Towards a Resilient Digital Ecosystem

Oghenekaro, Linda Uchenna (PhD) & Enyindah, Promise (PhD)
Department of Computer Science
University of Port Harcourt
Rivers State, Nigeria
E-mails: linda.oghenekaro@uniport.edu.ng; promise.enyindah@uniport.edu.ng

Abstract

This chapter x-rayed the cyberspace viz-a-viz cyber criminality, victimization and cyber security. The thrust of the discourse is to identify threats to users in cyberspace occasioned by the exponential increase in the number and complexity of threats, as compared to the shortage of cyber security workforce. The chapter propose cyber security automation as viable tools that can ensure cyber resilience in cyberspace.

Keywords: Cyberspace, Cyber criminals, Cybercrimes, Cyber resilience, Automation, Security

Introduction

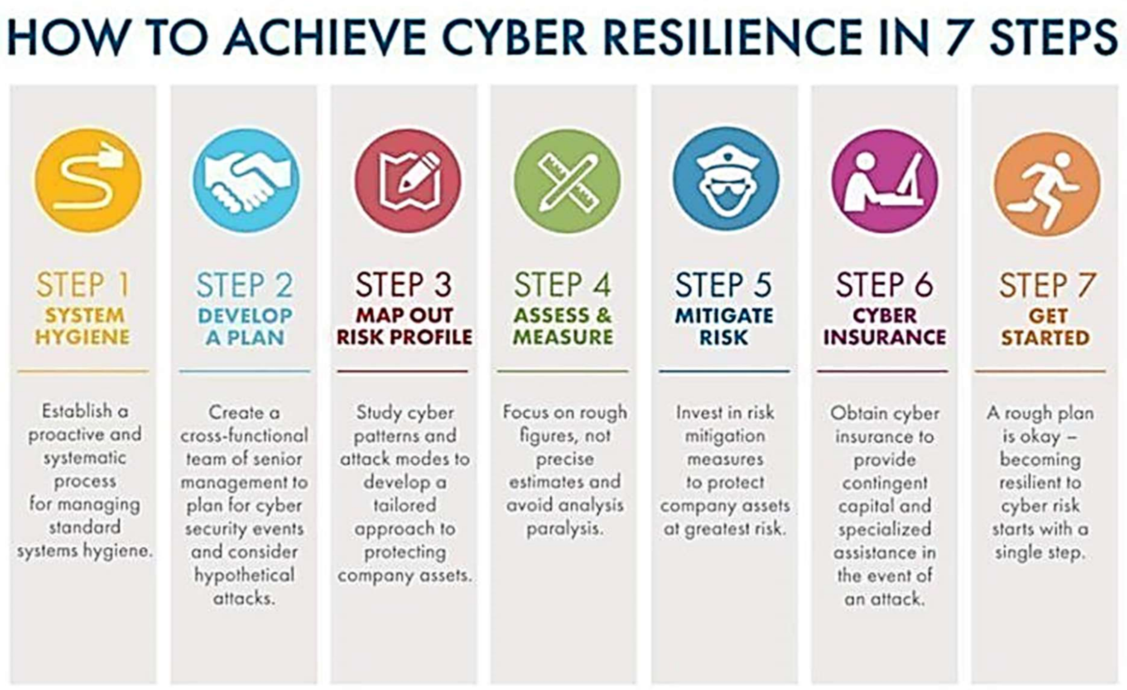
The digital ecosystem has been on a steady expansion, however during the year of the Covid-19 pandemic, it experienced an overwhelming amount of digital activities as businesses and institutions digitalized most of their activities to ensure continuity. This accelerating digital transformation has opened more opportunities for cyber crimes. More of cyber threats are seen in the “working from home” (WFH) practice, where employees use home computers and networks to carry out official transactions, thereby giving uncontrolled access to cyber criminals who take advantage of these weak architectures and unpatched systems.

Since the era of the pandemic, the activities carried out on digital and online environment have increased sporadically, and unfortunately, cyber attacks have also moved in the same direction. Digital transformation has accelerated now more than ever seen in history, as governments and institutions now operate in perimeter-less and interconnected online environment. This has attracted more of cyber crimes, and it is inevitable to have a cyber space without cyber criminals, hence it becomes a proactive step to go beyond cyber security and look towards cyber resilience.

Cyber Resilience

Cyber resilience according to [1] is the ability to prepare for cyber attacks, respond to them and recover seamlessly from these attacks.

Citation Oghenekaro, L.U. & Enyindah, P. (2022). Towards a resilient Digital Ecosystem.
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series
Book Chapter on Web of Deceit - African Multistakeholders’ Perspective on
Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical
and Design Approaches. Pp 261 -264. www.isteams.net/bookchapter2022.
DOI https://doi.org/ 10.22624/AIMS/BK2022-P43



HOW TO ACHIEVE CYBER RESILIENCE IN 7 STEPS

STEP 1 SYSTEM HYGIENE: Establish a proactive and systematic process for managing standard systems hygiene.

STEP 2 DEVELOP A PLAN: Create a cross-functional team of senior management to plan for cyber security events and consider hypothetical attacks.

STEP 3 MAP OUT RISK PROFILE: Study cyber patterns and attack modes to develop a tailored approach to protecting company assets.

STEP 4 ASSESS & MEASURE: Focus on rough figures, not precise estimates and avoid analysis paralysis.

STEP 5 MITIGATE RISK: Invest in risk mitigation measures to protect company assets at greatest risk.

STEP 6 CYBER INSURANCE: Obtain cyber insurance to provide contingent capital and specialized assistance in the event of an attack.

STEP 7 GET STARTED: A rough plan is okay – becoming resilient to cyber risk starts with a single step.

Fig 1: How to Achieve Cyber Resilience in 7 Steps Source:
https://www.cybersecobservatory.com/2018/08/27/achieve-cyber-resilience-7-steps/

A key tool to ensure cyber resilience is cyber security automation, and this is because of the exponential increase in the number and complexity of threats, as compared to the shortage of cyber security workforce [2]. Institutions can however make a move towards maintaining a resilient digital ecosystem by establishing a proactive and systematic process for maintaining standard system hygiene, creating a multi-functional team of senior management to develop a plan for cyber security events, review existing cyber attack patterns and develop a tailored approach to protecting company's assets, focusing on rough figures rather than precise estimates while assessing and measuring, so as to avoid analysis paralysis.

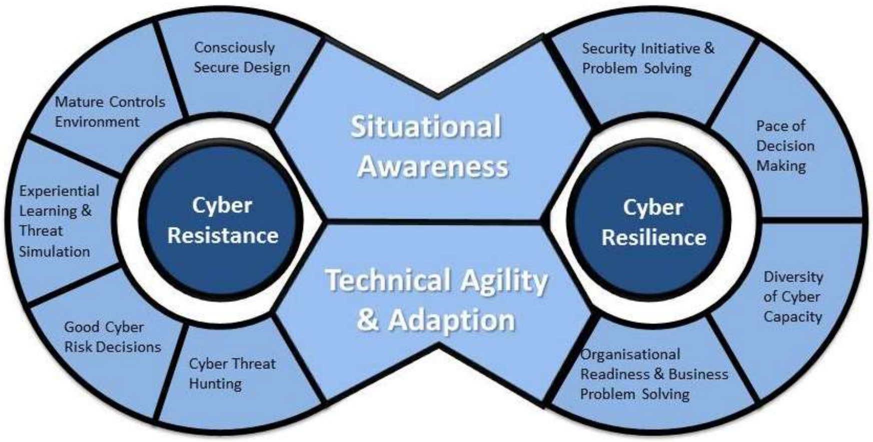

Consciously Secure Design
Mature Controls Environment
Experiential Learning & Threat Simulation
Good Cyber Risk Decisions
Cyber Threat Hunting
Cyber Resistance
Situational Awareness
Technical Agility & Adaption
Cyber Resilience
Security Initiative & Problem Solving
Pace of Decision Making
Diversity of Cyber Capacity
Organisational Readiness & Business Problem Solving

Fig 2: Cyber Resilience Component
Source: https://www.theresilience.ml/cyber-resilience/

Institutions should also invest in risk mitigation measures so as to protect all assets at greatest cyber risk. Cyber insurance should also be obtained to provide contingent capital in unforeseen attacks [3]. Cyber security automation using artificial intelligence techniques and algorithms with yield predictions that will further provide valuable insights which will assist organizations mount multilayered cyber security strategy that will be resilient against disruption and compromise.

Emerging Cyber Security Challenges & Emerging Technologies

Emerging cyber security challenges threatens economic and national security, and security leaders need to pay attention to potential mitigation strategies to help deter the evolving methods of cyber-criminals. While dealing with the present cyber security challenges within the digital ecosystem, the future of cyber security is still worrisome as the wider adoption to digital environment makes individuals and industries more vulnerable to cyber crimes. For instance, the number of IoT devices is expected to surpass 20 billion by 2023, and the consequence of this exponential growth in IoT devices, is that the number is equivalent to the potential access points that cybercriminals look to gain access to digital systems, same goes for edge computing devices [4]. Emerging technologies such as self-driving cars, robots, drones, mobile wallets payment platforms, blockchain networks, internet of senses, quantum computing, cryptocurrency technology, autonomous vehicles, cloud computing, and mobile computing, among others, also opens us more to the vulnerability of cyber crimes.

Cyber Criminality

Cyber criminals carry out cyber theft using common methods such as; Botnets, Phising, Ransomware, Browser Hijacking, Fraud Identity and Flood attacks [5]. These attacks are becoming more frequent each passing day, and institutions are working round the clock in putting a solid incident response plan (IRP) in place to always secure their cyber space. The IRP includes the preparation of the incident response team of every organization, identification of the right security tools to use in collecting evidence and deciding on what to do about every incident, containment of affected systems, identifying the main course of the incident and eradicating it, recovering from the cyber attack and applying measures to prevent similar attacks in future, and finally being able to draw out lesson learned as a team.

Threats to Security of Information Systems

There are several issues that threaten the security of information systems. The ransomware remains the number one threat on the list, as modern ransomware attack has been on the rise [6]. Other types of cyber-attack includes; cloud attacks, phishing attacks, outdated hardware, IoT attacks, malware and various software vulnerabilities [7]. An effective method of tackling cyber attack is by educating users and the public, about the types of threats that lies in the cyber space. Sensitization and awareness talk is a useful tool in protecting the public from these vulnerabilities. A domestic user can adopt some security measures such as installing a firewall as an extra security layer for the personal computer; it is also a good practice to use latest software and hardware for our digital needs [8]. Businesses should also consider cyber security resilience and exposure as a priority factor when establishing partnership and collaboration.

Conclusion

In conclusion, the digitalization of the different aspects of human life has led to creation of a myriad of data, including sensitive data, which if not properly secured and managed will lead to significant damage. In moving from cyber security to cyber resilience, everyone has a part to play, individually and collectively. Emerging technologies will also be leveraged on to maintain a secured cyber space, and there will be a need to grow forensic skills. As cyber attacks become more sophisticated, cyber security measure should also be advanced to curb the menace and ensure a safe cyber space for all.

References

[1] Herrington, L. and Aldrich, R. (2013). The Future of Cyber-Resilience in an Age of Global Complexity, SAGE Journals. 33(4) 299-310. https://doi.org/10.1111/1467-9256.12035

[2] Petrenko, S. A. and Vorobieva, D. E. (2019) Method of Ensuring Cyber Resilience of Digital Platforms Based on Catastrophe Theory. XXII International Conference on Soft Computing and Measurements (SCM). 97-10 https://doi.org/10.1109/SCM.2019.8903658

[3] Linkov I., Kott A. (2019) Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: Kott A., Linkov I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham. https://doi.org/10.1007/978-3-319-77492-3_1

[4] Hillard Heintze The Front Line 2020 Report

[5] Danquah, P. and Longe, O. B. (2011) Cyber Deception and Theft: An Ethnographic Study on Cyber Criminality from a Ghanaian Perspective. Journal of Information Technology Impact. 11(3). 169-182

[6] Graeme, P., Herd, D. P. and Sean, C. (2013) Emerging Security Challenges: Framing the Policy Context. Geneva Centre for Security Policy

[7] Jang-Jaccard, J. and Nepal, S. (2014) A Survey of Emerging Threats in Cybersecurity. Journal of Computer and System Sciences. 80(5). 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

[8] Rajasekharaiah, K., Dule, C. and Sudarshan, E. (2020). Cyber Security Challenges and its Emerging Trends on Latest Technologies. IOP Conference Series: Materials Science and Engineering. https://doi.org/10.1088/1757-899X/981/2/022062