RESEARCH PAPER ON INFORMATION SECURITY

PARTHA MANISH VICHARE

Keraleeya Samajam's Model College , Dombivili East,
Mumbai, Maharashtra, India

Abstract:

Information Security deals with the confidentiality, privacy, integrity, and availability of one of their most valuable resources: data and information. Information Security plays a important role in enterprise management. The core of Information Security includes information risk management a process which involvesthe assessment of the organization must deal with in the management and protection of assests as well as the dissemination of the risks to all appropriate stakeholders.

Introduction:

Information Security is a serious topic that needs to be included in the curricilum of every classroom that uses a computer. It is important for teachers, administrators, and technology coordinators to be informative on this topic in order to protect the intergrity of school records, student information, and institution credibility. But, it is EQUALLY important that we all understand the basics of information security in order to protect themselves and their work.

The COVID-19 pandemic has also had a detrimental impact in cybersecurity world wide, as more collaborators are working from home, which led to accelerate digital transformation in enterprises .
Organizations operating in tightly regulated industry verticals, such as healthcare or finance, may require a broad scope of security activities and risk mitigation strategies.

The ISO-27001:2013 belongs to a family of Information Security Standards. One of the core concepts of ISO-27001 is to identify information security risk and to further apply the appropriate controls that can evaluate and mitigate the risk. Under this family of standards, the ISO-27005 describes risk management methods. Interrelated to cybersecurity, the ISO-27037 fines guidelines that are related to security techniques that may identify, collect, acquire, and preserve a digital evidence.

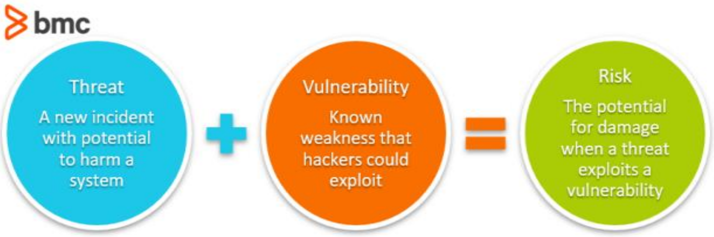
Creation of information security programs includes:

1. Creation of policies, standards, and practices, selection or creation of information security architecture and the development.

2. Use of a detailed information security blueprint creates plan for future success.

3. Creation of contingency planning consisting of incident response planning disaster recovery planning, and business continuity plans

4. Without policy, blueprints, and planning, organization is unable to meet information security needs of various communities of interest.


bmc
Threat
A new incident with potential to harm a system
+
Vulnerability
Known weakness that hackers could exploit
=
Risk
The potential for damage when a threat exploits a vulnerability

What is information security:

Information Security is not only about securing information from unauthorized access. Information Security is basically the pracritce of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or desctruction of informaation. Information can be physical or elecronic one.

Information Security is a discipline to protect information and information system from threats through security controls to:

i) Achieve the objectives of confidentality, integrity, and availability,or CIA for short,

ii) Support the organizational mission and processes, and

iii) Create and deliver values.

Which objective is most important?
i) Confidentality
ii) Integrity
iii) Availibility

History of Information Security:

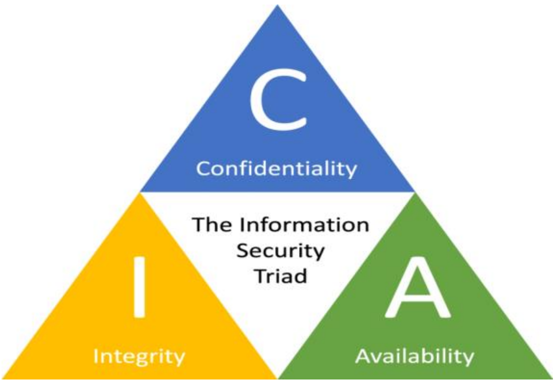
Today, the Internet has brought millions of unsecured networks into communication with each other. The ability for an individual to secure information on a computer relies on how good the overall network security is that the computer is connected to. If an outsider has access to the inside network, it would not take long to access an individual node on that network. Computer security has evolved into a component of acomplex, miltifaceted environment now defined as Information Security.

CIA triangle known as security triad tells the primary goals of Information Security

A) **Confidentiality**
Making sure that those who shouldnot see information.

B) **Integrity**
Making sure that the information has not been changed from its original lastly

C) **Availability**
Making sure that the information is available for use when you need it .



Advantages of information security:

i) Information security is extremely easy to utilize. For protection of less sensitive material users can simply password protect files. For the more sensitive material users can install biometric scanners, firewalls, or detection system.

ii) As technology increases so will the crimes associated with it. Making the use of information security very worth while.

iii) For the government it keeps top secret information and cabalities out of terrorist and enemy nation’s hand.

iv) Information security protects users valuable information both while in use and while it in being stored.

Disadvantages of Information Security:

Since technology is always changing nothing will ever be completely secure. If a user misses one single area that should be protected the whole system could be compromised. It can be extremely complicated and users might not totally understand what they are dealing with

.

i) Technology is always changing so users must always purchase upgraded information security.

ii) Since technology is always changing nothing will ever be completely secure.

iii) If a user misses one single area that should be protected the whole system could be compromised.

iv) It can be extremely complicated and users might not totally understand what they are dealing with

v) It can slow down productivity if a user is constantly having to enter passwords.

.

How Does Information Security Work:

Information security is achieved through a structured risk management process. Identifies information , related assets and the threats, vulnerability and impact of unauthorized access. Evalutes risks. Make decisions about how to address or treat risks avoid, mitigate, share or accept.

Information security is a process that moves through phases building and strengthening itself along way. Security is a journey not a destination. Although the Information Security process has many strategies and activities, we can group them all into three distinct phases- prevention, detection, and response.

Conclusion:

The protection of information and information systems from unauthorized access, use, discloure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Information security or infosec is the protection of information by people and organizations in order to keep information safe for themselves, their company, and clients.

Companies need to be confident that they have strong data security and that they can protect against cyber attacks and other unauthorized access and data breaches. Weak data security can lead to key information being lost or stolen, create a poor experience for customers that can lead business, and reputational harm if a company does not implement sufficient protections over customer data and information security weaknesses are exploited by hackers. Solid infosec reduces the risks of attacks in information technology ststem, applies security controls to prevent unauthorized access to sensitive data, prevents disruption of services via cyber attacks like denial-of-service (DoS attacks) , and much more.

REFERENCE:

1. Ikeda, K.; Marshall, A.; Zaharchuk, D. Agility, skills and cybersecurity: Critical drivers of competitiveness in times of economic uncertainty. In Strategy & Leadership; Emerald Publishing: Bingley, UK, 2019. 2. Huang, K.; Madnick, S.; Johnson, S. Framework for Understanding Cybersecurity Impacts on International Trade. 2019. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3555341 (accessed on 7 March 2021). 3. Al-Sartawi, A.M.M. Information technology governance and cybersecurity at the board level. Int. J. Crit. Infrastruct. 2020, 16, 150–161. [CrossRef] 4. ENISA Threat Landscape. 2020. Available online: https://www.enisa.europa.eu/topics/threat-risk-management/threats-andtrends/ (accessed on 7 March 2021). 5. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput. Secur. 2021, 105, 102248. [CrossRef] 6. Ahmad, T. Corona Virus (Covid-19) Pandemic and Work from Home:

Challenges of Cybercrimes and Cybersecurity. 2020. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3568830 (accessed on 7 March 2021). 7. Nistotskaya, M.; Charron, N.; Lapuente, V. The wealth of regions: Quality of government and SMEs in 172 European regions. Environ. Plan. Gov. Policy 2015, 33, 1125–1155. [CrossRef] 8. Small Business Standards. Available online: https://www.sbs-sme.eu/sme-involvement/standards-and-smes (accessed on 7 March 2021). 9. Kertysova, K.; Frinking, E.; van den Dool, K.; Mariˇci´c, A.; Bhattacharyya, K. Cybersecurity: Ensuring Awareness and Resilience of the Private Sector Across Europe in Face of Mounting Cyber Risks-Study; Technical Report; European Economic and Social Committee, The Hague Centre for Strategic Studies: Hague, The Netherlands, 2018. Available online: https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/cybersecurity-ensuring-awarenessand-resilience-private-sector-across-europe-face-mounting-cyber-risks-study#downloads (accessed on 7 March 2021). 10. Boletsis, C.; Halvorsrud, R.; Pickering, J.B.; Phillips, S.; Surridge, M. Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. In Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2021), Vienna, Austria, 8–10 February 2021. 11. Ozkan, B.Y.; Spruit, M. Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda. In Research Anthology on Artificial Intelligence Applications in Security; IGI Global: Hershey, PA, USA, 2021; pp. 1252–1278. 12. Whitehead, G. Investigation of Factors Influencing Cybersecurity Decision Making in Irish SME's from a Senior Manager/Owner Perspective. Ph.D. Thesis, National College of Ireland, Dublin, Ireland, 2020. 13. Saleem, J.; Adebisi, B.; Ande, R.; Hammoudeh, M. A state of the art survey-Impact of cyber attacks on SME's. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017. J. Cybersecur. Priv. 2021, 1 237 14. Carías, J.F.; Borges, M.R.; Labaka, L.; Arrizabalaga, S.; Hernantes, J. Systematic Approach to Cy