International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 05 – Issue 07 || July 2020 || PP. 61-72

Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era

Kenneth Okereafor[1], **Oluwasegun Adelaiye**[2]
[1]*Department of Information and Communications Technology, National Health Insurance Scheme (NHIS), Abuja, Nigeria*
[2]*Department of Computer Science, Bingham University, Karu, Nasarawa State, Nigeria*

Abstract: The social distancing practices triggered by the COVID-19 pandemic have caused a huge growth in the use of online technologies to support remote work, resulting in a sharp rise in computer crimes, privacy breaches and service disruptions across the globe. Cyber attackers are taking advantage of COVID-19 anxiety to launch email scams, misinform and mislead unsuspecting targets, and propagate harmful software using various threats. The trend beckons for a more proactive cybersecurity approach to detect, prevent, and mitigate potential computer crimes. This paper proposes a Randomized Cyberattack Simulation Model (RCSM), an enhanced cyber attack readiness checklist for tackling computer crimes in advance. The RCSM extends traditional incident response and offers a pre-forensic guide as a precursor to the redefinition of cybersecurity in the post COVID-19 digital era.

Keywords: Access, COVID-19, cyber attack, cyber security, hack, in advance, impact, proactive, RCSM, threat, vulnerability.

1.0 Introduction

In the wake of the COVID-19 pandemic, there has been a sharp rise in the use of online technologies to support remote work via cloud computing, high speed data networks, software applications, dynamic databases, the internet, and its web component. Using telecommuting and video conferencing [1], [2], these technologies have proven to be supportive in remote office collaboration, work-from-home sessions, online academics, and religious worships; activities that initially entailed physical clusters of persons at specific locations, timeframes, and durations. All such physical gatherings have changed, and the changes are likely to remain a long-lasting part of a new culture of reliance on online alternatives and virtual computing.

The alternative adoption of web and internet services has led to a corresponding increase in online crimes particularly spear phishing emails and ransomware. Similarly, social engineering remains an underlying deception tool in the hands of cybercriminals and fraudsters who take advantage of human weaknesses to steal confidential data and disrupt digital operations for mischievous gains [3].

Cyber attack incidents have been on a steady increase, with their impacts including rising financial implications [4] and millions of dollars [5] in tangential losses. Most attacks occur even in the midst of traditional mitigation methods, using obfuscation to evade [6] detection and gain persistence in the system [7]. Most recent cyber attacks use un-identified attack methods, which make signature-based detection grossly ineffective [8], including the recovery approach proposed by Weil and Murugesan [9].

Given the sophistication and frequency of COVID-19 related cyber attacks, mere detection and response are no longer sufficient to deal with their impacts on the cyberspace. A new prevention approach is required to anticipate their occurrence and take proactive countermeasures to minimize their impacts. This paper proposes the Randomized Cyberattack Simulation Model (RCSM) that was earlier introduced in [10] and [11], and now its components hereby discussed in detail as an optimized cyber attack readiness checklist capable of boosting the incident response capabilities. The paper makes projections on how post COVID-19 digital era could potentially influence global response to cybersecurity breaches which computer users and online consumers are exposed to.

2.0 Cyber Attack Landscape in the COVID-19 Pandemic

As changes to work practices and socialization mean that people would be spending increased periods of time online [12], the concept of work from home has brought about a shift in focus for hackers [13] to end-users, most of whose systems do not possess adequate protection to cope with the new cyber attack dynamics and relevant business alterations.

As a result, cybersecurity appears to have received the swiftest momentum from the COVID-19 crisis owing to the justifiable need to protect an overstretched cyberspace whose activities have astronomically risen in adherence to social distancing measures. Consequently, the spate of cyber attack incidents has skyrocketed.

2.1 Cyber attack profile

Key reasons that fuel the rise in cybercrime incidents in the COVID-19 pandemic are people's online behaviour and anxiety to access updated information on the disease, as well as inadequately protected data networks occasioned by unprecedented remote work limitations. Such shortcomings have increased the risk of falling prey to social engineering scams whereby fraudsters capitalize on the human factors of desperation, panic, fear, and ignorance to propagate malicious codes disguised as authentic COVID-19 related information [3]. The behavioural despair and anxiety exhibited by people in the face of adjusting in accordance with the pandemic's advisories exposes them to inherent threats, making humans easy targets of cyber attacks.

2.2 Cyber attack incidents

On 20th April 2020, Cognizant the American IT services company announced that it had been hit by the maze ransomware which affected personal information of employees and exposed active credit cards of customers, an attack the firm estimated could cost up to $70 million [14] in accumulated losses. Before the attack was contained on 1st May 2020 [15], it had resulted in the leakage of sensitive corporate documents to the public, raising fears of government sanctions for the personally identifiable information (PII) that got exposed in the attack [16].

On 15th July 2020, some Twitter employees were hit by a massive social engineering attack [17] which resulted in the compromise of user accounts belonging to some famous celebrities, tech executives, world leaders, philanthropists, and politicians including Bill Gates, Barack Obama, Joe Biden, Elon Musk, Michael Bloomberg, and Kanye West. After manipulating Twitter employees [18], the cyber attackers simultaneously hacked into high profile accounts, bypassed their access controls, downloaded private data [19], initiated self-styled tweets centered around bitcoin fraud, and posted crypto scam messages to millions of their followers, as shown in Figure 1.

Figure 1: Screenshots of 15th July 2020 Twitter account hacks on Bill Gates and Elon Musk.

Although the July 15th cyber attack was typically coordinated and socially engineered, and such cryptocurrency scams on Twitter are not particularly new, however the number of affected users was unusually high. The hackers compromised the accounts of 130 high-profile users and were able to reset the passwords of 45 of those accounts [20]. The social engineering attack successfully targeted some Twitter employees [21], [22] with access to internal systems and tools, through which the scams were orchestrated and launched. The attack highlighted a major flaw with a social media service which millions of people have come to rely on as an essential communications tool, raising serious reputational and trust issues.

As the compromised Twitter accounts were quickly hijacked in rapid succession [23], preliminary investigations so far tend to pin the motivation for the attacks to a combination of financial incentive, technical bragging rights, challenge, and disruption of service. Ultimately, the COVID-19 induced social distancing could have contributed to the attack as the majority of Twitter's employees with access to sensitive systems and tools are working from home or from remote locations which are more difficult to protect than the corporate network that sits behind hardened perimeter [22], firewals and intrusion detection systems.

As both Cognizant and Twitter work harder to regain customer trust and public confidence, there have been several other reported incidents of ransomware, social engineering and email phishing attacks on organizations, leading to loss of confidential information, leakage of customer data, and corporate reputational damage.

2.3 Cyber attack impacts

For each successful cyber attack there are various degrees of impacts on either the individual user, the computing systems, the environment, the organization, and/or its personnel. The greatest impacts are usually felt on the data stored on the victim's systems or transmitted across networks. Impacts on data can manifest on its confidentiality, integrity, or availability.

2.3.1 Impact on data confidentiality

Data stolen via a cyber attack leads to unauthorized access to and illegal disclosure of confidential information, resulting in privacy infringements. Identity theft jeopardizes the privacy of the victim's data. E.g. a loss of confidentiality involving healthcare data can lead to stigmatization of patients, and medical litigations.

2.3.2 Impact on data integrity

Unauthorized data alteration resulting from a cyber attack impacts the value and usefulness of the data. Unauthorized data modification compromises its correctness and trustworthiness. E.g. a compromised medical data can result in misdiagnosis, denial of healthcare, and fatality. Similarly, an integrity attack on aviation data could lead to catastrophic consequences.

2.3.3 Impact on data availability

Inaccessible data confined by a ransomware or computer virus attack can impact corporate business operations or individual online safety. E.g. an unreachable or irretrievable financial data can adversely hamper the timely delivery of goods and services across the eCommerce supply chain.

2.3.4 Impact on reputation and service delivery

In most cases a cyber attack disrupts an organization's corporate operations. It also leaves a negative impression that affects customer loyalty, trust, and business relationships, all of which can potentially trigger long-lasting reputational damage that can potentially threaten the survivability of the organization.

2.3.5 Impact on revenue loss

Every victim of cyber attack incurs a certain financial cost arising from regulatory fines for organizations, in addition to qualitative cost of the compromised data, and the quantitative cost of recovery for both individual and corporate victims.

2.3.6 Impact on patronage of information systems

The persistent attacks on computing and digital assets affects the trust in the utilization of Information Systems in solving problems [24] and can potentially lead to a sustained apathy against technology.

2.3.7 Impact on digital behaviours and cyberspace expectations

Cyber attacks in the COVID-19 pandemic seem to have reversed previously known conventions and ignited new behavioural adjustments, as human interactions have predominantly moved to the cloud. Figure 2 below provides an inexhaustive list of online services that have shifted to the cloud, and given the cyberspace the heightened super active status in the COVID-19 pandemic.

Figure 2: Some online and virtual computing services promoted by COVID-19 induced social distancing.

The shift in digital behaviours triggered by COVID-19 related cyber attacks comes with high societal expectations that the cyberspace be proactively secured to cope with the rising volume and complexity of such cyber attacks, most of which present as scams intended to deceive internet users, steal their identities or disrupt their online operations with the aid of social engineering.

2.4 Roles of social engineering in promoting or preventing cyber attacks

Humans interact closely with and have access to Information Technology (IT) resources [25] for everyday life. Unfortunately, poorly protected user access can become an attacker's entry point into the system [26]. In recent attacks the weakest links have remained the user [27] and the human factor. Cyber attackers use a technique known as social engineering to play on human intelligence in an attempt to gain unauthorized access to IT systems for malicious purpose [27]

Cyber attackers employ social engineering technique to exploit weaknesses in humans and obtain confidential information that can be used for blackmail, ransom demand, identity theft or unauthorized access to sensitive data. Hence human weakness is the underlying vulnerability, deception is the tool of attack, and malicious benefits remain the objective.

Social engineering skills play a significant role in both facilitating and preventing cyber attacks. Whereas the cyber attacker uses social engineering skills to exploit the human factor of security by taking advantage of online users' flaws for malicious intent, the security defender uses the skills to educate users on how best to protect themselves from falling prey to many online scams currently being popularized by the peculiarities of the COVID-19 pandemic. Unfortunately, balancing the ethical use of social engineering for awareness creation with its malicious use for exploitation has always tilted in favour of cyber attackers.

The incidents of social engineering have risen astronomically in the COVID-19 era due to the human curiosity and yearnings for coronavirus related information, the clinging for related news items and products, and the persisting weak networks supporting remote work popularized by COVID-19 control measures.

2.5 Types of cyber attacks in the COVID-19 pandemic

A partial listing of the most common cyber attack threats which internet consumers and online users have been exposed to in the COVID-19 pandemic is provided. For each cyber attack and threat presented in Table 1 below, a description of its mode of operation is summarized, followed by its impact, alongside how to prevent, detect, or respond to it.

Table 1: Popular cyber attacks and threats in the COVID-19 pandemic

SN	Cyber threat	Impact	Mitigation
1.	**Spear phishing and spam emails:** Unsolicited and deceptive emails that impersonate known brands and high-profile personalities, with the intention to extract confidential information or propagate other malware.	• Data leak • Data alteration • Data loss • Privacy infringement • System crash • Identity theft • Reputational damage • Revenue loss • Service disruption • Operational inefficiency • Regulatory fines • Public disclosure • Litigation • Scandal and fatality	• Intrusion detection • Intrusion prevention • Anti-malware tools • Cybersecurity awareness • Security training • Endpoint protection • Perimeter protection • Firewalling • Proper encryption • Steganography • Machine learning • Anomaly detection
2.	**Malware:** Hostile and disruptive software code that causes harm and undesirable outcome on the victim's computer or digital asset including unauthorized access and illegal data alteration. E.g. ransomware, computer virus, adware, spyware, worms, trojan, etc.		
3.	**Website highjack:** The seizure of a website by a cyber attacker who has gained full administrative control of the entire contents of the website for malicious intents including posting offensive content and propagating own ideologies.	• Ransom demand • Defaced content • Deep fakes • Fake news • Scandal • Image smearing • Service disruption • Occupational nuisance • Reputational damage	• Proper encryption • Sound password ethics • Biometric authentication • Multi-factor authentication • Steganography • Honeypot
4.	**Website cloning:** The illegal replication of a victim's website by an internet fraudster for the purpose of deceiving unsuspecting users by diverting their legitimate web requests to the cloned website and obtaining confidential information for malicious benefits.		• Public disclaimer • Corporate damage control • Cybersecurity awareness
5.	**Cyber espionage:** The use of online techniques to spy on the digital behaviour or online transactions of an individual or a corporate organization through social engineering, spyware, shoulder surfing, cyber stalking, man-in-the-middle, brute-force, keylogging, or other methods.	• Identity theft • Privacy infringement • Image smearing	• Counter-espionage • Anti-espionage • Network monitoring tools • Biometric authentication • Sound password ethics • Cybersecurity awareness • Anti-malware tools • Online ethics • Intrusion detection • Firewalling
6.	**Cyber bullying:** The use of digital assets to victimize, harass or disseminate falsehood and offensive content against an individual, group, or corporate organization, by hiding under the anonymity of online platforms, blogs, and forums.	• Scandal • Individual nuisance • Occupational nuisance • Service disruption • Reputational damage • Libel • Hate speech	• Public disclaimer • Sound password ethics • Cybersecurity awareness • Online ethics

Apart from the cyber attacks and threats described in Table 1 above which pose major risks to internet activities, there are many other emerging security concerns which internet users must take note of in order to improve on safe computing, reduce data loss and minimize disruption of online operations.

3.0 Proposed Randomized Cyber attack Simulation Model (RCSM)

3.1 Background

The sudden nature of cyber attacks is a challenge to the effectiveness of existing incident response approaches, and fixing this challenge requires a more efficient alternative approach. Today's cyber defences are largely static in nature, allowing adversaries to pre-plan their attacks [28] and capitalize on human and system vulnerabilities. The problem with this approach is that most individual and corporate cyberspace consumers are only alerted by indicators of compromise (IoC), which are majorly reactionary in nature.

Furthermore, mere awareness has been shown to be inadequate in mitigating social engineering related attacks, and thus a technical approach irrespective of the user is needed [29].

A post COVID-19 digital era requires stronger strategies for cybersecurity action, including a more effective approach to dealing with cyber attacks in a proactive manner. The **Random Cyberattack Simulation Model (RCSM)** is proposed to proactively strengthen cyber attack response in the post COVID-19 digital era.

3.2 Features

The RCSM provides an easy-to-reference set of best practices for incident response teams to evaluate and assess, in advance, the IT infrastructure's resilience and preparedness to neutralize malicious activities and resist spontaneous cyber attacks. As a novel cyber attack simulation approach, it is designed to offer an instantaneous checklist for the cyber defence preparedness of the organization, with the following key features:

1. Proactively analyses the scope of vulnerabilities in critical applications.
2. Appraises the strengths and capabilities of existing controls.
3. Strengthens the organization's pre-forensic and cybersecurity functions.
4. Differs from a pre-scheduled vulnerability and penetration testing.
5. Deployed rather spontaneously in a typical security drill fashion.
6. Detects weak controls that must be compulsorily fixed in advance.
7. Evaluates how incident responders truly react to unexpected attacks.

3.3 Implementation

Implementation of the model can be adapted to suit individual needs and organizational peculiarities based on:

- Data transaction size
- System capabilities
- Network topology
- Architectural layout
- Operating conditions
- Staff capacity
- Computing environmental factors, etc.

While its execution in a corporate setting should be unannounced as a real-time audit drill, it should only be applied on a periodic basis simply as a spontaneous drill to complement, rather than replace, traditional cyber threat checks such as daily virus signature scans, periodic antivirus definition updates, event log checks, and regular authentication audits. It should also not be run as a substitute to other established security defence measures including vulnerability analysis and penetration testing.

3.4 Modular structure

The Randomized Cyberattack Simulation Model (RCSM) is composed of six modules, each of which addresses a category of potential cyber attacks or threats namely: malware, social engineering, distributed denial of service (DDoS), access control, cyber ethics, and cyber administration.

The components of the model are pictorially illustrated in Figure 3, showing the six modules depicted by six blocks built on top of a proactive cyber attack readiness foundation. Each building block represents a cyber attack preparedness checklist later expanded in Table 2 through Table 7 below.

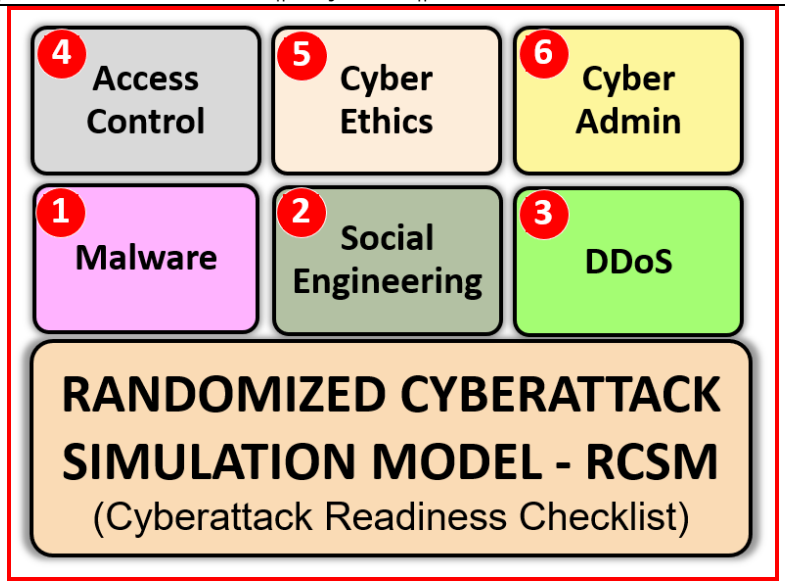

Figure 3: Pictorial representation of the Randomized Cyber attack Simulation Model (RCSM).

3.4.1 RCSM Module 1 – Malware

RCSM Module 1 focuses on boosting the ability of the organization's incident response to proactively tackle malware triggers as depicted in Table 2.

Table 2: RCSM Module 1 – Malware

Objective	To determine the ability of an organization's anti-malware and threat mitigation systems to correctly detect indicators of compromise, and proactively identify patterns that suggest malware activity, including suspicious hostile installation and externally instigated threats.
Checklist examples	Advanced Persistent Threat (APT), ransomware, virus, adware, trojan, worm, logic bomb, key-logger, hidden backdoors, expired software housing harmful code, unlicensed application, unpatched utility, etc.
Frequency	Quarterly for organizations that manage highly classified corporate data, otherwise bi-annually.

Malware action is a serious threat to an organization's data and information systems architecture. Owing to COVID-19 social distancing restrictions, the incidents of malware have increased exponentially as organizations migrate to online alternatives. In the wake of this sudden new normal, the readiness of organizations to cope with the scope and frequency of malware attacks must be guaranteed.

Testing an organization's anti-malware preparedness ahead of time in a spontaneous manner is a sure way to minimize the chances of cyber attacks and enhance the capacity of incident responders to tackle notorious viruses, ransomware, and other threats including unpatched software. Activating the malware module of the RCSM every six months evaluates the strength of available tools for checkmating malware attack in order to address any existing gaps before the actual attacks occur.

3.4.2 RCSM Module 2 – Social engineering

RCSM Module 2 focuses on optimizing social engineering awareness to minimize the propensity of personnel falling prey to manipulations of human weaknesses that could potentially lead to data loss and expose information to unauthorized alterations, as illustrated in Table 3 below.

Table 3: RCSM Module 2 – Social engineering

Objective	To determine the vulnerability of individuals and personnel to human errors, weaknesses, and other exploitable social engineering pitfalls in the workplace and on the cyberspace.
Checklist examples	Email phishing, spear phishing, phone conversation pranks, shoulder surfing, spoofed portal scams, email spams, cloned websites, tailgating, piggybacking, steganographic gimmicks, deceptive SMS alerts and messages, insider vulnerabilities, etc.
Frequency	Monthly for all organizations.

Social engineering represents both a major vulnerability to individuals and a threat to an organization's digital assets residing locally and in the cloud. The panic and apprehension associated with COVID-19 has progressively exposed individuals to a variety of online scams using vulnerable systems as a platform, email as a predominant tool, and social engineering as the technique. This challenge calls for increased awareness of the tactics of social engineers and how to detect and respond to them in order to maintain online safety.

Determining an organization's human vulnerabilities in advance minimizes employees' chances of falling victims to spear phishing, shoulder surfing, and other social engineering attacks based on the art of deception. Stimulating the social engineering module of the RCSM every month evaluates users' awareness of social engineering tactics in advance and provides an opportunity to address gaps before the actual attacks occur.

3.4.3 RCSM Module 3 – DDoS

RCSM Module 3 focuses on strengthening an organization's data network to withstand all forms of denial of service from internal and external sources. Module 3 focus is illustrated in Table 4 below.

Table 4: RCSM Module 3 – DDoS

Objective	To identify porous segments of the organization's network and digital architecture that are potentially vulnerable to Distributed Denial of Service (DDoS) attacks, particularly by observing, in advance, abnormal network traffic patterns indicating the likelihood of such attacks.
Checklist examples	Ping of death, smurf attack, DNS suffocation, cache poisoning, buffer overflow, SQL injection, DNS poisoning, privilege escalation, Cross Site Scripting (XSS), etc.
Frequency	Quarterly for all organizations.

Denial of service attacks are very disruptive to corporate and individual computing operations and could leave a huge impact on reputation or erode customer trust within service organizations that have once fallen prey. Cybercriminals have taken advantage of COVID-19 restrictions to launch massive DoS attacks on organizations with weak controls, thereby drowning their operations, causing service outages, and resulting in tangential loss of revenues. Addressing this challenge requires a proactive approach that ascertains that all applicable loopholes are identified in advance and mitigated in a proactive manner.

Confirming that an organization's security solutions are able to contain DDoS helps to proactively tackle DNS poisoning, ping of death, and other threats that rely on suffocation of resources with unnecessary traffic. Applying the DDoS module of the RCSM every three months determines and resolves issues with readiness to combat any form of denial of service indications long before the actual attacks occur.

3.4.4 RCSM Module 4 – Access control

RCSM Module 4 focuses on reinforcing authentication measures and forestalling all possible compromise that bypass security controls using various means, as shown in Table 5 below.

Table 5: RCSM Module 4 – Access control

Objective	To proactively assess the instantaneous level of user compliance with password and authentication requirements, and adherence to other access restriction regulations.
Checklist examples	Multi-factor authentication, dynamic authentication, password complexity, password age, password change interval, password reuse, password chaos, password fatigue, encryption status, biometric template safety [30], etc.
Frequency	Monthly

Access control is an essential component of the security overview. It limits access to digital resources based on many indices including functional roles, exposure to threats, and compliance with authentication standards. A compromised access control results in privacy breaches, loss of data and unauthorized alterations, all of which could impose significant impacts on the organization's reputation, operations, and sustainability. On individual computing, access control breaches could be an awful nightmare capable of causing data loss and access denial and could be terribly scandalous.

As the COVID-19 restrictions rage, and as more and more employees continue to work remotely, with less protection due to untrusted remote access, the world continues to witness numerous access control related breaches and cyber attacks. Cybercriminals have taken advantage of this proliferation to launch massive attacks on organizations with weak access controls.

Addressing access control challenge requires a proactive approach that possibly identifies compliance loopholes in advance. Activating the access control module of the RCSM every month measures and evaluates the ability of the individual or organization to adhere to access related guidelines, all in advance of any potential actual attack.

3.4.5 RCSM Module 5 – Cyber ethics

RCSM Module 5 ascertains the level of compliance with computing technology morals related to cybersecurity, to forestall user ignorance and ensure adequate protection of digital assets from preventable attacks from internal and external sources, as shown in Table 6 below.

Table 6: RCSM Module 5 – Cyber ethics

Objective	To verify the extent to which users (employees and individuals) adhere to computing morals, conducts, principles, and standards whose circumvention could expose the individual's and organizations' computing resources to cyber attacks, or place corporate data under threat of loss, unauthorized modification or illegal access.
Checklist examples	Single Sign On (SSO), One Time Password, (OTP), idle time out, account lockout, privilege escalation, authorization creep prevention, password management, identity sharing, expired, unlicensed or unpatched software, incident response promptness, etc.
Frequency	Monthly

3.4.6 RCSM Module 6 – Cyber administration

RCSM Module 6 focuses on evaluating the effectiveness and efficiency of cybersecurity governance structure and technology policies to ascertain conformity with best practices by the individual or an organization. Module 6 is illustrated in Table 7 below.

Table 7: RCSM Module 6 – Cyber administration

Objective	To evaluate the effectiveness and efficiency of available cybersecurity strategy directives and administrative controls used in the organization or practiced by the individual user.
Checklist examples	Cybersecurity policies, safety regulations, data protection frameworks, guidelines, standards, recommendations, regulations, etc.
Frequency	Quarterly for all organizations.

The cybersecurity governance framework adopted by an organization determines how well it administers data protection and can become a guarantee of the safety of its data assets. Societal adjustments due to COVID-19 have impacted the ability of organizations to exercise full compliance to cybersecurity and technology standards, resulting in frequent cyber attacks. A renewed approach becomes imperative, and the cyber administration module of the RCSM is designed to monitor compliance proactively.

Testing an organization's compliance is a sure way to minimize the chances of cyber attacks that could otherwise take advantage of inadequate cybersecurity governance. The cyber administration module of the RCSM provides the opportunity to periodically evaluate the applicability of best practices to appraise compliance before an actual attack occurs.

4.0 Conclusion

The social isolation triggered by the COVID-19 pandemic created an opportunity to switch to remote cyberspace technologies and innovative online alternatives. However, these technology alternatives have also resulted in a sharp spike in online fraud, identity theft, and other cyber-related scams adapted from previously known exploits. The complexity of COVID-19 induced cybercrimes has exposed the deficiencies in existing countermeasures and has raised concerns over the reliability of current computer incident response strategies.

Consequently, prevention has been identified as a panacea [31] and the much-needed vaccine that organizations should prescribe, rather than reactive approach to cyber attacks, which is regrettably the most dominant current practice.

This paper has once again presented the **Randomized Cyberattack Simulation Model (RCSM)** as a novel approach to ascertaining the preparedness of incident responders in mitigating cyber attacks in a proactive manner. The uniqueness of the model is the spontaneity of its application, as opposed to the predictability of existing protocols such as vulnerability analysis and penetration testing, both of which are usually pre-scheduled in nature and often require pre-notification of users and employees.

The Randomized Cyberattack Simulation Model presented in this paper is designed as a proactive and an improved tool for ascertaining individual and corporate preparedness to detect, prevent, respond to, and mitigate cyber attacks in the post COVID-19 digital era.

It is intended to evaluate and give readiness assurances in the areas of malware, social engineering, denial of service, access control, cyber administration, and cyber ethics. Applying this model within the proposed intervals will assist in pre-empting and mitigating threats to an organization's digital assets and can potentially stimulate a reformed post COVID-19 cybersecurity culture across industry, government, and academia.

Acknowledgement

Support from the National Health Insurance Scheme, and Bingham University Karu, Nigeria are appreciated.

About the Authors

Kenneth Okereafor is a United Nations trained cybersecurity and biometric expert, a former United States DoS employee with two and half decades of global experience in threat mitigation technologies across industry, government, and academia. With a PhD in Cybersecurity from Azteca University Mexico, he is Deputy General Manager at Nigeria's National Health Insurance Scheme (NHIS) where he coordinates database security and health informatics, and provides digital health security liaison with the World Health Organization through the Federal Ministry of Health. With a second PhD in ICT administration and governance, Kenneth is an alumnus of the UNESCO International Centre for Theoretical Physics (ICTP) Italy, and has published several papers in cybersecurity, biometric authentication, and digital forensics. Contact: nitelken@yahoo.com.

Oluwasegun Ishaya Adelaiye is a PhD candidate at the University of Abuja, Nigeria, and a lecturer in Computer Science at Bingham University, Karu. Adelaiye has published over ten academic articles and has supervised over a dozen undergraduate students. He has a BSc in Computer Science from University of Abuja and an MSc in Information and Network Security from Robert Gordon University, UK. Adelaiye's research interests include cybersecurity, network security, anomaly detection and machine learning. Contact: oluwasegun.adelaiye@binghamuni.edu.ng.

References

[1] K. Okereafor and P. Manny, "Understanding Cybersecurity Challenges of Telecommuting and Video Conferencing Applications in the COVID-19 Pandemic," International Journal in IT & Engineering, vol. 8, no. 6, pp. 13-23, 2020.

[2] K. Okereafor and P. Manny, "Solving Cybersecurity Challenges of Telecommuting and Video Conferencing Applications in the COVID-19 Pandemic," International Journal in IT & Engineering (IJITE), vol. 8, no. 6, pp. 24-32, 2020.

[3] K. Okereafor and O. Adebola, "Tackling the Cybersecurity Impacts of the Coronavirus Outbreak as a Challenge to Internet Safety," International Journal in IT and Engineering (IJITE), vol. 8, no. 2, pp. 1-14, 2020.

[4] K. Kammoun, A. Bounfour, A. Özaygen and R. Dieye, "Financial market reaction to cyberattacks," Cogent Economics & Finance, vol. 7, no. 1, p. 1645584, 2019.

[5] P. V. Kumar, "Growing cyber crimes in india: A survey," in 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE), 2016, 2016.

[6] A. O. Aslan and R. Samet, "A comprehensive review on malware detection approaches," IEEE Access, vol. 8, pp. 6249-6271, 2020.

[7] J. Hong, T. Kim, J. Liu, N. Park and S.-W. Kim, "Phishing url detection with lexical features and blacklisted domains," in Adaptive Autonomous Secure Cyber Systems, Springer, 2020, pp. 253-267.

[8] J. Hwang, J. Kim, S. Lee and K. Kim, "Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques," Wireless Personal Communications, vol. 112, no. 4, pp. 2597-2609, 2020.

[9] T. Weil and S. Murugesan, "IT Risk and Resilience—Cybersecurity Response to COVID-19," IEEE Computer Society - IEEE Computer Architecture Letters, vol. 22, no. 3, pp. 4-10, 2020.

[10] K. Okereafor and R. Djehaiche, "New Approaches to the Application of Digital Forensics in Cybersecurity: A Proposal," International Journal of Simulation: Systems, Scienece and Technology (IJSSST), vol. 21, no. 2, pp. 36.1-36.6, 2020.

[11] K. Okereafor and R. Djehaiche, "A Review of Application Challenges of Digital Forensics," International Journal of Simulation Systems Science and Technology, vol. 21, no. 2, pp. 35.1 - 35.7, 2020.

[12] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple and X. Bellekens, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," arXiv:2006.11929v1 [cs.CR], pp. 1-20, 2020.

[13] Chike Onwuegbuchi, "Expert Blames Fundamental Flaw in IP for Cyberattacks," Nigeria Communications Week, 13 July 2020. [Online]. Available: https://www.nigeriacommunicationsweek.com.ng/expert-blames-fundamental-flaw-in-ip-for-cyberattacks/. [Accessed 13 July 2020].

[14] Anandi Chandrashekhar, "Cognizant hit by 'Maze' ransomware attack," Economic Times, 21 April 2020. [Online]. Available: https://economictimes.indiatimes.com/tech/internet/cognizant-hit-by-maze-ransomware-attack/articleshow/75228505.cms?from=mdr. [Accessed 22 June 2020].

[15] The News Minute, "Cognizant ransomware attack: Credit card info, personal data of some employees leaked," The News Minute, 22 June 2020. [Online]. Available: https://www.thenewsminute.com/article/cognizant-ransomware-attack-credit-card-info-personal-data-some-employees-leaked-127076. [Accessed 22 June 2020].

[16] Lifars, "Cognizant hacked by Maze Ransomware Attack," Lifars, 5 May 2020. [Online]. Available: https://lifars.com/2020/05/cognizant-hacked-by-maze-ransomware-attack/. [Accessed 22 June 2020].

[17] Crist Ry, Wong Queenie, "Twitter hack hits Elon Musk, Obama, Kanye West, Bill Gates and more in Bitcoin scam," CNET, 16 July 2020. [Online]. Available: https://www.cnet.com/news/coordinated-twitter-hack-hits-elon-musk-obama-kanye-west-bill-gates-and-more-in-bitcoin-scam/. [Accessed 20 July 2020].

[18] R. McMillan and E. Choi, "Twitter Hack Revives Concerns Over Its Data Security," The Wall Street Journal, 19 July 2020. [Online]. Available: https://www.wsj.com/articles/twitter-hack-revives-concerns-over-its-data-security-11595156402. [Accessed 21 July 2020].

[19] BBC News, "Twitter says hackers downloaded private account data," 18 July 2020. [Online]. Available: https://www.bbc.com/news/technology-53455092. [Accessed 21 July 2020].

[20] BARBARA ORTUTAY, "Twitter: Hack hit 130 accounts, company 'embarrassed," AP News, 19 July 2020. [Online]. Available: https://apnews.com/860daee9d51ceb588c9bd0feebddc323#:~:text=OAKLAND%2C%20Calif.,of%2045%20of%20those%20accounts. [Accessed 21 July 2020].

[21] Nick Statt, "Twitter reveals that its own employee tools contributed to unprecedented hack," The Verge, 15 July 2020. [Online]. Available: https://www.theverge.com/2020/7/15/21326656/twitter-hack-explanation-bitcoin-accounts-employee-tools. [Accessed 21 July 2020].

[22] Joseph Carson, "The Twitter Hack and the Failure to Protect Privileged Access," Thycotic, 17 July 2020. [Online]. Available: https://thycotic.com/company/blog/2020/07/17/twitter-hack-and-failure-to-protect-privileged-access/. [Accessed 21 July 2020].

[23] Z. Whittaker, T. Hatmaker and S. Perez, "Apple, Biden, Musk and other high-profile Twitter accounts hacked in crypto scam," Tech Crunch, 15 July 2020. [Online]. Available: https://techcrunch.com/2020/07/15/twitter-accounts-hacked-crypto-scam/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABdy7SfrfOZToXPFsqSeuEysH1_PDAcf6hp0FX1LaM1yDwNsu4TEwmU6ZUZ0OxwDqdLn_JtGyTWShRn1VKB4FxwE-sfj6dQkGLpwpM4. [Accessed 21 July 2020].

[24] O. I. Adelaiye, A. Showole and S. A. Faki, "Evaluating Advanced Persistent Threats Mitigation Effects: A Review," International Journal of Information Security Science, vol. 7, no. 4, pp. 159-171, 2018.

[25] T.-H. Tsai, C.-C. Huang and K.-L. Zhang, "Design of hand gesture recognition system for human-computer interaction," Multimedia Tools and Applications, vol. 79, no. 9, pp. 5989-6007, 2020.

[26] Z. A. Wen, Z. Lin, R. Chen and E. Andersen, "What. hack: engaging anti-phishing training through a role-playing phishing simulation game," in 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, Scotland, 2019.

[27] R. Heartfield and G. Loukas, "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework," Computers Security, vol. 76, pp. 101-127, 2018.

[28] S. Jajodia, G. Cybenko, P. Liu and C. Wang, Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Control- and Game-Theoretic Approaches to Cyber Security, 2019.

[29] M. Bada, A. Sasse and J. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" arXiv preprint arXiv:1901.02672, 2019.

[30] K. U. Okereafor, O. E. Osuagwu and C. Onime, "Enhancing Biometric Liveness Detection Using Trait Randomization Technique," in 2017 UKSim-AMSS 19th International Conference on Modelling & Simulation, Cambridge, 2017.

[31] Sharda Tickoo, "Demystifying ransomware - the cyber pandemic," Econimic Times, 29 June 2020. [Online]. Available: https://ciso.economictimes.indiatimes.com/news/demystifying-ransomware-the-cyber-pandemic/76684165. [Accessed 1 July 2020].