IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 December 2022, accepted 21 December 2022, date of publication 23 December 2022,
date of current version 29 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3231847

RESEARCH ARTICLE

Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents

OLUFUNSHO I. FALOWO, (Member, IEEE), SAHEED POPOOLA, JOSETTE RIEP, VICTOR A. ADEWOPO, AND JACOB KOCH, (Member, IEEE)
School of Information Technology, University of Cincinnati, Cincinnati, OH 45221, USA
Corresponding author: Olufunsho I. Falowo (falowooi@mail.uc.edu)

ABSTRACT The exponential growth in the interconnectedness of people and devices, as well as the upward trend in cyberspace usage will continue to lead to a greater reliance on the internet. Most people's daily activities are dependent on their ability to navigate the internet to access and manage information. There are usually real risks associated with managing or accessing information, and these risks when exploited by threat actors, often lead to cybersecurity incidents. It is a common knowledge that a major cybersecurity incident is likely to result in significant financial losses, legal liability, privacy violations, reputational damage, sensitive data compromises, as well as national security implications. Threat actors usually employ various attack techniques to cause these incidents. After we identified the major cybersecurity incident report that is consolidated by the Center for Strategic & International Studies (CSIS) from which we derived the data of about the 803 major incidents that we analyzed, we then verified its (CSIS) credibility, non-partisan, global outreach and cybersecurity attack coverage by cross-referencing it with Data Breach Investigation Report (DBIR). We also through the lens of the Global Cybersecurity Index (GCI) ensured that this study is conducted within the context of cybersecurity principles. In reference to these attack techniques employed by threat actors, we conducted an exploratory investigation of 803 major cybersecurity incidents that were reported over the last decade. From a group of 244 of these major security incidents that happened and were reported between 2005 and 2021, this study reports that malware attack techniques were employed by threat actors to cause 48 percent of them and phishing attack techniques account for 19.7 percent of them. As many sources have confirmed the fact that major incidents will always happen, we echo the importance of readiness of organizations to conduct cybersecurity incident triage and or thorough investigation as necessary. Given the relevance of the guidelines outlined in the National Institute of Standards and Technology (NIST) incident response framework, we also recommend that organizations should adopt it or at least embrace similar guidelines as best as possible.

INDEX TERMS Data breach, DoS attacks, DDoS attacks, exploits of unpatched vulnerabilities, IoT attacks, major cybersecurity incidents, malware attacks, password attacks, phishing attacks, threat actors, zero-day exploits.

I. INTRODUCTION

The effectiveness of a cybersecurity incident investigation is largely dependent on sets of facts about what happened and insights which are available during the analysis and response to such incidents [1]. The availability of timely insights for cybersecurity incident response professionals and business leaders will enable them to make better judgements when investigating a cybersecurity incident or when thinking about investing in a defense [2]. In this study we seek to unravel insights that might be learned from major historical cyberattacks, especially with respect to common attack techniques used to execute major cybersecurity incidents that happened and were reported between 2005 and 2021.

The dependency on information through the cyberspace creates a landscape of vulnerabilities that are constantly being

The associate editor coordinating the review of this manuscript and approving it for publication was Yuan Gao.

analyzed or even exploited by threat actors [3]. Many private and public enterprises for example are not only vulnerable to cybersecurity threats on a daily basis but have also either directly or indirectly been impacted by at least a major cyber-attack in the last decade [4]. Because threat actors exploit these vulnerabilities, major cybersecurity incidents coupled with financial or reputational loss for victims are often the result [5].

As many public and private organizations are developing cybersecurity programs and initiatives, cyber threat actors are also constantly conducting reconnaissance attacks to gather intel on how organizations are thinking, which create an ever-evolving cybersecurity threats [6]. As an evolving cybersecurity landscape creates virtual ecosystem, nefarious actors would continue to conduct sophisticated cyberattacks [6]. Another example of a virtual ecosystem is the darknet marketplaces and hacker forums where discussion threads are a source of knowledge exchange and learning as members are constantly exchanging information [7]. This study aims to reflect on those significant cybersecurity incidents, analyze methods of attack, identify commonality and patterns synonymous to each incident and more importantly understand attack technique most prominent about each of the incidents.

A. RESEARCH QUESTIONS

The Center for Strategic and International Study [8] published more than 800 major cybersecurity incidents that occurred between 2005 and 2021. Figure 1 summarizes the count of these major incidents. This paper attempted to learn about the methods of attack that led to these major incidents with the objective to answer the research questions listed below. As Figure 1 highlights, more than 800 major cybersecurity incidents happened from 2005 to 2021. Using the under-listed research questions, this study attempted to explore these significant cybersecurity incidents with the objective of obtaining insights about how threat actors behaved over the last decade.

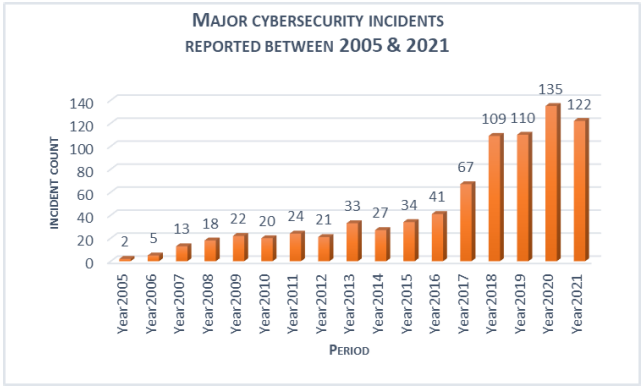

FIGURE 1. Major cybersecurity incidents.

- RQ1: With reference to the major cybersecurity incidents that happened over the last decade as reported by the CSIS [8], what are some of the lessons learned from common attack techniques?
- RQ2: With reference to the major cybersecurity incidents that happened over last decade as reported by the CSIS [8], are there evidence of major data breach?

B. COMMON ATTACK TECHNIQUES INVESTIGATED

In our effort to understand threat actors behavior over the last decade, we looked for common cyber attack techniques which include the following:

1) Denial of service (DoS) & Distributed denial of service (DDoS) attack technique,
2) Malware attack technique,
3) Phishing attack technique,
4) Zero-day exploit attack technique,
5) Password related attack techniques,
6) Exploit of unpatched vulnerability attack techniques and
7) Internet of things (IoT) attack technique.

There are many examples of common cyber attack techniques that threat actors usually employ to cause major incidents [8], [9] but this study focused on the ones listed above because they are very important and also very common with majority of the incidents that we investigated in this study. The frequency of the identified seven attack techniques is notable over the last decade [8] and hence another important reason we investigated them as part of this study.

II. BACKGROUND LITERATURE

Middleton [10] explored the history of cybersecurity attacks from 1980 to 2017, where he traced back cybersecurity incidents to 1976 when threat actors would use a combination of social engineering (and literally crawled into trash dumpsters to search through the garbage for computer information such as phone numbers, computer codes, technical information, usernames, and passwords) to circumvent a punch card system. Our study did not reflect on incidents beyond 2005 as Middleton [10] did but we explored up to 2021. Unlike Middleton, [10] our study did more thorough analysis and derived insights that business enterprises could consult when considering what cyber attack technique or method to pay most attention to. In Middleton's publication [10], he attempted to narrate some of the most notable attack techniques that threat actors leveraged to cause notable cybersecurity incidents but failed to share enough insights that might at least tell us what's trending in terms of attack techniques.

With reference to some of the major security incidents that happened from 2014 to 2018, Van's appraisal in his work [11] addressed the African perspective and as much as his publication articulated how those incidents impacted the African region, the outcome of that study did not provide sufficient analysis of cybersecurity threats and how they trended during the period investigated in that study. Unlike Van [11], our study is more inclusive of all the continents and have a more global perspective as no relevant nation state was was excluded. In this study, major cybersecurity incidents as

they impacted every region of the world, with consideration to global businesses and governments were factored into our thought process of how threat actors behaved and what types of attack techniques or methods were mostly used.

While major trends and challenges associated with cybersecurity in the US is appraised in Fonseca's work [12], it seems to exclude other parts of the world and did not in our view provide adequate insight into how threat actors behaved with respect to major incidents that impacted all the regions across the globe. Fonseca [12] focused more on how major trends and challenges in cybersecurity impacted US with very little or no context about threat actors' behavior towards other regions while our study on the other hand investigated every major cybersecurity incidents that were reported or announced and met a very high bar in terms of scope and impact. With reference to the items listed below, as identified in some of the above literature, our study intended to do a more thorough analysis of what is most notable attack techniques that were used by threat actors with the goal of identifying useful insights. Below are recap of the pros and cons of some of the related literature:

1) PROS OF RELATED LITERATURE

1) Through the lens of cybersecurity incidents, the literature we surveyed were insightful to the extent that we were able to compare and contract how cybersecurity attacks are approached in Africa and United States.
2) Clear articulation and valuable information about how threat actors leveraged social engineering and combine it with other attack techniques to execute successful attacks against their victim.
3) Variants of different attack techniques were also discussed in manner that is very informative.

2) CONS OF RELATED LITERATURE

1) With respect to cybersecurity attack trends, we identified insufficient insights in the study conducted by Middleton [10].
2) There seem to be exclusion of other continents in the analysis contained in van's paper [11] especially within the context of the impact of major cybersecurity incidents.
3) Lack of adequate information about how threat actors behaved in terms of attack techniques that lead to major incidents [12].

III. METHODOLOGY

The scope of this study centers around addressing the two research questions identified in the prior section of this paper. There is a report on Significant Cyber Incidents that ''focuses on cyber-attacks on government agencies, defense and high-tech companies, or has economic crimes or with losses of more than a million dollars'' [8] and is being consolidated by the Center for Strategic and International Studies (CSIS) [13]. In order to understand the facts about every major incident that we investigated, we studied the description of every incident in this CSIS report from 2005 to 2021 out of which we derived data represented in Figure 2, table 1 and table 2. The attack techniques that was scoped as the primary focal point of this study were selected because they are common [8], [9].

1) Malware Attack
2) Phishing Attack
3) Dos / DDoS Attack
4) Zero-Day Exploit
5) Exploit of Unpatched Vulnerabilities
6) Password Attacks
7) IoT Attacks

A. CONCEPTS AND DEFINITIONS

This section provides an overview of the major concepts and terminologies that we used or referred to in this paper.

1) RECONNAISSANCE

Reconnaissance phase of any attack is where threat actors gather information about the weakness of the targeted entity by conducting assessment to discover more intel that will sooner or later be exploited [6]. A reconnaissance attack could either be passive or active one, active reconnaissance is where the threat actor gathers information about the target in very subtle way while active reconnaissance on the other hand involves much deeper profiling of the target which often includes some advance methodology which sometimes might even trigger an alert if the target has the adequate detection system in place [14]. Significant cybersecurity incident that impacts hundreds, thousands or even millions of individuals and creates impacts on personal identifiable information or leads to significant financial loss are usually orchestrated with some level of reconnaissance planning by threat actors [15]. These threat actors in many cases usually begin the attack by conducting reconnaissance on the targeted victim [6].

2) DoS/DDoS ATTACKS

While DoS is an acronym that stands for denial of service, DDoS on the other hand means distributed denial of service [16]. A DoS attack is simply when entities or persons are denied authorized access to resource or service because threat actor have used a specific method or a combination of attack techniques to destroy or disrupt the underlying infrastructure with aim of making resources unavailable [17]. DDoS attack is usually based on a DoS principle but involves the deployment of multiple computers to flood the target [18].

3) PHISHING ATTACKS

Phishing is a new term coined from the word 'fishing', it first appeared in the hacking community in 1990 and it is a type of attack that typically attempt to trick the victim into clicking on a malicious link with goal of obtaining sensitive information [19]. Phishing attack leverages a social engineering technique whereby a threat actor deceives the targeted victim in order to obtain valuable information and in most phishing

attacks, the impacted person gets redirected to a malicious website [20]. Phishing attack could be targeted at a specific high value target or an organization or even an entire nation state, depending on the goal of the threat actor behind the attack [21], [22], [23].

4) MALWARE ATTACKS

This type of attack is very common in software [24]. Malware is a software that harmfully attacks other software in ways that causes the actual behavior to differ from the intended behavior [24]. Threat actors tend to use this type of method to execute many attacks that could be in form of viruses, ransomware, trojans, remote access trojans (RAT), advanced persistent threats (APT) and the list goes on [25], [26], and [27]. APT is one of the most concerning type of malware, as it persistently collects data from a specific target by exploiting vulnerabilities using diverse attack techniques [28].

5) DATA BREACH

A data breach is the intentional or inadvertent exposure of confidential or proprietary information to unauthorized parties which could lead to significant reputational damage, financial losses, and might be detrimental to the long-term stability of the impacted organization [29]. Data breach is often used interchangeably with network breach [29], [30].

6) PASSWORD ATTACKS

In attempt to either compromise systems or steal sensitive information, threat actors leverage different types of method and technique to conduct password related attacks [31], [32]. Access into any system requires some sort of credentials which typically include username and password or and code [31]. Threat actors persistently combine many techniques such as social engineering attack, dictionary attack, or brute force attacks to extract login credentials which include usernames and passwords in many cases [31], [32]. Millions of user login credentials have been compromised in the last decade with usernames and passwords exposed into the dark web [33]. In April 2020 for example, an estimate of 500,000 stolen zoom passwords including login credentials, victim personal meeting URLs, and host keys were available for sale in darknet markets while some account credentials were made available for free [33].

7) ZERO-DAY EXPLOIT

While many security systems have capability to detect known vulnerabilities due to the signatures associated with them, a zero-day vulnerability is hard to detect [34]. Zero-day exploits are very difficult to detect because of no previously known signature associated with them until its exploit is eventually announced to the public [35]. A zero-day attack may be executed in many forms, for example it could be application based or network based. A network based zero-day attack for example may be described as any new attack that seeks to exploit unknown vulnerabilities in a network system [36].

8) EXPLOIT OF UNPATCHED VULNERABILITIES

Unlike zero-day exploit, the exploit of unpatched vulnerabilities is predictable [37], [38]. Threat actors conduct reconnaissance to gather information about unpatched vulnerabilities as these are like the low-hanging fruits for hackers [6]. While many organizations and government institutions are doing Vulnerability Management program across their enterprises, it is impossible and not cost-effective to patch all detected known vulnerabilities, therefore many of these organizations end up focusing on the high to critical severity vulnerabilities while in some cases the low to medium severity vulnerabilities are either accepted as a risk or ignored as benign security issue [39], [40]. Threat actors never stop searching for those unpatched vulnerabilities to exploit [41], [42]. There are other scenarios where the design of software systems may contain flaws that negatively affect quality and maintainability [43], thereby creating a vulnerability that if exploited may be disruptive to an organization [39], [40].

9) IoT ATTACKS

IoT stands for internet of things which describes the interconnectedness of devices over the internet [44]. IoT devices underpin many technological trends and infrastructures, such as smart homes and smart cities [44], [45]. While these internet-connected devices generate, process, and exchange significant volumes of data during their operations, utilizing many internet protocols, in many cases they are exposed to cybersecurity threats [44], [45], [46].

B. STUDY STRATEGY

As part of the preliminary assessment to determined if this study was relevant or not, we searched Google database by querying for "**major cybersecurity incidents**" and the result of that search included non-independent or partisan reports from many organizations but after reading through and reviewing some of them, we decided to narrow down to the report from an independent and non-partisan organisation. We agreed to use the report titled 'Significant Cyber Incidents' from the Center for Strategic and International Study. In addition, we queried the Google scholar search engine database for literature that helped us understand prior research related to our study. During the selection of literature referenced in this paper, Google scholar search engine was where we identified relevant works that provided us with additional contexts of what have already been written about major cybersecurity incidents and what the trends are.

C. STUDY PROCEDURE & DATA EXTRACTION

After we studied the identified background literature to gather additional contexts and to learn from similar works, we identified gaps and limitations in those works which subsequently led to the beginning of our study. As part of our efforts to gather relevant information, we then analyzed the report titled 'Significant Cyber Incidents' [8] to identify useful data-point,

metrics and other useful information that were instrumental in deriving the data referenced in figure 2, table 1 and table 2.

1) VALIDATION OF THE CSIS DATABASE

Even though we established the credibility, independence, non-partisan, global outreach and attack coverage of the CSIS major incident report [13], we also as part of our due diligent, used the Data Breach Investigation Report (DBIR) [47], [48], [49] to cross-validate the attack techniques that we analyzed. We also through the lens of the Global Cybersecurity Index (GCI) [50], [51], [52], ensured that this study is conducted within the context of cybersecurity principles

2) DATA BREACH INVESTIGATION REPORT

One of the most thorough cyber security reports available online is Verizon's Data Breach Investigation Report (DBIR) [47], [48], [49]. The DBIR is used by security professionals to gather first-hand accounts of potentially devastating data breaches based on data-driven analysis [47], [48], [49]. This report was also used to validate the occurrences of some of the cybersecurity incidents and attack methods that we looked at.

3) THE GLOBAL CYBERSECURITY INDEX

Due to the wide range of applications that cybersecurity has, the level of system development in each nation is evaluated using five categories: capacity building, organizational measures, technical measures, legal measures, and cooperation [50], [51], [52]. These categories are then combined to produce an overall evaluation by nations and oftentimes are also referenced by private organizations [50], [51], [52]. In this study, the GCI was consulted prior to our analysis of the cybersecurity incidents and the attack techniques that we looked at in order to enhance our awareness of the significance and various aspects of the Global Cybersecurity Index which is a reliable tool that tracks how governments throughout the world are carrying out their obligations to cyber security.

D. DATA COLLECTION

After the analysis of 803 incidents, we identified 244 major incidents that are related to the seven attack techniques highlighted in the prior subsections. The dataset in the figure 2 represents the breakdown of these 244 major cybersecurity incidents that happened during the period of 2006 and 2021 that subsequently emerged as the most relevant derived data used in this study. As part of our efforts to derive that data used in this study, our analysis included the studying of the consolidated major incident report obtained from Center for Strategic and International Study [8] and based on the facts presented in the description of each incidents, we made determination of what attack technique(s) was used by threat actors for each major incident. Another important reason for the selection of the CSIS database [8] as the source of major cybersecurity incidents that we analyzed is due to its inclusiveness of all the regions [53] of the world which includes the coverage of the following regions:

1) Africa
2) America
3) Arctic
4) Asia
5) Europe
6) Middle East
7) Russia and Eurasia

1) EXAMPLES OF INCIDENTS IN CSIS REPORT [8]

The following are description of five examples out of the identified 803 significant cyber incidents reported in the CSIS report [8] that we analyzed for this study:

1) "April 2021: Malware triggered an outage for airline reservation systems that caused the networks of 20 low-cost airlines around the world to crash" [8].
2) "April 2021: Russian hackers targeted Ukrainian government officials with spearphishing attempts as tensions between the two nations rose during early 2021" [8].

TABLE 1. Data breach incidents (Group A).

Year	2005	2006	2007	2008	2009	2010	2011	2012	2013
Data Breach	2	2	11	16	15	14	16	9	18
Year	2014	2015	2016	2017	2018	2019	2020	2021	2022
Data Breach	17	19	24	20	26	5	21	25	NA

3) "May 2021: A large DDoS attack disabled the ISP used by Belgium's government, impacting more than 200 organizations causing the cancellation of multiple Parliamentary meetings" [8].

TABLE 2. Other attack techniques (Group C).

Year	2006	2007	2008	2009	2010	2011	2012	2013
Other Attack techniques	1		1	3	2	3		6
Year	2014	2015	2016	2017	2018	2019	2020	2021
Other Attack techniques	6	7	4	22	50	78	70	46

4) "March 2021: U.S. Cyber Command confirmed that it was assisting Columbia in responding to election interference and influence operations" [8].
5) "March 2021: Both Russian and Chinese intelligence services targeted the European Medicines Agency in 2020 in unrelated campaigns, stealing documents relating to COVID-19 vaccines and medicines" [8].

2) ANALYSIS OF INCIDENT

This section is additional description of how we analyzed the incidents in the CSIS [8] report. Looking at the first incidents in the 5 examples in the above subsection, malware attack technique is the most notable cause of that attack. The second example above also highlights how phishing attack was employed to conduct the hack [8] which validates that phishing attack technique as the notable method used to execute that attack. While the forth example suggests that threat actor(s) employed other attack technique(s) different

from the techniques mentioned in Figure 2, the fifth example indicates evidence of a data breach because confidential documents were exposed to unauthorized parties. Analysis of these examples are similar to how we evaluated the entire 803 incidents that we investigated for this paper.

Year / Attack Techniques	Occurrences of Malware Attacks	Occurrences of Phishing Attacks	Occurrences of DoS / DDoS Attacks	Occurrences of Zero-Day Exploit Attacks	Occurrences of Exploit of Unpatched Vulnerabilities	Occurrences of Password Attacks	Occurrences of IoT Attacks
2006	1		1				
2007	1		1				
2008	1						
2009	3		1				
2010	3				1		
2011	1	3	1				
2012	8	2	2				
2013	3		5	1			
2014	2	1		1			
2015	3	3	1			1	
2016	5	3	1		2	2	
2017	12	6	1		4	2	
2018	25	1	2	2	1	1	1
2019	9	8	5		2	2	1
2020	19	13	4	2	6		
2021	21	8	8	1	7	6	

FIGURE 2. Count of major incidents (Group B).

IV. RESULTS

In this study, we analyzed a total of 803 cybersecurity incidents of major significance from 2005 to 2021. With reference to figure 2 above, 30 percent of these 803 major cybersecurity incidents were caused by at least one of the following attack techniques or methods: malware attack technique, phishing attack technique, DoS/DDoS attack technique, zero-day exploit, exploit of unpatched vulnerabilities, password attack technique and IoT attacks. In respect to table 2, we also report that 38 percent of the major cybersecurity incidents (the total 803 incidents) analyzed were either caused because of cyber espionage, undisclosed causes, or a combination of multiple unclear attack techniques.

We found 32 percent of the total 803 major incidents that we investigated to have evidence of notable data breach as highlighted in table 1. For the purpose of analysis of the data used in this study, all the major data breach incidents identified in table 1, which constitute the 32 percent of the total 803 incidents (we looked into) is labeled as **Group A**, while the incidents highlighted in figure 2, which constitute the 30 percent of the 803 incidents investigated is labelled as **Group B** and the last category of major incidents identified in table 2, which constitute 38 percent of the total 803 incidents are incidents that were either caused by cyber espionage or other undisclosed methods - this category is labelled as **Group C.** Overall, this study reports that significant cybersecurity incidents have been increasingly trending upward since 2005 to 2020 as highlighted in the trend line below:

A. MALWARE ATTACKS

This study reports that malware attacks (which includes ransomware, virus, worms, RAT, APT, etcetera) have been persistently, increasingly, and mostly being used by threat actors from 2005 to 2021. Out of the major cybersecurity incidents investigated in Group B category, malware attack techniques were the most notable cause of 48.0 percent of the group of

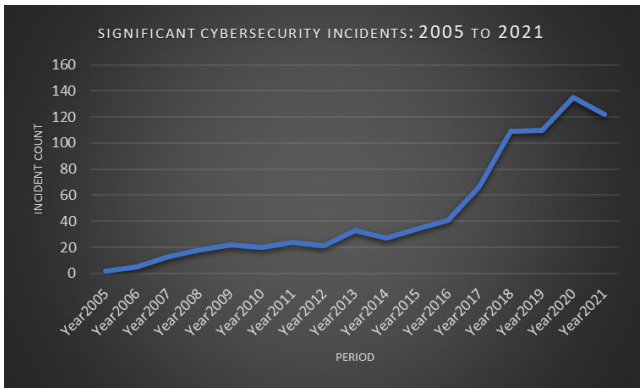

FIGURE 3. Trends of major cybersecurity incidents.

244 major incidents. Threat actors significantly increased the use of malware attack methods in 2017 as figure 4 indicates. In this same figure 4, the 2018 number of significant cybersecurity incidents caused by malware doubled the 2017 count which suggest the aggressive use of malware attack techniques by threat actors to disrupt. Still on figure 4 below, this study reports a downward trend from 2012 to 2014, but later increased into double digit and eventually surged in 2018. These evidences suggest that use of malware attack techniques is increasing at an alarming rate.

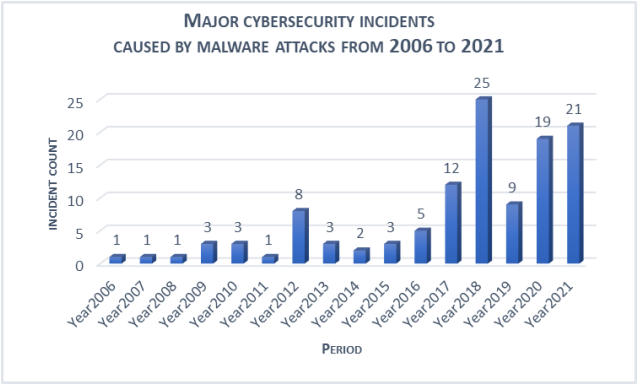

FIGURE 4. Major cybersecurity incidents caused by malware.

B. PHISHING ATTACKS

In the Group B category, it was also notable to find that threat actors successfully employed phishing attack methods to cause significant cybersecurity incidents between 2011 and 2021. Phishing in the framework of this study includes all the various types of phishing attacks such as vishing, smearphishing etc. This study reports 19.7 percent of all the major cybersecurity incidents analyzed in Group B category was caused by phishing attacks. It is also clear from the chart below (figure 5) that threat actors were more aggressive with use of phishing attacks from 2019 to 2021.

C. DoS/DDoS ATTACKS

This type of attack is very common as it is one of the techniques easily used by threat actors to disrupt services or

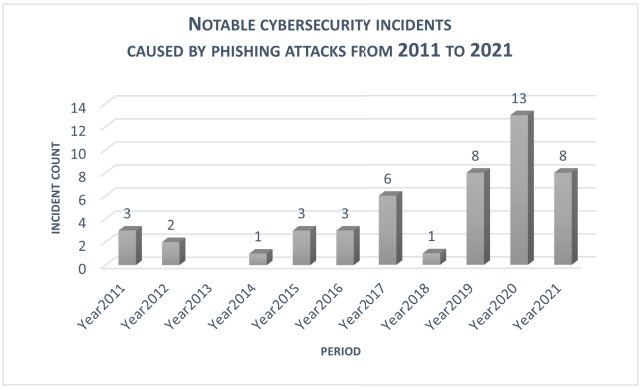

FIGURE 5. Major cybersecurity incidents caused by phishing.

resources of the target victims [16]. DoS/DDoS attacks have caused major cybersecurity incidents since 2006 with a big leap in 2013 as indicated from the chart below (figure 6). Like phishing attacks highlights in figure 5, DoS/DDoS as well led to significant cybersecurity incident between 2019 and 2021. This study reports DoS/DDoS attack techniques account for 13.5 percent of major cybersecurity incidents investigated in the Group B category of this study.

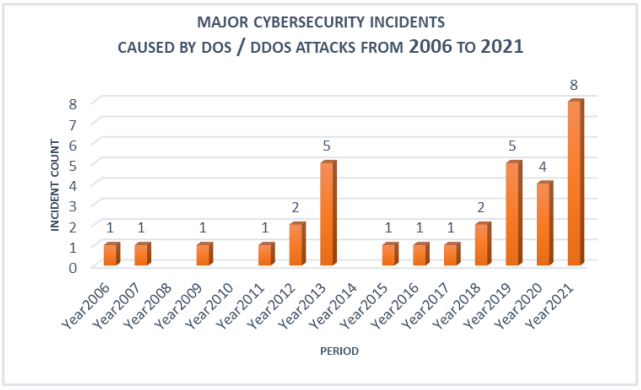

FIGURE 6. Major cybersecurity incidents caused by DoS or DDoS.

D. ZERO-DAY EXPLOIT

From the major cybersecurity incidents that we investigated in the Group B category, this study reports zero-day exploit was announced to have been the notable cause of a major cybersecurity incident in 2013 and the following year but this type of attack later doubled in both 2018 and 2020 according to our study. This type of attack is accountable for less than 3 percent of the major cybersecurity incidents that we investigated in the Group B category.

E. EXPLOIT OF UNPATCHED VULNERABILITIES

This study reports that exploit of unpatched vulnerabilities makes up the cause of 9.4 percent of the major cybersecurity incidents we investigated in the Group B. This type of attack, according to our study, picked up the steam again in 2016 and have been increasingly causing significant cybersecurity incident up to 2021 as highlighted in the chart below:

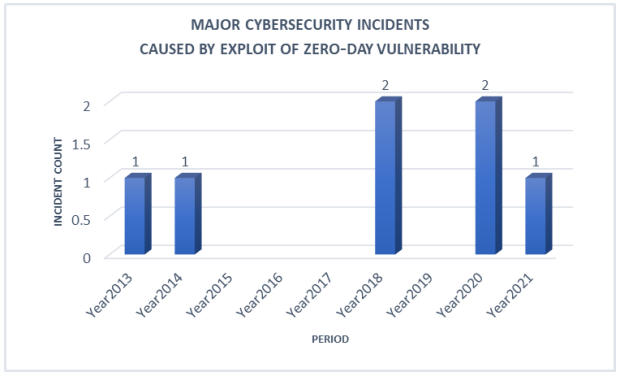

FIGURE 7. Major cybersecurity incidents caused by zero-day.

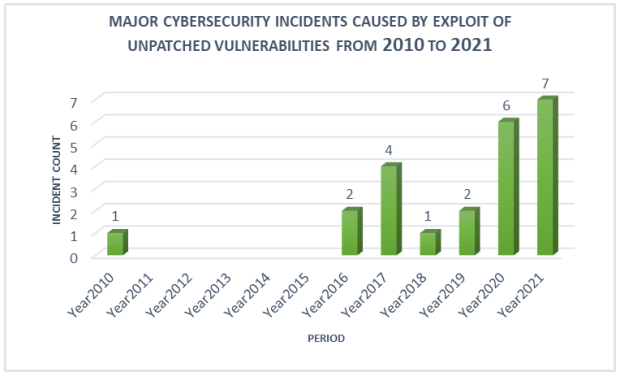

FIGURE 8. Major cybersecurity incidents caused by exploit of unpatched vulnerabilities.

F. PASSWORD ATTACKS

Password attacks which include among many, the dictionary password attacks, password brute force attacks, or password attack based on social engineering [31], [32], constitute less than 2 percent of the cybersecurity incidents that we investigated in Group B of this study. This study reports that threat actors started more recently in 2015 to engage in password related attack techniques to cause major cybersecurity incidents. This study also report that occurrences of major cybersecurity incidents caused by password related attacks in 2021 multiply by three from 2019, which is very significant.

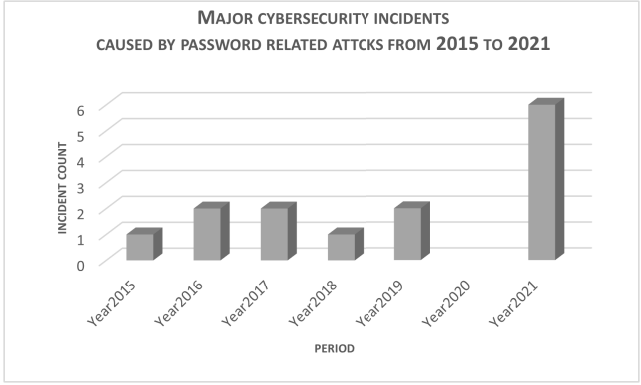

FIGURE 9. Major cybersecurity incidents caused by password attacks.

G. IoT ATTACKS

From the major incidents that we investigated in Group B category of this study, we only observed two IoT cybersecurity incidents which were announced or disclosed in 2018 and 2019.

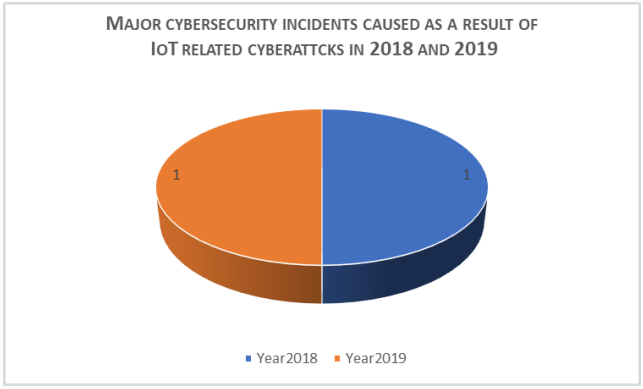

FIGURE 10. Major cybersecurity incidents caused by IoT attacks.

H. TRENDS OF ATTACK METHODS

Out of the common attack techniques that were used as a criteria to analyze the major cybersecurity incidents we investigated in this study, malware attack and DoS/DDoS attack have been persistently used by threat actors since 2006 in almost every year up to 2021. Malware attack techniques according to our study are the most likely to be used by threat actors, which we can derive from the chart below to be trending upward again from 2019.

I. COMPARISON OF ATTACK TECHNIQUES

Even when the seven attack methods we used as criteria to conduct our study is compared side-by-side as highlighted in figure 12, our study reports that malware attack techniques are employed by threat actors to cause the majority of the cybersecurity incidents that were reported between 2016 and 2021 more than other attack techniques.

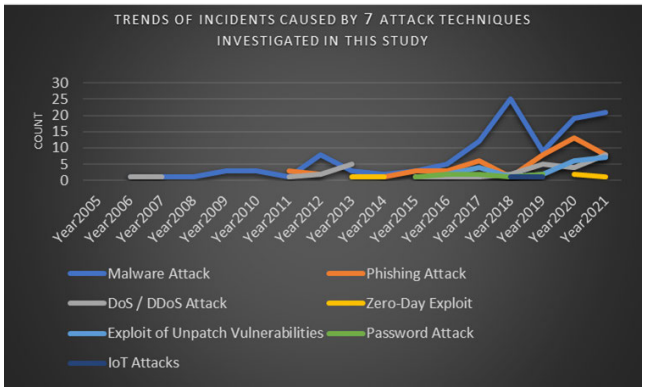

FIGURE 11. Trends of major cybersecurity incidents.

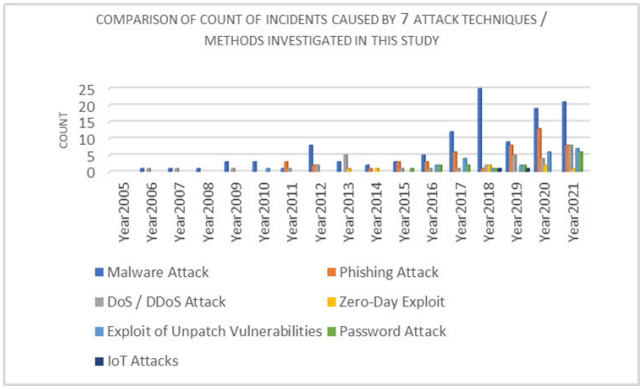

FIGURE 12. Comparison of attack techniques.

J. TRENDS OF NOTABLE DATA BREACH INCIDENTS, COMPARED WITH 7 ATTACK TECHNIQUES

With reference to the chart in figure 13, this study reports notable drop in major cybersecurity incidents that were caused by either malware attacks and a drop in the number of incidents that resulted in a data breach in 2019. We also observe immediate upward trends in similar situations (malware attacks and data breach incidents) by 2020 and 2021. Regardless of these similarities, our study did not make any direct correlation between every data breach and every malware attacks that happened between 2019 and 2021.

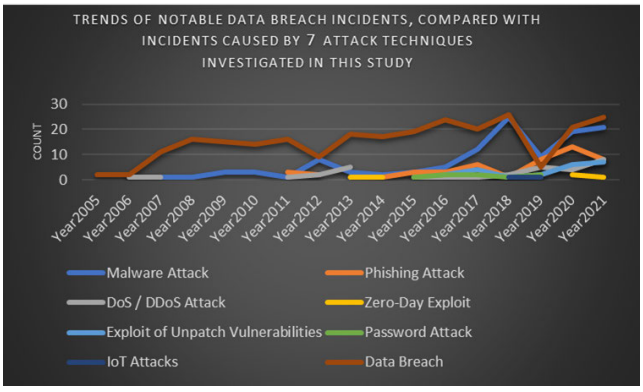

FIGURE 13. Trends of notable data breach incidents compared with other cybersecurity incidents.

K. OTHER ATTACK TECHNIQUES

Apart from the major cybersecurity incidents that resulted in data breach events as we investigated in Group A category and major cybersecurity incidents caused by the seven attack techniques that we studied from the Group B category, we also did a very limited exploration of incidents caused by other attack techniques. The incidents in this category (incidents caused by other attack techniques) were either caused by cyber espionage, other undisclosed attack methods, or had insufficient information [8]. Figure 14 below indicates that there are many other major cybersecurity incidents that were caused by different types of attack techniques and methods between 2006 and 2021.

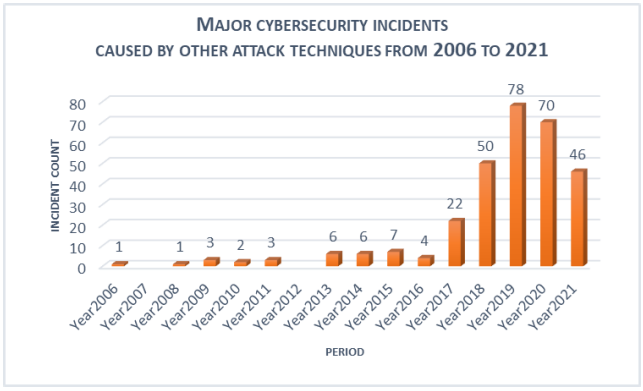

FIGURE 14. Major security incidents caused by other attack techniques.

V. DISCUSSION

A. THREAT ACTORS' BEHAVIOR:- ANALYSIS/LESSONS LEARNED

As observed in this study, phishing attacks are becoming more sophisticated as threat actors are adopting multiple new and creative methods through which to conduct this type of attacks. Distributed denial of service (DDoS) or denial of service (DoS) attacks remain a persistent nuisance on the Internet [54] and this is also confirmed by our study. Although zero-day exploit has been something threat actors have always used in many decades [55] but we did not observe many of it leading to major cybersecurity incident over the last decade.Unlike zero-day exploit, the exploit of unpatched vulnerability is predictable [38] and seems to be trending up since 2016 according to our finding.

Although this study reports one major incident from exploit of unpatched vulnerabilities in 2010 (as highlighted in figure 8) but the following four years later indicated that either government agencies and corporate organizations had a comprehensive patching programs together with system hardening programs in place or threat actors were focused on the use of other techniques to attack their victims. This type of techniques allows threat actors to easily conduct reconnaissance, gather information about unpatched vulnerabilities and then most likely exploit it [41].

Password attacks are very common and have always been a major concern in the cybersecurity space [31], [32]. This type of attack experienced a surge in 2021 as indicated in figure 9, especially when compared with other years since 2015. Although millions of devices are connected to the internet and there have always been IoT related cybersecurity incidents in last decade [44], [45] but our study did not report many of IoT related attacks. Given findings and observations obtained from this study, the two research questions posed at the beginning of this study have been reasonably addressed. Using the common attack techniques as one of the criteria used to evaluate the CSIS report [8], this study reports how threat actors behaved in terms of what common attack types were explored the most or the least over the last decade.

1) ADDITIONAL INSIGHTS FROM COMMON ATTACK TECHNIQUES

Based on insights derived from this study, the real-world impact of these major incidents are very significant. In reference to the dataset in Figure 2 for example, malware attacks were primarily responsible for 48.0 percent of major cybersecurity incidents while phishing attacks accounts for 19.7 percent of them. The percent of major incidents caused by malware attacks as reported in this study is very likely to be the result of the computerization of many enterprises and the user interaction with these computer attacks [56], [57]. DoS/DDoS on the other hand, caused 13.5 percent of the major cybersecurity incidents identified in this study. This is significant, but also expected, as a DoS attack can happen at every layer of the OSI model [58]. While this study indicates that, exploit of unpatched vulnerabilities resulted in 9.4 percent of major incidents, it is important to add that by remediating unpatched vulnerabilities, it has the likelihood to reduce incidents caused by the exploit of unpatched vulnerabilities [59], [60].

2) DATA BREACH INCIDENTS

This study also found evidence that some of the major cybersecurity events that happened over the last decade, lead to major data breach incidents. The data in Table 1 highlights our observation of data breach incidents between 2005 and 2021. These findings about major data breach incidents answers our second research question. The data about major data breach incidents as we observed in this study, suggests that the likelihood major incident will lead to a major data breach incident is certain. In addition to a thorough investigation, and incident response plan, it is also highly recommended that every organization have a recovery plan in place to address data breach incidents when it happens [30], [61], [62].

VI. CONCLUSION

No organization, including small, medium, and large businesses or government institutions, is safe from today's sophisticated cyberattacks, even those with the highest or most robust security controls in place [63]. This is also confirmed in the geographical distribution of all the different sizes of organizations impacted by cybersecurity incidents that were investigated in this study. Therefore, the outcome of this study vis-à-vis the analysis of these cybersecurity attack methods have indicated the importance of having a prepared incident management capability in place and by that we mean having a combination of both administrative and technical capabilities in place to respond when any of the attack methods mentioned in this study occurs.

A. ADMINISTRATIVE MITIGATION CONTROLS

In this part, we highlight a few administrative measures that businesses use, or at the very least consider, when getting ready for or responding to a cybersecurity attack. Although

the list below is not exhaustive, it does at least outline some of these administrative mitigation controls:

1) COMMUNICATION

Leveraging effective internal and external communication during the handling of a cybersecurity attack (such as the ones mentioned in this study) may be valuable towards addressing identified cyber threats, especially given how in "today's cyber threat landscape, a wide variety of skills and coordination are needed to combat increasingly complex challenges." [64]. The value of effective communication should not be undermined when addressing cybersecurity threats.

2) INFORMATION SHARING

Prior to the occurrence of a significant security attack or during active cybersecurity incident investigation, having the necessary information sharing strategy in place and effectively executing such strategy is very important for ensuring that all parties are kept informed in the prior, during, and post stages of any given cybersecurity incident handling [64], [65], [66], [67], [68], [69]. "Information about threats can improve an organization's situational awareness, expand its understanding of the current threat horizon and increase its defensive agility by improving decision making" [64].

3) TRAINING

An organization's information assets often leak out due to employees' careless behavior, such as downloading emails sent by an unknown sender, checking linked pages hastily, or setting passwords by their own birthdays [70]. Therefore, it is crucial to make the necessary investments and implement the appropriate programs to ensure the implementation of information security training and education for employees [70]. A routine tabletop exercise improves the knowledge, comprehension, and readiness of cybersecurity incident response teams, making it one of the ways to prepare for addressing a severe cybersecurity attack [71].

4) POLICIES, PROCESSES, PROCEDURE AND STANDARD FRAMEWORKS

In order to ensure readiness for a potential cybersecurity attack, it is essential to have an enterprise incident response policy, well-documented processes, clear procedures, defined standards, and other relevant artifacts in place [72], [73], [74]. If these artifacts are rigorously enforced, they could not only ensure adequate response during incident handling but may also help to avoid a disastrous situation [72], [73], [74].

B. TECHNICAL MITIGATION CONTROLS

Some of the major procedures necessary to address cybersecurity attacks include monitoring security events, compiling and keeping security logs, correlating and evaluating all data related to the incident that has occurred or is occurring [63]. This section focuses on some of the technical mitigation capabilities used by businesses to handle cybersecurity incidents. The capabilities mentioned in this area frequently call for advanced technology and technical knowledge.

1) MONITORING AND DETECTION

Gaining visibility into the continuously changing security threats, spotting early warning signs of compromise, and correlating security logs to determine whether a cybersecurity event has taken place are crucial for successfully implementing a prompt and suitable reaction to cybersecurity attacks [63], [75], [76]. An organization may be able to achieve a reasonable mean-time-to-detect a major cybersecurity event by ensuring monitoring and detection capabilities are implemented [63], [75].

2) ANALYSIS AND CORRELATION OF SECURITY LOGS

As a result of the increasing frequency, scope, sophistication, and severity of cybersecurity attacks, which constantly pose a danger to organizations, governments, and enterprises, it is crucial to be able to undertake data-driven analysis as well as real-time analytics of the incident [63], [75], [75]. Unnecessary delays in cyber threat detection, analysis, and response may cost organizations a high price [63]. Therefore, by leveraging a Security Information & Event Management (SIEM) tool may enhance efficiency in detecting these attacks.

3) CONTAINMENT, REMEDIATION AND RECOVERY

After detection, analysis and investigation of a cybersecurity attack, the next phase usually involves containment, remediation, and, where necessary, ensuring recovery after the threat has been detected and analyzed [77]. Employing intrusion prevention systems, patching the vulnerable programs, hardening the operating system, changing passwords, blocking hash values of malicious files, and utilizing endpoint protection systems are some examples of containment capabilities [77], [78], [79], [80] that are applicable to deal with the cybersecurity attacks mentioned in this study.

C. LIMITATIONS

This study had limitations in some areas and given the limited scope of this study, we focused on the information that is available to us during our investigation and analysis. Below are some of the limitations associated with this study:

1) This study relied on the accuracy of the consolidated report of Significant Cyber Incidents [8] published by the Center for Strategic & International Studies, from which we derived the dataset used in this study. We leveraged DBIR reports to validate the credibility and accuracy of this CSIS data.
2) In this study, we did not have the resources to obtain the root cause analysis of each of the incidents we analyzed, therefore, no rigorous investigation was done. Root cause of every incident was irrelevant to our study, hence out of scope.
3) While our study provided insights on how threat actors have behaved over the last decade, it did not sufficiently

addressed real-world impacts such as financial losses, legal liability, privacy violations, reputational damage, sensitive data compromises, as well as national security implications etc. Future study will address this gap.

4) The decision of what is most notable technique or method in each of the incidents investigated was solely based on the professional experience and interpretation of the authors of this study and may reflect some subjective views.
5) Some of the security incidents investigated were based of combination of more than one attack techniques or methods in some scenarios but the determination of what's most notable about each of these incidents was decided based on the experience and interpretation of the authors of this study and may reflect some subjective views.

D. FINAL THOUGHTS

Given how malware, phishing, DoS/DDoS and the exploit of unpatched vulnerabilities attacks have been very prominent in the cause of major cybersecurity incidents over the last decade according to our study, one of our future works will include the reflection and investigation of how government entities, individuals and many organizations have been significantly impacted by these types of attack techniques, especially in relation to financial, privacy or legal impacts. Following the indicators in this study that threat actors have constantly aimed to cause data breach, execute malware and phishing attacks, we recommend that organizations and government agencies should expect these attacks and not just be prepared to respond with mitigation controls in place but should enhance their cybersecurity programs to ensure defense in depth. Below are some ideas on how to manage or handle the cybersecurity attacks that we mentioned in this study.

1) IMPORTANT INCIDENT RESPONSE FRAMEWORKS

Identified here are two of the most widely used guidelines for handling cybersecurity attacks i.e. (1) The National Institute of Standards and Technology (NIST) and (2) Sysadmin, Audit, Network, and Security (SANS) incident response frameworks [81]. Both of these incident response frameworks concur on the following steps necessary for an efficient incident response, as shown in the "incident response steps" (figure 15):

No.	NIST Framework	SANS Framework
1	Preparation	Preparation
2	Detection & Analysis	Identification
3	Containment, Eradication & Recovery	Containment
4		Eradication
5		Recovery
6	Post-Incident Activity	Lesson Learned

FIGURE 15. Incident response steps.

The National Institute of Standards and Technology, or NIST for short, is a branch of the U.S. government that specializes in all things technological [2], [81], [82]. One of the most well-known methods for better comprehending and managing cybersecurity risk is the Cybersecurity Framework it provides [2], [81], [82]. A component of the NIST overall guidelines is the NIST Incident Framework, one of the most commonly used incident response standards in the world [2], [81], [82]. Sysadmin, Audit, Network, and Security (SANS) is a private organization that carries out research and educates the industry in cyber disciplines. In contrast to the NIST framework, which has a wider operational scope, the SANS framework primarily focuses on security [2], [81], [82]. For the fact that cybersecurity attacks will always happen, the readiness of organizations to conduct triage and in-depth investigations are crucial. Using the NIST framework as an example, we recommend that organizations decide which stages of the NIST framework are applicable to them.

2) GLOBAL PRIVACY & CYBERSECURITY REGULATIONS

It is also a fact and a common knowledge that with regards to how organizations respond to cyberattacks, ensuring compliance with the law of any given country is very important. Hence, besides leveraging either the NIST or the SANS incident response framework as we highlighted in this study, we also recommend that organizations must regularly evaluate how their cybersecurity incident and data breach response strategies will be impacted by the constantly changing regulatory requirements / laws. As of the time of this study, there are many of these laws in various countries but below in table 3 are very few examples of these regulatory and privacy laws.

3) POTENTIAL SIZE BIAS

Considering the fact that there are many thousands of IoT related attacks, password attacks or attacks caused by exploits of unpatched vulnerabilities etc., which do not reflect in our derived data, it is pertinent to reiterate that we only focused on cyber-attacks on government agencies, defense and high technology companies, or economic crimes with losses of more than a million dollars. While our primary data provided empirical content on major organizations, there is no evidence that suggested or provided hints on small and medium sizes of organizations. While small and medium-sized businesses make up the vast majority of businesses in the United States of America [96] as well as in the Organisation for Economic Co-operation and Development (OECD) countries where 95 percent of businesses in these countries are small and medium-sized [97], [98], we primarily focused on large-size organizations in this study. Given the enormous number of small and medium-sized businesses, it is highly possible that the empirical inputs from the majority of the cybersecurity incidents that we analyzed may also be size-biased, and consequently, our output may have differed slightly.

In response to the size-bias, we also recommend further research in near future to investigate possible impacts and

TABLE 3. Privacy & cybersecurity regulations.

Regions	Countries	Privacy & Cybersecurity Regulations
Asia	China	Personal Information Protection Law (PIPL) [83], [84]
	South Korea	Personal Information Protection Act (PIPA) [84]
	Singapore	Personal Data Protection Act (PDPA) [84]
European	European Union	General Data Protection Regulation (GDPR) [85]
	United Kingdom	Data Protection Laws (DPA 2018, GDPR) [86]
North America	Canada	Personal Information Protection and Electronic Documents Act (PIPEDA) [87]
	Virginia	Consumer Data Protection Act (CDPA) [88]
	Colorado	Colorado Privacy Act (CPA) [89]
	Califonia	California Consumer Privacy Act (CCPA) [90]
	US Banks	Computer-Security Incident Notification Requirements for US Banks [91]
	US Critical Infrastructure	Cyber Incident Reporting for Critical Infrastructure Act [92]
Oceania	Australia	Australian Privacy Act [93]
	New Zealand	New Zealand Privacy Act 2020 [94]
South America	Brazil	Lei Geral de Proteção de Dados Pessoais (LGPD) [95]

trends caused by these cybersecurity attack methods on small and medium size businesses.

ACKNOWLEDGMENT

The authors would like to thank the School of Information Technology, University of Cincinnati, OH, for providing them with the tools, environment, and guidance to conduct this study. The primary dataset used or referenced in this study is derived from the Significant Cyber Incidents report that is consolidated by the Center for Strategic & International Studies (CSIS), but cross-referenced and validated with Data Breach Investigation Reports (DBIR). Any perspective, findings, observation, interpretations, recommendation, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of either the CSIS or the DBIR. The data used or referenced in this study is derived from the Significant Cyber Incidents report that is consolidated by the Center for Strategic & International Studies but cross-referenced and validated with Data Breach Investigation Reports.

REFERENCES

[1] G. K. I. Shea, "A phenomenological examination of susceptibility to cyber deception," Ph.D. dissertation, Colorado Tech. Univ., 2016.

[2] N. Shinde and P. Kulkarni, "Cyber incident response and planning: A flexible approach," *Comput. Fraud Secur.*, vol. 2021, no. 1, pp. 14–19, Jan. 2021.

[3] M. Sailio, O.-M. Latvala, and A. Szanto, "Cyber threat actors for the factory of the future," *Appl. Sci.*, vol. 10, no. 12, p. 4334, Jun. 2020.

[4] M. Albahar, "Cyber attacks and terrorism: A twenty-first century conundrum," *Sci. Eng. Ethics*, vol. 25, no. 4, pp. 993–1006, Aug. 2019.

[5] A. Garg, J. Curtis, and H. Halper, "The financial impact of IT security breaches: What do investors think?" *Inf. Syst. Secur.*, vol. 12, no. 1, pp. 22–33, Mar. 2003.

[6] H. P. Sanghvi and M. S. Dahiya, "Cyber reconnaissance: An alarm before cyber attack," *Int. J. Comput. Appl.*, vol. 63, no. 6, pp. 36–38, Feb. 2013.

[7] V. Adewopo, B. Gonen, and F. Adewopo, "Exploring open source information for cyber threat intelligence," in *Proc. IEEE Int. Conf. Big Data*, Dec. 2020, pp. 2232–2241.

[8] C. Strategic and I. Studies. (2022). *Significant Cyber Incidents in Center for Strategic and International Studies, Significant Cyber Incidents Since 2006*. [Online]. Available: https://www.csis.org/programs/strategictechnologies-program/significant-cyber-incidents

[9] A. Nicholson, T. Watson, P. Norris, A. Duffy, and R. Isbell, "A taxonomy of technical attribution techniques for cyber attacks," in *Proc. Eur. Conf. Inf. Warfare Secur.*, 2012, p. 188.

[10] B. Middleton, *A History of Cyber Security Attacks: 1980 to Present*. Auerbach Publications, 2017.

[11] R. Van Heerden, S. Von Solms, and J. Vorster, "Major security incidents since 2014: An African perspective," in *Proc. IST-Africa Week Conf. (IST-Africa)*, 2018, pp. 1–11.

[12] B. Fonseca and J. D. Rosen, "Cybersecurity in the US: Major trends and challenges," in *The New US Security Agenda*. 2017, pp. 87–106.

[13] C. Strategic and I. Studies. (2022). *About U. S. in Center for Strategic and International Studies, About US* . [Online]. Available: https://www.csis.org/programs/about-us

[14] T. Yadav and A. M. Rao, "Technical aspects of cyber kill chain," in *Proc. Int. Symp. Secur. Comput. Commun.* Cham, Switzerland: Springer, 2015, pp. 438–452.

[15] J. T. Soma, J. Z. Courson, and J. Cadkin, "Corporate privacy trend: The value of personally identifiable information (PII) equals the value of financial assets," *Rich. JL Tech.*, vol. 15, p. 1, Jan. 2008.

[16] B. B. Gupta and O. P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment," *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3655–3682, Dec. 2017.

[17] W. Liu, "Research on DoS attack and detection programming," in *Proc. 3rd Int. Symp. Intell. Inf. Technol. Appl.*, 2009, pp. 207–210.

[18] Z. Chao-yang, "DOS attack analysis and study of new measures to prevent," in *Proc. Int. Conf. Intell. Sci. Inf. Eng.*, Aug. 2011, pp. 426–429.

[19] T. Egharevba, "Phishing attack—A challenge in cybersecurity," Tech. Rep.,.

[20] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers Comput. Sci.*, vol. 3, Mar. 2021, Art. no. 563060.

[21] B. Parmar, "Protecting against spear-phishing," *Comput. Fraud Secur.*, vol. 2012, no. 1, pp. 8–11, Jan. 2012.

[22] A. K. Ghazi-Tehrani and H. N. Pontell, "Phishing evolves: Analyzing the enduring cybercrime," *Victims Offenders*, vol. 16, no. 3, pp. 316–342, Apr. 2021.

[23] J. Seymour and P. Tully, "Generative models for spear phishing posts on social media," 2018, *arXiv:1802.05196*.

[24] S. Kramer and J. C. Bradfield, "A general definition of malware," *J. Comput. Virol.*, vol. 6, no. 2, pp. 105–114, 2010.

[25] I. J. Cruickshank and K. M. Carley, "Analysis of malware communities using multi-modal features," *IEEE Access*, vol. 8, pp. 77435–77448, 2020.

[26] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, "Survey of publicly available reports on advanced persistent threat actors," *Comput. Secur.*, vol. 72, pp. 26–59, Jan. 2018.

[27] E. K. J. Hooi, A. Zainal, M. A. Maarof, and M. N. Kassim, "TAGraph: Knowledge graph of threat actor," in *Proc. Int. Conf. Cybersecurity (ICoCSec)*, Sep. 2019, pp. 76–80.

[28] S. Singh, P. K. Sharma, S. Y. Moon, D. Moon, and J. H. Park, "A comprehensive study on APT attacks and countermeasures for future networks and communications: Challenges and solutions," *J. Supercomput.*, vol. 75, pp. 4543–4574, Aug. 2019.

[29] L. Cheng, F. Liu, and D. D. Yao, "Enterprise data breach: Causes, challenges, prevention, and future directions," *Wiley Interdiscipl. Rev., Data Mining Knowl. Discovery*, vol. 7, no. 5, p. e1211, Sep. 2017.

[30] S. Goode, H. Hoehle, V. Venkatesh, and S. A. Brown, "User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach," *MIS Quarterly*, vol. 41, no. 3, pp. 703–727, Mar. 2017.

[31] M. Raza, M. Iqbal, M. Sharif, and W. Haider, "A survey of password attacks and comparative analysis on methods for secure authentication," *World Appl. Sci. J.*, vol. 19, no. 4, pp. 439–444, 2012.

[32] D. Silver, S. Jana, D. Boneh, E. Chen, and C. Jackson, "Password managers: Attacks and defenses," in *Proc. 23rd USENIX Secur. Symp.*, 2014, pp. 449–464.

[33] V. Adewopo, B. Gonen, N. Elsayed, M. Ozer, and Z. S. Elsayed, "Deep learning algorithm for threat detection in hackers forum (deep web)," 2022, *arXiv:2202.01448*.
[34] P. Patidar and H. Khandelwal, "Zero-day attack detection using machine learning techniques," *Int. J. Res. Anal. Rev.*, vol. 6, no. 1, pp. 1364–1367, 2019.
[35] A. Kumar, "Zero day exploit," Tech. Rep., 2014.
[36] I. Mbona and J. H. P. Eloff, "Detecting zero-day intrusion attacks using semi-supervised machine learning approaches," *IEEE Access*, vol. 10, pp. 69822–69838, 2022.
[37] R. Shu, X. Gu, and W. Enck, "A study of security vulnerabilities on Docker hub," in *Proc. 7th ACM Conf. Data Appl. Secur. Privacy*, Mar. 2017, pp. 269–280.
[38] B. L. Bullough, A. K. Yanchenko, C. L. Smith, and J. R. Zipkin, "Predicting exploitation of disclosed software vulnerabilities using open-source data," in *Proc. 3rd ACM Int. Workshop Secur. Privacy Anal.*, Mar. 2017, pp. 45–53.
[39] R. Bojanc and B. Jerman-Blažic, "An economic modelling approach to information security risk management," *Int. J. Inf. Manag.*, vol. 28, no. 5, pp. 413–422, Oct. 2008.
[40] C. Ioannidis, D. Pym, and J. Williams, "Information security trade-offs and optimal patching policies," *Eur. J. Oper. Res.*, vol. 216, no. 2, pp. 434–444, Jan. 2012.
[41] E. U. Opara and O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *Int. J. Electron. Inf. Eng.*, vol. 3, no. 1, pp. 10–18, 2015.
[42] V. Susukailo, I. Opirskyy, and S. Vasylyshyn, "Analysis of the attack vectors used by threat actors during the pandemic," in *Proc. IEEE 15th Int. Conf. Comput. Sci. Inf. Technol. (CSIT)*, Sep. 2020, pp. 261–264.
[43] S. Popoola, X. Zhao, and J. Gray, "Evolution of bad smells in LabVIEW graphical models," *J. Object Technol.*, vol. 20, no. 1, pp. 1–15, 2021.
[44] C. Wheelus and X. Zhu, "IoT network security: Threats, risks, and a data-driven defense framework," *IoT*, vol. 1, no. 2, pp. 259–285, Oct. 2020.
[45] S. M. A. A. Abir, S. N. Islam, A. Anwar, A. N. Mahmood, and A. M. T. Oo, "Building resilience against COVID-19 pandemic using artificial intelligence, machine learning, and IoT: A survey of recent progress," *IoT*, vol. 1, no. 2, pp. 506–528, Dec. 2020.
[46] G. D. L. T. Parra, P. Rad, K.-K.-R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *J. Netw. Comput. Appl.*, vol. 163, Aug. 2020, Art. no. 102662.
[47] W. Baker, M. Goudie, A. Hutton, C. D. Hylender, J. Niemantsverdriet, C. Novak, D. Ostertag, C. Porter, M. Rosen, and B. Sartin. (2011). *2011 Data Breach Investigations Report*. [Online]. Available: www.verizonbusiness.com/resources/reports/rp_databreach-investigationsreport-2011_en_xg.pdf
[48] V. R. Team, "2015 data breach investigations report," Tech. Rep., 2015.
[49] M. Jartelius, "The 2020 data breach investigations report—A CSO's perspective," *Netw. Secur.*, vol. 2020, no. 7, pp. 9–12, Jul. 2020.
[50] R. Bruggemann, P. Koppatz, M. Scholl, and R. Schuktomow, "Global cybersecurity index (GCI) and the role of its 5 pillars," *Social Indicators Res.*, vol. 159, no. 1, pp. 125–143, Jan. 2022.
[51] K. Farahbod, C. Shayo, and J. Varzandeh, "Cybersecurity indices and cybercrime annual loss and economic impacts," *J. Bus. Behav. Sci.*, vol. 32, no. 1, pp. 63–71, 2020.
[52] W. Burke, T. Oseni, A. Jolfaei, and I. Gondal, "Cybersecurity indexes for eHealth," in *Proc. Australas. Comput. Sci. Week Multiconf.*, Jan. 2019, pp. 1–8.
[53] C. Strategic and I. Studies. (2022). *Regions in Center for Strategic and International Studies*. [Online]. Available: https://www.csis.org/regions
[54] R. R. Brooks, L. Yu, I. Ozcelik, J. Oakley, and N. Tusing, "Distributed denial of service (DDoS): a history," *IEEE Ann. Hist. Comput.*, vol. 44, no. 2, pp. 44–54, Jan./Jun. 2022.
[55] L. Bilge and T. Dumitras, "Before we knew it: An empirical study of zero-day attacks in the real world," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, 2012, pp. 833–844.
[56] A. Acar, L. Lu, A. S. Uluagac, and E. Kirda, "An analysis of malware trends in enterprise networks," in *Proc. Int. Conf. Inf. Secur.* Cham, Switzerland: Springer, 2019, pp. 360–380.
[57] L. E. Branch, W. S. Eller, T. K. Bias, M. A. McCawley, D. J. Myers, B. J. Gerber, and J. R. Bassler, "Trends in malware attacks against United States healthcare organizations, 2016–2017," *Global Biosecurity*, vol. 1, no. 1, p. 15, Feb. 2019.
[58] S. Wankhede and D. Kshirsagar, "DoS attack detection using machine learning and neural network," in *Proc. 4th Int. Conf. Comput. Commun. Control Autom. (ICCUBEA)*, Aug. 2018, pp. 1–5.
[59] J. Jacobs, S. Romanosky, I. Adjerid, and W. Baker, "Improving vulnerability remediation through better exploit prediction," *J. Cybersecurity*, vol. 6, no. 1, Jan. 2020, Art. no. tyaa015.
[60] A. Arora, R. Krishnan, A. Nandkumar, R. Telang, and Y. Yang, "Impact of vulnerability disclosure and patch availability-an empirical analysis," in *Proc. 3rd Workshop Econ. Inf. Secur.*, vol. 24, 2004, pp. 1268–1287.
[61] K. Masuch, M. Greve, and S. Trang, "What to do after a data breach? Examining apology and compensation as response strategies for health service providers," *Electron. Markets*, vol. 31, no. 4, pp. 829–848, Dec. 2021.
[62] M. Greve, K. Masuch, S. Hengstler, and S. Trang, "Overcoming digital challenges: A cross-cultural experimental investigation of recovering from data breaches," in *Proc. ICIS*, 2020, pp. 1–17.
[63] A. Naseer, H. Naseer, A. Ahmad, S. B. Maynard, and A. M. Siddiqui, "Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis," *Int. J. Inf. Manag.*, vol. 59, Aug. 2021, Art. no. 102334.
[64] S. Bradshaw, "Combating cyber threats: CSIRTs and fostering international cooperation on cybersecurity," *SSRN Electron. J.*, vol. 23, Dec. 2015.
[65] C. Onwubiko and K. Ouazzane, "SOTER: A playbook for cybersecurity incident management," *IEEE Trans. Eng. Manag.*, vol. 69, no. 6, pp. 3771–3791, Dec. 2022.
[66] M. Malatji, A. L. Marnewick, and S. Von Solms, "Cybersecurity policy and the legislative context of the water and wastewater sector in south Africa," *Sustainability*, vol. 13, no. 1, p. 291, Dec. 2020.
[67] J. Steinke, B. Bolunmez, L. Fletcher, V. Wang, A. J. Tomassetti, K. M. Repchick, S. J. Zaccaro, R. S. Dalal, and L. E. Tetrick, "Improving cybersecurity incident response team effectiveness using teams-based research," *IEEE Secur. Privacy*, vol. 13, no. 4, pp. 20–29, Jul. 2015.
[68] T. Takahashi, H. Fujiwara, and Y. Kadobayashi, "Building ontology of cybersecurity operational information," in *Proc. 6th Annu. Workshop Cyber Secur. Inf. Intell. Res. (CSIIRW)*, 2010, pp. 1–4.
[69] F. E. Catota, M. G. Morgan, and D. C. Sicker, "Cybersecurity incident response capabilities in the ecuadorian financial sector," *J. Cybersecurity*, vol. 4, no. 1, Jan. 2018, Art. no. tyy002.
[70] E. Kweon, H. Lee, S. Chai, and K. Yoo, "The utility of information security training and education on cybersecurity incidents: An empirical evidence," *Inf. Syst. Frontiers*, vol. 23, no. 2, pp. 361–373, Apr. 2021.
[71] G. N. Angafor, I. Yevseyeva, and Y. He, "Game-based learning: A review of tabletop exercises for cybersecurity incident response training," *Secur. Privacy*, vol. 3, no. 6, p. e126, Nov. 2020.
[72] A. Ahmad, S. B. Maynard, and G. Shanks, "A case analysis of information systems and security incident responses," *Int. J. Inf. Manag.*, vol. 35, no. 6, pp. 717–723, Dec. 2015.
[73] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, "Incident response teams—Challenges in supporting the organisational security function," *Comput. Secur.*, vol. 31, no. 5, pp. 643–652, Jul. 2012.
[74] C. Hove, M. Tarnes, M. B. Line, and K. Bernsmed, "Information security incident management: Identified practice in large organizations," in *Proc. 8th Int. Conf. IT Secur. Incident Manag. IT Forensics*, May 2014, pp. 27–46.
[75] N. Sun, J. Zhang, P. Rimba, S. Gao, Y. Xiang, and L. Y. Zhang, "Data-driven cybersecurity incident prediction: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1744–1772, 2nd Quart., 2018.
[76] J. Uramova, P. Segec, J. Papan, and I. Bridova, "Management of cybersecurity incidents in virtual lab," in *Proc. 18th Int. Conf. Emerg. eLearning Technol. Appl. (ICETA)*, Nov. 2020, pp. 724–729.
[77] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," *NIST Special Publication*, vol. 800, no. 61, pp. 1–147, 2012.
[78] N. Miloslavskaya, "Security operations centers for information security incident management," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2016, pp. 131–136.
[79] R. Ruefle, A. Dorofee, D. Mundie, A. D. Householder, M. Murray, and S. J. Perl, "Computer security incident response team development and evolution," *IEEE Security Privacy*, vol. 12, no. 5, pp. 16–26, Sep. 2014.
[80] P. H. Meland, I. A. Tondel, and B. Solhaug, "Mitigating risk with cyberinsurance," *IEEE Secur. Privacy*, vol. 13, no. 6, pp. 38–43, Nov. 2015.
[81] P. Shedden, A. Ahmad, and A. Ruighaver, "Organisational learning and incident response: Promoting effective learning through the incident response process," Tech. Rep., 2010.

[82] R. Andrade, J. Torres, and S. Cadena, "Cognitive security for incident management process," in *Proc. Int. Conf. Inf. Technol. Syst.* Cham, Switzerland: Springer, 2019, pp. 612–621.
[83] J. Chen and J. Sun, "Understanding the Chinese data security law," *Int. Cybersecurity Law Rev.*, vol. 2, no. 2, pp. 209–221, Dec. 2021.
[84] D. Setiawati, H. A. Hakim, and F. A. H. Yoga, "Optimizing personal data protection in indonesia: Lesson learned from China, South Korea, and Singapore," *Indonesian Comparative Law Rev.*, vol. 2, no. 2, pp. 95–109, 2020.
[85] C. J. Hoofnagle, B. Van Der Sloot, and F. Z. Borgesius, "The European union general data protection regulation: What it is and what it means," *Inf. Commun. Technol. Law*, vol. 28, no. 1, pp. 65–98, Jan. 2019.
[86] M. Cornock, "General data protection regulation (GDPR) and implications for research," *Maturitas*, vol. 111, pp. 1–2, May 2018.
[87] Privacy Commissioner of Canada and Denham, *Report of Findings Into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) Against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*. Office of the Privacy Commissioner of Canada, Ottawa, QC, Canada, 2009.
[88] P. S. Chauhan and N. Kshetri, "2021 state of the practice in data privacy and security," *Computer*, vol. 54, no. 8, pp. 125–132, Aug. 2021.
[89] C. Schmit, B. Larson, and H.-C. Kum, "Data privacy in the time of plague," *Yale J. Health Policy, Law, Ethics*, vol. 21, no. 1, pp. 152–227, 2022.
[90] E. Goldman, "An introduction to the California consumer privacy act (CCPA)," Santa Clara Univ. Legal Studies Research Paper, Tech. Rep., 2020.
[91] R. Mukhi, A. M. Shults, and J. I. Nkodo, "Banking regulators approve final rule establishing cyber incident notification requirements," Tech. Rep.,.
[92] A. R. Bruce, "Cyber security during international conflict," Tech. Rep., 2022.
[93] C. Anyanwu, "Challenges to privacy law in the age of social media: An Australian perspective," *Austral. J. Commun.*, vol. 40, no. 3, pp. 121–137, 2013.
[94] J. K. Gurney, "The impact of the COVID-19 pandemic on cancer diagnosis and service access in new Zealand—A country pursuing COVID-19 elimination," *Lancet Regional Health-Western Pacific*, vol. 10, Jan. 2021, Art. no. 100127.
[95] F. A. Dos Santos, "A lei geral de proteção de dados pessoais (LGPD) e a exposição de dados sensíveis nas relações de trabalho," *Revista do Tribunal Regional do Trabalho da Região*, vol. 24, no. 2, pp. 145–151, 2020.
[96] B. Headd and B. Kirchhoff, "The growth, decline and survival of small businesses: An exploratory study of life cycles," *J. Small Bus. Manag.*, vol. 47, no. 4, pp. 531–550, Oct. 2009.
[97] E. Bartelsman, S. Scarpetta, and F. Schivardi, "Comparative analysis of firm demographics and survival: Evidence from micro-level sources in OECD countries," *Ind. Corporate Change*, vol. 14, no. 3, pp. 365–391, Jun. 2005.
[98] M. A. Carree and A. R. Thurik, "The lag structure of the impact of business ownership on economic performance in OECD countries," *Small Bus. Econ.*, vol. 30, no. 1, pp. 101–110, Nov. 2007.

OLUFUNSHO I. FALOWO (Member, IEEE) received the B.A. degree in philosophy from the University of Lagos, Nigeria, in 2004, and the M.B.A. degree from the Isenberg School of Management, University of Massachusetts, in 2021. He is currently pursuing the Ph.D. degree in information technology with the School of Information Technology, University of Cincinnati, OH. He has been a Certified Information Systems Security Professional, since 2017, a Certified Information Security Manager, since 2020, a Certified Computer Hacking Forensic Investigator, since 2011, and a Certified Security Analyst, since 2010. His research interests include cloud security, security information and event management, security incident detection and response, ethical computer hacking, and digital forensic investigation among others. He is also a member of the International Information System Security Certification Consortium and a member of the Information Systems Audit and Control Association.

SAHEED POPOOLA is currently an Assistant Professor with the School of Information Technology, University of Cincinnati. His research interest includes the area of software engineering. For more information visit the link (http://sopopoola.github.io).

JOSETTE RIEP is currently pursuing the Ph.D. degree in information technology with the School of Information Technology, University of Cincinnati. She is also the Executive Director for Development in Information Technology at the University of Cincinnati, Innovations & Partnerships. She has worked in the field of software development for over 20 years. Her current research interests include leadership over custom development initiatives spanning education, research, patient care and administration, equity and inclusion sponsorship activities, customer relationship management, budget planning and resource allocation, project planning, establishment of methods to share lessons learned, and implementation of best practices among developers with an emphasis on creating and sustaining secure platforms for broad use.

VICTOR A. ADEWOPO received the Associate degree in health informatics from Lagos University Teaching Hospital, Lagos, Nigeria, in 2017, the B.Sc. degree in computer science from Lead City University, Nigeria, in 2019, and the M.S. degree in information technology from the University of Cincinnati, OH, USA, in 2021, where he is currently pursuing the Ph.D. degree in information technology. From 2019 to 2022, he was a Research Assistant with the Applied Machine learning Laboratory, School of Information Technology, University of Cincinnati. His research interests include action recognition (AR), mainly on activity detection and incident prediction based on video streams. He currently works as a Data Scientist at the Great American Insurance Group, Cincinnati. His awards and honors include the Data Science Fellowship (Lawrence Berkeley National Laboratory), the Google Generation Scholarship, and Research Fellowship Award (Graduate Student Government—University of Cincinnati).

JACOB KOCH (Member, IEEE) received the master's degree in computer information technology (CIT) from Northern Kentucky University, in May 2022. He is currently pursuing the Ph.D. degree (full-time) in the information technology program with the University of Cincinnati. He also serves as a Teaching Assistant with the College of Education, Criminal Justice, and Human Services (CECH), and a Research Assistant at the Smart Synergies Laboratory at Digital Futures. His research interests include cloud computing, virtualization, and cyber security. From which, several papers have been published including "Practical Applications of Edge Computing to Accelerate Cloud Hosted Web Content," which won an award for best presentation at the 2022 IEEE World AI IoT Congress (AIIoT).