New Approaches to the Application of Digital Forensics in Cybersecurity: A Proposal

Kenneth Okereafor [1], Rania Djehaiche [2]

[1] *Department of Information and Communications Technology*, Database Security Division, National Health Insurance Scheme (NHIS) Abuja, Nigeria.
nitelken@yahoo.com

[2] *Department of Electronics*, Faculty of Sciences and Technology, Mohamed El Bachir El Ibrahimi University of Bordj Bou Arreridj, Algeria.
rania.djehaiche@univ-bba.dz

***Abstract* - The challenges faced by organizations in effectively carrying out digital forensic operations have been identified to include poor capacity and defective Information and Communications Technology (ICT) policies, resulting in organizational cluelessness when high profile cyberattacks occur. Organizational unpreparedness in the face of cyberattacks leads to negative impacts including operational disruption, financial loss, reputation damage and crippling litigations. Unfortunately, the sophistication of contemporary cyberattacks makes their investigations even more difficult except where a methodical approach for forensic data collection and analysis is adopted. This paper proposes the Randomized Cyberattack Simulation Model (RCSM) as a checklist for assessing corporate preparedness to digital forensics and as a systematic approach towards enshrining organizational incident response capabilities. The paper also proposes the Baseline Data Classification Model (BDCM) as a pre-forensic data categorization model. Prudent application of both models can potentially mitigate the impacts of cyberattacks on operational sustainability and organizational survivability across all sectors.**

Keywords - Breach, cyberattack, cybersecurity, digital forensics, incident response, impact.

I. INTRODUCTION

Digital forensics applies scientific techniques to retrieve data from digital sources for the purpose of investigating a computer related problem or auditing a cyberattack incident. This includes the recovery of evidence [1] [2] from any device that has a digital processor or digital storage capability. It bridges the gap between cyberattack prevention and response procedures [2] [3]. Digital forensic procedures are in alignment with standard incident response steps namely preparation, identification, containment, eradication, recovery and lessons learnt. Many of the challenges that face digital forensics relate to negligence and ignorance of, or lukewarmness to, cybersecurity [4] policies and standards on the part of organizations. Having identified the impacts of cyberattacks to include losses in revenue, reputation and data value, there is therefore a great need to adopt measures that are both scalable and effective in mitigating these undesirable consequences rather proactively. This paper proposes proactive approaches towards the application of forensic techniques as the reactive component of cybersecurity particularly to assist with computer incident response.

The rest of the paper is organized as follows: Section II presents proposals on data classification for optimizing digital forensics in organizations. Section III presents proposals on cyberattack simulation. Section IV presents proposals on digital forensics preparedness for optimizing efficiency in organizations. Section V concludes the paper and summarizes the key points in organizational embrace of routine digital forensics.

II. PROPOSALS FOR DATA CLASSIFICATION

Being mindful of data value is an important prerequisite in every forensic exercise, without which critical data could remain unprotected while insignificant data is undeservedly secured with heavy investments. The following are presented to take care of the identified data classification challenges associated with digital forensic as a cybersecurity component.

A. Classifying Data Clearly and Early Enough

It is mandatory for every corporate organization to identify and adopt a data classification model that conforms to global standards and aligns perfectly with its data sets. Data classification within an organization paves the way to categorizing data based on relevance, criticality and value. Without appropriate classification of data, it is difficult to determine what constitutes a data breach or to draw the line between open data and privacy infringements.

A clearly defined data classification approach helps the organization to determine the magnitude of protection that must be accorded to each digital asset. It also helps to estimate the strength and scope of cybersecurity systems

that must be deployed to monitor the status of data based on value. Ultimately, it determines the commensurate security investment applicable for budgetary computations. Early and prompt data classification ensures that those digital assets which host critical data are accorded a greater proportion of detective, preventive and deterrent controls, and are placed under a higher level of monitoring and surveillance to preserve their integrity, and guarantee their availability at all times.

For example, a higher level of security investment is required for deploying an event monitoring system for a bank's database server as opposed to the level of protection expected for a standalone thin client computer. The difference lies in the disparity between the value of the database server and that of the client computer. The corporate data residing in the database server is more sensitive and has more business value than that of the client computer, and its loss or compromise could trigger greater impact on the organization. Sensitivity and impact upon loss are two major determinants of data classification for the purpose of estimating the strength of cybersecurity countermeasures.

B. Proposing Baseline Data Classification Model (BDCM)

A proposed 3D Baseline Data Classification Model (BDCM) showing three sensitivity levels (High, Medium and Low) is presented in Table 1 below. The uniqueness of the model is in its reliance on a qualitative appraisal of the impacts of data loss or cybersecurity breach on the organization's reputation, revenue and operations. Datasets whose loss are capable of triggering grievous or life-threatening consequences are assigned the highest sensitivity and subsequently classified as restricted. Lower classifications follow in that order.

TABLE I. PROPOSED 3D BASELINE DATA CLASSIFICATION MODEL (BDCM) BASED ON IMPACT ON ORGANIZATION UPON DATA LOSS OR CYBERATTACK

Data Classification	Sensitivity	Impact upon Data Loss or Breach	Examples
Restricted or Confidential	High	• Critical • Total system failure • Catastrophic or scandalous • Fatal or damaging • Financial or legal risk	Medical diagnosis records, flight data, Intellectual property data.
Sensitive	Medium	• Less severe when lost • Marginal impact when breached • Easy recovery from effects of loss	Employee records, financial data, academic records.
Unrestricted or Public	Low	• Minimal impact when lost, modified or mis-communicated. • Of general knowledge • Non-critical to corporate operations and national security • Mostly of deliberate public knowledge	Meeting notice, Price list, road accident statistics.

To simplify the applicability of the proposed model for digital forensics purposes, the data classification is denoted by colour codes with red representing *restricted or confidential data*, amber or yellow signifying *sensitive data* and green indicating *unrestricted or public data*. Organizations can finetune the categorization of their corporate data to align with an appropriate sensitivity level indicated on the reference BDCM, as long as sensitivity and impact upon loss remain the categorization criteria.

III. PROPOSALS FOR CYBERATTACK SIMULATION

Responding to a cyberattack through incident management is a methodical exercise that requires prior rehearsal by both first responders and the entire cybersecurity team. Unfortunately, it is the typical emergency nature of a cyberattack that makes it a source of worry for organizations. Dealing with such worry entails a proactive simulation approach, hence this proposal.

A. Proposed Randomized Cyberattack Simulation Model (RCSM)

The Randomized Cyberattack Simulation Model is proposed. The model is an instantaneous checklist for the cyber defence preparedness of the organization, hence its randomization. Since cyberattacks usually come unannounced, the organization should permanently be in a ready mode through regular cybersecurity audit and drills aimed at familiarization with different forms of digital threats. Furthermore, the proposed simulated drill provides a spontaneous assessment of the preparedness of incident responders and cybersecurity personnel in an unscheduled and surprising manner. It also helps to identify potential hiccups that must be fixed in advance to avert undesirable consequences. The randomness and spontaneity of the proposed model differentiates it from regular penetration testing which is usually a scheduled activity that often comes with pre-notification of employees amidst other pre-planned prerequisites. The RCSM should be unannounced and executed as a real-time audit drill. The proposed comprehensive Randomized Cyberattack Simulation Model

is presented in Table II below covering vital components of the organization's cybersecurity programme.

TABLE II. PROPOSED HIGH-LEVEL RANDOMIZED CYBERATTACK SIMULATION MODEL (RCSM) FOR ORGANIZATIONS

SN	Cyberattack Category	Simulation		
		Objectives	**Specific Examples**	**Frequency**
1.	Malware	To ascertain the ability of the organization's threat mitigation systems to correctly and proactively identify patterns that could suggest externally instigated malware activity or suspicious hostile installation.	Advanced Persistent Threat (APT), Ransomware, Trojan, Worm, Virus, Logic bomb, keylogger, hidden backdoors, expired, unlicensed or unpatched software, etc.	Quarterly
2.	Social Engineering	To determine the vulnerability of personnel to falling victims to exploitable human weaknesses in the workplace and on the cyberspace.	Phishing, phone conversation pranks, shoulder surfing, spoofed portal scams, email spams, cloned websites, tailgating, piggybacking, steganographic gimmicks, deceptive SMS alerts or messages, insider vulnerabilities, etc.	Monthly
3.	DDoS	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 abnormal network traffic patterns indicating the likelihood of such attacks.	Ping of death, smurf attack, DNS suffocation, cache poisoning, buffer overflow, SQL injection, privilege escalation, Cross Site Scripting (XSS), etc.	Quarterly
4.	Access control	To assess the level of employee compliance with password and authentication requirements, and adherence to other access restriction regulations.	Password complexity, password age, password change interval, password reuse, password chaos, password fatigue, encryption status, biometric template safety [5], etc.	Monthly
5.	Cyber ethics	To verify the extent to which employees obey computing morals, conducts, principles and standards whose circumvention could expose the organizations' computing resources to cyberattacks or place corporate data under threat of loss, unauthorized modification or illegal access.	Single Sign On (SSO), One Time Password, (OTP), idle time out, account lockout, privilege escalation, authorization creep, password management, identity sharing, expired, unlicensed or unpatched software, incident response promptness, etc.	Monthly
6.	Cyber admin	To check for the effectiveness of available cybersecurity strategy directives and administrative controls in the organization.	Cybersecurity policies, guidelines, standards, recommendations, regulations, etc.	Quarterly

The proposed model serves as a benchmark that can be adapted to suit the peculiarities of the organization's operating conditions, environmental factors, architectural pattern and other metrics. Organizations adopting the RCSM should use it only periodically simply as a spontaneous drill that should complement, rather than totally replace, the routine cybersecurity threat checks such as daily virus signature scans, daily antivirus definition updates, daily event log checks, regular authentication audits, etc.

IV. PROPOSALS FOR DIGITAL FORENSICS PREPAREDNESS

A. Developing Policies and Evolving a Holistic Cybersecurity Approach

Establishing a forensic capability should start with the development of corporate ICT strategies and cybersecurity policies and procedures. Organizations should prioritize the development of relevant policies particularly to guide specific aspects of enterprise computer security operations, including but not limited to network maintenance, email use, password management, wireless device guidelines, data retention policies, storage management, Bring Your Own Device (BYOD) safeguards, etc. The existence of, and adherence to, relevant ICT policies provide the administrative foundation to minimize cyberattack incidents and lower the frequency of computer forensics. A holistic cybersecurity approach centred on the effectiveness of the incident response function requires the combined application of physical, administrative and technical countermeasures, alongside adherence to the standard set of incident response procedures including preparation, identification, containment, eradication, recovery and lessons learnt.

B. Building Superior Capacities in Digital Forensics

Organizations should invest in building and developing the capacities of their workforce for carrying out digital forensics operations as may be necessary. Since sound application of digital forensics requires excellent knowledge of principles and global advancements in forensic techniques and procedures, acquiring and refining superior expertise should be the focus of every capacity building initiative in this regard. There are multiple approaches to building organizational digital forensics capacity, including:

- Alliance with other organizations though cross-exchange of skills.
- In-house organizational security drills and simulation.
- Self-paced training.
- Real-time hostile response.

C. Institute Collaboration on Data Security and Digital Forensics

As a benchmark approach, organizations should establish appropriate synergy with each other for the purpose of exchanging digital forensic ideas, projects and initiatives. Collaboration is not an exclusive preserve of academic institutions alone, but government agencies and other commercial and not-for-profit bodies can and should endeavour to undertake symbiotic collaborations with each other for the purpose of technology transfer. Four major advantages of inter-organizational collaboration in digital forensics are:

- Reduces the overhead for responding to avoidable cybersecurity breaches.
- Eliminates the corresponding corporate reputational damage that could arise from unanticipated cyberattacks.
- Facilitates the acquisition of best practices and testing of digital forensic tools.
- Reduces the chances of repeating mistakes that could lead to avoidable cyber incidents.

D. Carrying Out Research and Development (R&D)

The rate of technological advancements is so rapid that organizations should consistently embrace an innovative ICT strategy rather than merely play catch-up. Organizations should undertake and participate in R&D initiatives that expose them to contemporary best practices in forensics. As societies evolve, strategies also change in response to the global dynamics, hence R&D should become a handy option for advancing an organization's capacity to confidently perform forensics more creditably.

E. Adopting and Implementing Standards

Organizations should establish strict adherence to recommendations, protocols and guidelines that conform to universal standards [6] [7] [8] in cyber forensics and computer security. Nonconformity to standards can result in a number of consequences including the risk of frequent data losses, regulatory sanctions, preventable revenue losses, higher probability of recurrent cyberattacks, and many other negative impacts. Applicable guidelines exist in all aspects of computer security including but not limited to recommendations from the National Institute of Standards and Technology (NIST) and the SANS Institute on trustworthy email security recommendations [9] [10], digital identity, authentication and password security recommendations [11] [12] [13], web security recommendations [14] [15] [16] [17], network intrusion management recommendations [18] [19], etc. Organizations should incorporate standardization into their technology policies for safer computing, greater impact, and cleaner compliance record.

F. Building Preventive and Detective Architecture against Widespread Malware

Organizations are encouraged to invest in preventive and detective control systems and other threat mitigation technologies that can anticipate, deter or halt cyberattacks proactively. The devastating impacts of Stuxnet [20] [21], WannaCry [22] [23] and NotPetya [24] [25] cyberattacks on organizations with inadequate protection are still fresh in memory. Preventive, detective and deterrent systems are very resourceful cybersecurity assets that save organizations from the following problems:

- Damage to digital networks and systems
- Loss of sensitive information
- Disruption of regular operations
- Financial loss
- Long term reputational harm
- Prolonged litigations
- Risk of collapse

Many cyberattacks targeted at critical system files can be prevented or detected if proactive countermeasures are put in place, rather than reactive strategies that often come with costly consequences. Organizations should patronize reputable security tools that can proactively check file systems for malicious files and are able to initiate early alert for a speedy intervention.

- The WannaCry cyberattack for example was only halted by the emergency, but costly, release of patches [22] [23] by Microsoft and the unconfirmed discovery of a kill switch that allegedly prevented infected computers from spreading the ransomware any further.
- In the NotPetya case, most of the infected computers were found to be using older versions of the Windows Operating System (OS) while the higher Windows 10 OS was fully capable of mitigating the attack [26]. This system deficiency could have been detected if the appropriate security tools were available and fully functional prior to the attack.
- The Stuxnet virus incident presents a vital lesson to implement secure architectures which prevent or restrict access to stand-alone Supervisory Control and Data Acquisition (SCADA) systems [27] [28] [29] [30] from the main corporate IT network [31]. SCADA are the Industrial Control System (ICS) [31] facilities that are used for remote monitoring of a variety of stand-alone processes including refineries, rail systems, power utilities, and nuclear plants. They also provide remote surveillance and maintenance for wind turbines, water/sewage flow, dams, industrial processes, and air/water pollution facilities. Essentially the key to a guaranteed recovery from cyberattacks on networked or stand-alone systems is early detection and response

which is hinged on possessing and using tools with good preventive and detective capabilities as part of the architecture design.

G. Deployment of Honeypots

Another innovative way of preventing and detecting computer malware infection in a large network is the use of honeypots to trick the malware into believing that it is already resident on the target system, almost a semblance of the pattern of biological virus that checks for a disease's antibody in a human host as an assessment of the host's immunity against the disease. A honeypot is a network security asset (system, account, file, device, software, routine, etc) primarily installed as a trap to deceive malware and cyberattackers, detect hacking attempts, study attack patterns or prevent unauthorized access to data and information systems. In the NotPetya attack for example, a vaccine-like honeypot was applied by researcher Amit Serper [32] using the Windows directory folder (C: Windows) to create a honeypot file named "perfc" which protects personal computers (PC)s. During infection, the malware undertakes a self-destruct as soon as the "perfc" file is found to be pre-existing in the target folder [33], thereby protecting the PC.

V. CONCLUSION

As the cyberspace is increasingly governed by data, cyberattacks are progressively becoming inevitable in today's corporate digital world, resulting in revenue loss, reputational damage and operational disruptions. At the same time, the growth in identity fraud and other data security breaches influence the need for digital forensics.

This paper proposed two models for approaching digital forensics more efficiently: The 3D Baseline Data Classification Model (BDCM), and the Randomized Cyberattack Simulation Model (RCSM). BDCM model helps organizations in categorizing corporate data more effectively with emphasis on forensic relevance, while labelling data classification as a mandatory exercise for organizations desirous of providing value-based security. The novel RCSM model is a checklist to assist organizations in performing spontaneous cyberattack drills as a routine part of their cybersecurity audit culture. These proposals should optimize organizations' approaches to the professional application of digital forensics as a cybersecurity component. Ultimately cybersecurity policies must be comprehensive enough to proactively accommodate every aspect of threat detection, prevention and response.

ACKNOWLEDGMENT

Kenneth Okereafor thanks the National Health Insurance Scheme (NHIS), Nigeria; the Computer Forensics Institute, Nigeria (CFIN); and the Mohamed El Bachir El Ibrahimi University of Bordj Bou Arreridj, Algeria for supporting this work.

Conflict of Interest: None declared.

About the Authors

Kenneth Okereafor is Deputy General Manager and a United Nations trained Cybersecurity and Biometric expert with over two decades of Cybersecurity experience and special skills in managing and teaching Cyber Threat Intelligence & Mitigation Technologies in industry, government, and academia. He is a member of the International Organization for Standardization's Technical Committee on Health Informatics (ISO-TC-215), and he chairs the ISO's Security and Privacy Working Group-4 in Nigeria where he supports the development and adoption of Cybersecurity standards for Nigeria's digital health ecosystem. He holds a PhD in Cybersecurity & Biometrics from Azteca University, Mexico; and has research interests in, and publications on, Cybersecurity Incident Response, Multi-biometric Liveness Detection, Electronic Health Security, Telemedicine, Automation Management, and Digital Identities.

Rania Djehaiche is a PhD student in Electronics and Telecommunications Systems at the Mohamed El Bachir El Ibrahimi University of Bordj Bou Arreridj, Algeria. She has developed mobile applications in transport technology, electronic health, and home automation, and has research interests in Network Security, Mobile Applications, M2M Communications, and Internet of Things.

REFERENCES

[1] F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, N. F. Binti, M. Sani and F. Daryabar, "Digital Forensic Trends and Future," International Journal of Cyber-Security and Digital Forensics (IJCSDF) , vol. 2, no. 2, pp. 48 - 76, 2014.

[2] R. Bassett, L. Bass and P. O'Brien, "Computer Forensics: An Essential Ingredient for Cyber Security," Journal of Information Science and Technology, vol. 3, no. 1, pp. 22 - 32, 2006.

[3] "Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria," Internation Journal of Cybersecurity Intelligence and Cybercrime, vol. 2, no. 1, pp. 56 - 63, 2019.

[4] K. U. 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.

[5] 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.

[6] K. Kent , S. Chevalier, T. Grance and H. Dang , "Guide to Integrating Forensic Techniques into Incident Response," National Institute of Standards and Technology Special Publication 800-86 , Maryland, USA, 2006.

[7] Marthie Grobler, "Digital Forensic Standards: International Progress," in South African Information Security Multi-Conference (SAISMC) 2010, Port Elizabeth, South Africa, 2010.
[8] W. S. Tonye, "Cyber Forensic and Data Collection Challenges in Nigeria," Global Journal of Computer Science and Technology: G Interdisciplinary, vol. 18, no. 3, pp. 1 - 5, 2018.
[9] M. Tracy, W. Jansen, K. Scarfone and J. Butterfield , "NIST Guidelines on Electronic Mail Security," National Institute of Standards and Technology (NIST) Special Publication 800-45 Version 2, Maryland, USA, 2007.
[10] S. Rose, S. Nightingale, S. Garfinkel and R. Chandramouli, "Trustworthy Email," National Institute of Standards and Technology (NIST) Special Publication 800-177 Revision 1, Maryland, USA, 2019.
[11] P. A. Grassi, J. L. Fenton, E. M. Newton, N. B. Lefkovitz and Y.-Y. Choong, "Digital Identity Guidelines: Authentication and Lifecycle Management," National Institute of Standards and Technology (NIST) Special Publication 800-63B, Maryland, USA, 2017.
[12] SANS Institute, "Password Protection Policy," SANS Institute, Maryland, USA, 2017.
[13] SANS Institute, "Password Construction Guidelines," SANS Institute, Maryland, USA , 2017.
[14] A. Singhal , T. Winograd and K. Scarfone , "Guide to Secure Web Services," National Institute of Standards and Technology (NIST) Special Publication 800-95, Maryland, USA, 2007.
[15] SANS Institute, "Web Application Security Policy," SANS Institute, Maryland, USA, 2014.
[16] Krishni Naidu, "Web Application Security Checklist," SANS Institute, Maryland, USA, 2001.
[17] SANS Institute, "Securing Web Application Technologies (SWAT) CHECKLIST, Version 1.6," SANS Security Roadmap, Austin Texas, 2013.
[18] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," National Institute of Standards and Technology (NIST) Special Publication 800-94 , Maryland, USA, 2007.
[19] J. Wack, M. Tracy and M. Souppaya, "Guideline on Network Security Testing," National Institute of Standards and Technology Special Publication 800-42, Maryland, USA, 2003.
[20] Siddharth Prakash Rao, "Stuxnet , A new Cyberwar weapon : Analysis from a technical point of view," Aalto University, 2014.
[21] James Moos, "Cyber Forensics in a Post Stuxnet World," ITNOW, vol. 57, no. 4, pp. 32-32, 2015.
[22] M. Mago and F. F. Madyira, "Ransomware Software: Case of WannaCry," International Research Journal of Advanced Engineering and Science, vol. 3, no. 1, pp. 258-261, 2018.
[23] M. Akbanov, V. G. Vassilakis and M. D. Logothetis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms," Journal of Telecomminucations and Information Technology, vol. 1, no. 2019, pp. 113-124, 2019.
[24] CERT-MU , THE PETYA CYBER ATTACK, June 2017 .
[25] Reyner Aranta Lika, "NotPetya: Cyber Attack Prevention through Awareness via Gamification," IEEE, 2018.
[26] Team GAIT , THE NOTPETYA CASE, 2017.
[27] Shubhada S. Warke, "A Review on Applications of Supervisory Control and Data Acquisition (SCADA) Systems," Journal of Emerging Technologies and Innovative Research, vol. 3, no. 8, pp. 73-74, 2016.
[28] S. Hopkins and E. Kalaimannan, "Towards establishing a security engineered SCADA framework," Journal of Cybersecurity Technology, vol. 3, no. 1, pp. 47-59, 2019.
[29] P. W. Singer, "Stuxnet and its hidden lessons on the ethics of cyberweapons," Case Western Reserve Journal of International Law, vol. 47, no. 1, pp. 79-86, 2015.
[30] S. Collins and S. McCombie, "Stuxnet: the emergence of a new cyber weapon and its implications," Journal of Policing, Intelligence and Counter Terrorism, vol. 7, no. 1, pp. 80-91, 2012.
[31] Hindawi Publishing Corporation, "Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2012, no. 268478, pp. 1-10, 2012.
[32] G. KALLENBORN, "Six questions pour tout comprendre sur la cyberattaque mondiale NotPetya," 28/06/2017.
[33] T. Brewster, "3 Things You Can Do To Stop 'NotPetya' Ransomware Wrecking Your PC," Forbes, 28 6 2017. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2017/06/28/three-things-you-can-do-to-stop-notpetya-ransomware-wrecking-your-pc/#12853be377b0. [Accessed 23 4 2020].

.