practice of securing any information system.

**Basic Compliance:**

 Basic level of compliance corresponds to a state of the system in which all of the machines are patched with available patches from vendors but there are some known issues with the operation of the system. These operational errors make the system to qualify for the basic level of compliance, but it cannot be designated as fully compliant with the organizational security policy. During the state organization may have little implementation of security procedures, policies, and systems. Information technology departments may have assigned duties, but the implementation is poor regarding the use of services.

 Some organizations do not consider the interaction between the users and systems as risks. It may be due to the fact that a user may not pose any risk to the system in isolation mode. But in enterprise environments there is no or little-known isolation of systems and their corresponding users. In networked environments a large number of risks are initiated by the actions of the users. Thus, user actions are considered to be the initiation of a large-scale attack on the system. Therefore, interaction between the users and systems must be included in cyber security strategic plan of the organizations. Users of the systems are prone to social engineering attacks. Such as any employee may find a data traveler at a public place and may connect it to the system out of curiosity. That action may lead to severe consequences in case of infected device. A major cyber-attack campaign known as Stuxnet was successful due to social engineering tactics employed by the attackers.

**Acceptable Compliance:**

Acceptable compliance is the state of the system when all of the connected devices are patched by the central security officers and managed by the information technology departments security team. They will make sure that system have the patches installed. It is acceptable state of the system because apparently there are no threats to the system. On the other hand, there may be several vulnerabilities that are not known to local staff. Such vulnerabilities can be exploited by the criminals.

 As in many studies and investigations it has been revealed that user interaction with system can pose a serious risk to overall information technology infrastructure of the organization. In many cases the user of the system goes for the easiest option to perform a complex task. In doing so the user may trigger an attack as well because going for plaintext data storage may be vulnerable to eavesdropping. There is a mindset of organizations that consider it a fault of the system designer instead of the user. They claim that it is the fault of the designer to create an easy option for performing the same job. To eradicate such problems in organizational networks there must be a culture of security among people working in organization.

 It has been observed in many organizations that information technology support executives configure different passwords for different applications. They consider the move as application hardening which is not true in reality because in this way the user has to remember multiple passwords. Such passwords are changed regularly reducing the capability of user to memorize the passwords. The result is that a user may write down passwords to avoid any confusion. It is a practice that must be discouraged in anyway. Passwords must never be stored in plaintext format. To promote culture of security in organization there must be appropriate meetings between security teams and users to educate them about possible threats to information systems being used.

**Full Compliance:**

In this state the system is in full compliance with the information assurance strategic plan of the organization and equipped with the capabilities of halting down nay future threats to the system. The system is capable of halting down targeted attacks or at-least an early warning system to make the response effective. To make an organization fully compliant to information security policies and procedures security is managed by identifying security concerns. Security incidents are tracked in a systematic way (Wahlgren, Fedotova, Musaeva, & Kowalski, 2016). A full compliance organization must have formal security policies and information assurance items as part of the business plan. A full compliance investigation also considers the security architecture of the organization. As the business architecture of an organization considers all external factors, a security architecture considers the interaction between the systems and their users before implementation of any new policy or procedure.

**Measurements:**

In information assurance and security policies metrics are used to measure and predict future trends based on the analysis of historical data collected over the years in an organization. Security metrics are designed to monitor and as a tool to get insight about the performance of security controls implemented previously. Metrics are required to be designed carefully if they are required to locate failure points and anomalies in security architecture of the organization. Metrics are collected across many different organizations because these are operational metrics without complete information of security processes (Le & Hoang, 2017). It is crucial to maintain redundancy in collecting the operational metrics as an organization may not want to disclose internal information assurance and security infrastructure. On the other hand, collection of operational metrics across organization presents with a more complex and challenging problem of security risks (Ormrod & Turnbull, 2016). The details and properties of different operational security systems may vary during the lifecycle of the system. So, data collected for analysis at one point in time may not be appropriate for an analysis at a later point in time. Any appropriate metrics or measurement framework must be designed in a way to accept the possible changes in target as well as changes in the existing measurement security infrastructure of the organization (Savola, Savolainen, & Salonen, 2016).

 While designing metrics for security assessment of any information technology system the researchers and security engineers must have to choose between the usability of the system and security. For example, a most secure system will be one disconnected from everything even from the power source and buried down the earth in a concrete block. That system will be incredible secure as no one can access the system and breach the information stored in the system (Jacobs, 2015b). On the other hand, the system will be the most useless system on earth because it will not be usable. If a system is so secure that it cannot be used, then there is no point in designing such a system in first place. Information assurance and capability maturity model is about finding the best suitable framework of usability and security for organizations. It helps organizations to minimize the tradeoff between security and usability of any information system. Security assurance measurements often require data aggregation from various sources. It is practical to manage or assess a complex system architecture independently. It is also not feasible because the properties of security infrastructure and implementation goals may change over time in an organization or will drastically change from one organization to the other.

**Metrics in ISA-CMM:**

Metrics used in capability maturity model for information security assurance are based on the principle that the thing that cannot be measured will not be managed. The principle reflects the fact that an organization must be able to measure the risks and define appropriate strategies based on the chosen metrics. Therefore, there are four stages of compliance are defined in the paper to help organizations assess their present security posture and plan improvements for future endeavors (Englbrecht, Meier, & Pernul, 2019). These indicators of security assurance are based on the domain specific goals rather than focused on processes. They measure the aspects of structure, practices, management, and performance of the organization in terms of the security of the information being processed by the organization for business continuity. The practices involved in the paper are for the persons responsible for management of the organizational processes to draw their attention to good processes for information security.

**Limitation of the Study:**

It is evident by the research study that the capability maturity stages and metrics can help organizations to assess their information assurance architecture and formulate future strategies. However, the metrics may not be applicable to every possible business or process in information technology. Particular compliance stages will help organizations to formulate processes at domain level, but the qualitative approach of the model implementation may result in subjective details that may not be appropriate for a particular business. Future research may focus on quantitative metrics for information assurance of an organization based on capability maturity model.

**Conclusion**

 Effective information assurance cannot be achieved without incorporating information assurance in the business plan and implementation phase. It must be applied to the process level to ensure the continuity of the business. Factors must be considered such as people, networks, culture, and system architecture while devising policies to protect information assets. All these factors certainly influence the effectiveness of the strategies for information assurance (Sabillon, Serra-Ruiz, Cavaller, & Cano, 2017). Later investments in the information security model may not yield the expected benefits. As legacy systems may not accept the latest technologies and limitations associated with human factor must also be considered. All these obstacles and vulnerability windows can be minimized by following the information assurance maturity model by the organizations (Kisekka & Giboney, 2018). Depending on the complexity and level of sophistication associated with modern cyber-attacks such as code obfuscation there is no silver bullet to rule all the attacks out of the organization. Therefore, information assurance must be a part of the business plan and exactly coherent to the business goals of the organization.

**References**

Abraham, A., Dutta, P., Mandal, J. K., Bhattacharya, A., & Dutta, S. (2018). Emerging Technologies in Data Mining and Information Security. *Proceedings of IEMIS*, *2*.

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360–376.

Cambou, B., Flikkema, P., Palmer, J., Telesca, D., & Philabaum, C. (2018). Can Ternary Computing Improve Information Assurance? *Cryptography*, *2*(1), 6.

Chapple, M., Stewart, J. M., & Gibson, D. (2018). *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide*. John Wiley & Sons.

Duncan, B., & Whittington, M. (2014). Compliance with standards, assurance and audit: does this equal security? *Proceedings of the 7th International Conference on Security of Information and Networks*, 77. ACM.

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

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

Kisekka, V., & Giboney, J. S. (2018). The effectiveness of health care information technologies: evaluation of trust, security beliefs, and privacy as determinants of health care outcomes. *Journal of Medical Internet Research*, *20*(4).

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.

Ormrod, D., & Turnbull, B. (2016). The Military Cyber-Maturity Model: Preparing Modern Cyber-Enabled Military Forces for Future Conflicts. *11th International Conference on Cyber Warfare and Security: ICCWS2016*, 261.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, 253–259. IEEE.

Savola, R. M., Savolainen, P., & Salonen, J. (2016). Towards security metrics-supported IP traceback. *Proccedings of the 10th European Conference on Software Architecture Workshops*, 32. ACM.

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.