IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 6, Ser. I (Nov - Dec 2019), PP 16-18
www.iosrjournals.org

The Hard Reality of Information Security

OmoyiolaBayoOlushola
School of Information Systems & Technology, Walden University,
Minneapolis, Minnesota, USA

Abstract
The hard reality of information security today is that there would be security risks. Therefore every individual, organization, and government must be prepared to handle these risks. Whether it comes in the form of security vulnerabilities, hacks,data breaches, insider threats, employee errors, or privacy mistakes, all securityrisks must be mitigatedbecause they can cause great havoc. This paper explores the hard reality of information security, analyzing the hard reality of the existence of Information Security risks, threats, and vulnerability, the three pillars of information security, the gaps between defenses, and emerging threats.

Keywords: *Emerging threats, gaps, risks, security, vulnerabilities, attacks, and breach*

Date of Submission: 16-11-2019 Date of Acceptance: 30-11-2019

I. Introduction

The facts about the existence of Information Security risks, threats, and vulnerability are hard to believe, but they are real. Hu, Xu, Dinev, & Ling (2011) reportedthat the annual cost of cyber-attacks is over a trillion dollars. It was also reported that an average of 30,000 websites get hacked every day. Last year, Instagram fell victim to hackers, and data from over 6 million verified accounts on it got stolen. The hackers went to the extent of selling the personal information of the users (IBM, 2018). That attack was an example of a data breach. Many organizations have experienced such and many other cases of security risks. These risks are real. Therefore, the management of organizations must accept them and always be ready to tackle them. Already several organizations across the world have tightened their security to make sure their security risks are brought down to the barest minimum. Cybersecurity has evolved and is consistently developing. Security solution providers work day and night, improving on their security solutions to tackle current and emerging security threats and risks. The current trends of Information Security include GDPR compliance, Internet of Things (IoT) security, cloud data protection, Blockchain application, Data Science and Analytics application and Artificial Intelligence (and Machine Learning) application, Mobile security, etc. (Symantec, 2019; Verizon, 2019). Organizations are now implementing GDPR privacy compliance. Many organizations have also implemented BYOD policies. Mobile security is another current trend. Mobile phone manufacturers have upgraded the security on their phone products. Security solution providers have also now extended the applications of security to modern technologies like IoT, Blockchain, Data Science and Analytics, and Artificial Intelligence (and Machine Learning). On the other hand, hackers have been developing software that would enable them to hack into systems built on these modern technologies (Symantec, 2019; Verizon, 2019).

II. The Pillars of Information Security

The three pillars of Information Security are Confidentiality, Integrity, and Availability. These three pillars are the basis or foundation of every aspect of Information Security. Irrespective of whether the security domain is physical security or administrative control or technical control, business continuity, disaster recovery, system security, risk management, identity and access management, software security, communications, and network security, or security architecture and engineering, etc. The threats to the three pillars are of utmost concern to organizations of all kinds (Jouini, Rabai, &Aissa, 2014). The threats to the three pillars are disclosure, alteration, and destruction. The main threat to confidentiality is disclosure. One good example of the confidentiality attack is the theft of PII (Personally Identifiable Information) such as data in credit cards. The main threat to Integrity is unauthorized alteration or modification. The main danger to Availability is destruction or lack of service. An excellent example of it is a denial of Service which denies availability or service (Conrad, Misena& Feldman, 2011).

III. Gaps between defenses

The gaps between existing defenses include the vulnerabilities found in software, the flaws in the design, insufficient or lack of security awareness education and training, lack of analytics, inadequate security

technologies or lack of it, immature intelligent security systems, lack of an updated security policy, no review of security risk, lack of a mature risk culture, and lack or absence of risk management programs, inadequate budget, and the human aspect which includes internal and external human gaps etc. These could also include risky user behaviors and unintentional carelessness of the employees (Guo, 2013; Lebek, Uffen, Neumann, Hohler, &Breitner, 2014; Safa, Sookhak, Von Solms, Furnell, Ghani, &Herawan, 2015). PwC (2017) explained that a proper security budget, security policies, security technologies, security strategy, and review of security and privacy risks are extraordinary security measures. These are like the defense-in-depth strategy in Figure 1 below.When these security measures are lacking in any standard organization, gaps are bound to exist in their security architecture.

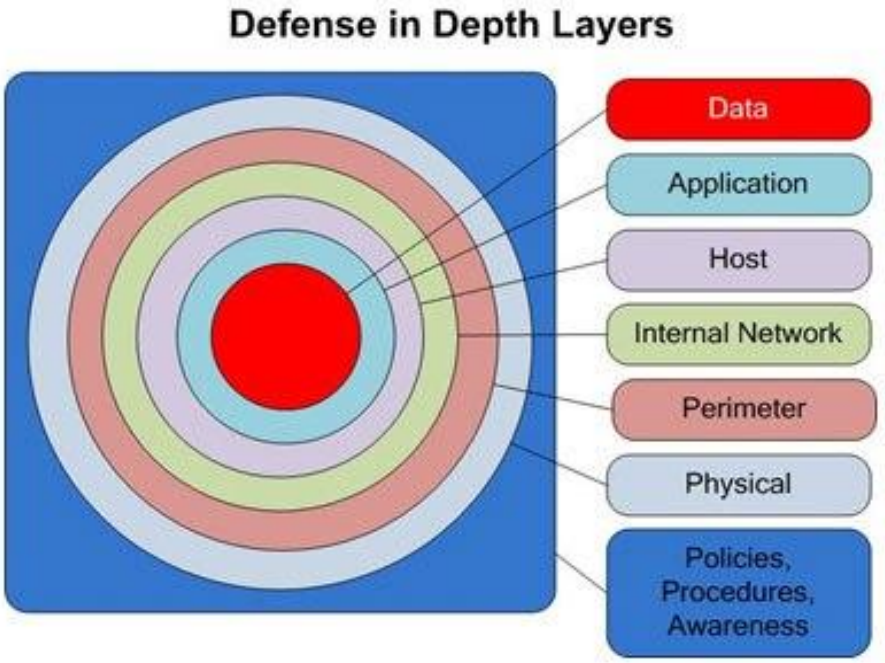

Figure 1. Defense-in-depth strategy

IV. Emerging Threats

The emerging security threats include ransomware, malware, phishing, IoT hacking, Cloud hacking, Artificial Intelligence hacking, Data breaches, Blockchain attacks, Cryptocurrency mining, MagecartMalware, Mobile malware, attacks on biometric systems, Cyber espionage and Zero-day vulnerability, etc. The tools of hackers are getting more sophisticated. With Ransomware, hackers get paid after they have taken over the system of their victims. Microsoft (2019), however reported that the number of ransomware attack incidents has reduced.In contrast, Symantec (2019) said that ransomware could attack Cloud service in 2019. Hackers still use malware and phishing to penetrate the accounts of organizations and individuals (Microsoft, 2019). Microsoft (2019) reported that malware and phishing attacks still occur. Hackers hack Mobiles and Biometric systems and also hack Systems with IoT, Cloud services, Artificial Intelligence, Cryptocurrency, and Blockchain. Some organizations have suffered immensely from data breaches. These data breaches have led to a significant financial loss, loss of consumer data and confidence, and increased liability (Sen &Borle, 2015). Breaches are attacks on the Confidentiality, Integrity, and Availability of data (Laube& Bohme, 2016; Zafar, Ko, &Osei-Bryson, 2016). Symantec (2019) reported how Facebook suffered a data breach in September 2018, exposing personal data of over 30 million of its account users. A data breach is still a threat. Cryptojacking and malicious power scripts are also threats. Artificial Intelligence hacking could also be an emerging threat. Hackers could use it to develop more sophisticated malicious software (Symantec, 2019). Verizon (2019) reported about the Zero-day vulnerability, Backdoor, Spyware, Cyber-espionage, MagecartMalware, Ransomware credential attacks, and Cryptocurrency attacks are also threats of 2019.

V. Conclusion

The existence of Information Security risks, threats, and vulnerability is an actual reality.Vulnerabilities, hacks, data breaches, insider threats, employee errors, andprivacy mistakes do exist, and they must be mitigated to prevent danger on all levels. While it is true that cyber attacks could sometimes be hard to stop, the reality is that they can be mitigated (Omoyiola, 2018). Individuals, organizations, and

governments must implement security controls to ensure that their data and assets are well secured. The hard reality of information security was explored in detail, as the three pillars of information security, the gaps between defenses, and emerging threats were analyzed.

References

[1]. Conrad E., Misena S. & Feldman J. (2011). *Eleventh hour CISSP study guide 11th hour*. Burlington, MA: Elsevier

[2]. Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242-251. doi:10.1016.j.cose.2012.10.003

[3]. Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54(6), 54–60. doi:10.1145/1953122

[4]. IBM (2018). Introduction to Cybersecurity. Retrieved from: https://dw1.s81c.com/caas-storage/skillscollection/dna/africa-prod/explorer-cybersecurity/en/_attachments/Intro-to-Cybersecurity.pdf

[5]. Jouini, M., Rabai, A., &Aissa, B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496. doi:10.1016/j.jprocs.2014.05.452

[6]. Laube, S., & Bohme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, *2*(1), 29-41. doi:10.1093/cybsec/tyw002

[7]. Lebek, B., Uffen, J., Neumann, M., Hohler, B., &Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *ManagementResearch Review*, *37*(12), 1049-1092. doi:10.1108/MRR-04-2013-0085

[8]. Microsoft (2019). *Microsoft security intelligence report.* Retrieved from: https://info.microsoft.com/SIRv24Report.html

[9]. Omoyiola, B. O (2018). The legality of ethical hacking. *IOSR Journal of Computer Engineering (IOSR-JCE). 20* (1), 61-63.doi: 10.9790/0661-2001016163

[10]. PwC (2017). *Strengthening digital society against cyber shocks.* Retrieved from: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks.html

[11]. Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., &Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computers & Security*, *53*65-78. doi:10.1016/j.cose.2015.05.012

[12]. Sen, R., &Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314-341. doi:10.1080/07421222.2015.1063315

[13]. Symantec (2019). *Cyberthreat trends: 2019 cybersecurity threat review*. Retrieved from: https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html

[14]. Verizon (2019). *2019 Data breach investigations report.* Retrieved from: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[15]. Zafar, H., Ko, M. S., &Osei-Bryson, K. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers*, *18*(6), 1205-1215. doi:10.1007/s10796-015-9562-5