6-1-2023

A System Dynamics Approach to Evaluate Advanced Persistent Threat Vectors

Mathew Nicho
Rabdan Academy, UAE

Christopher D. McDermott
Robert Gordon University

Hussein Fakhry
Zayed University, hussein.fakhry@zu.ac.ae

Shini Girija
Zayed University

Recommended Citation
Nicho, Mathew; McDermott, Christopher D.; Fakhry, Hussein; and Girija, Shini, "A System Dynamics Approach to Evaluate Advanced Persistent Threat Vectors" (2023). *All Works*. 5906.
https://zuscholars.zu.ac.ae/works/5906

A System Dynamics Approach to Evaluate Advanced Persistent Threat Vectors

Mathew Nicho, Rabdan Academy, UAE

Christopher D. McDermott, Robert Gordon University, UK

Hussein Fakhry, Zayed University, UAE

Shini Girija, Zayed University, UAE*

https://orcid.org/0000-0002-0984-5769

ABSTRACT

Cyber-attacks targeting high-profile entities are focused, persistent, and employ common vectors with varying levels of sophistication to exploit social-technical vulnerabilities. Advanced persistent threats (APTs) deploy zero-day malware against such targets to gain entry through multiple security layers, exploiting the dynamic interplay of vulnerabilities in the target network. System dynamics (SD) offers an alternative approach to analyze non-linear, complex, and dynamic social-technical systems. This research applied SD to three high-profile APT attacks - Equifax, Carphone, and Zomato - to identify and simulate socio-technical variables leading to breaches. By modeling APTs using SD, managers can evaluate threats, predict attacks, and reduce damage by mitigating specific socio-technical cues. This study provides valuable insights into the dynamics of cyber threats, making it the first to apply SD to APTs.

KEYWORDS

Advanced Persistent Threats, Cyberattacks, Cyberthreats, Data breach, Systems dynamics

1. INTRODUCTION

Cyberattacks on high-profile targets leverage a combination of user, technical, and organizational vulnerabilities to gain illegal entry into the system. Hence, preventing them at the security perimeter and detecting them once they enter the system is a challenge and a growing threat worldwide. Their prevention and mitigation require adopting a holistic approach to information system (IS) security management that addresses both hard and soft factors (Özbayrak et al., 2007; Trček, 2006) in IS. Cyberattacks that take the form of advanced persistent threats (APTs) are dynamic threats that necessitate dynamic defenses (Huang & Zhu, 2018). Subsequently, a dynamic mechanism (namely, one in which entities interact with one another) describes how target objects affect each other in a specific field, much like the APT vector targets an organization's network (Xu et al., 2022).

DOI: 10.4018/IJISP.324064

*Corresponding Author

Integrating IS research with system dynamics (SD) involves studying the design, implementation, management, and effects of IS on people, organizations, and markets (Georgantzas & Katsamakas, 2008). SD is an approach to computer-based systems used to understand and model the behavior of transient systems in which the sociotechnical variables are dynamic. Specifically, SD aims to uncover the effects of multiple sociotechnical variables that act at various critical points in a system and to provide the decision-maker with "what if" questions concerning probable transitory system behaviors, boosting understanding of the causes of previously unexpected behavioral patterns. Real-world dynamic systems are characterized by interdependence, mutual interaction, information feedback, and circular causality (Martinez-Moyano et al., 2008) that can be simulated to visualize APT attack scenarios. Accordingly, simulations are used to model the dynamics of threats to analyze the behavior of complex systems over time (Hunker & Probst, 2011). A comprehensive APT threat mitigation strategy must consider user vulnerabilities, technical vulnerabilities, and organizational factors to provide a holistic view of the dynamics of APT attack scenarios.

APT attacks involve exploiting multiple systems and the use of advanced penetration tools or methods. Additionally, they are persistent in penetration, move stealthily within the environment, can stay unnoticed, escalate the privileges (i.e., unauthorized access) at each level (Alshamrani et al., 2019), exploit multiple vulnerabilities (Zhu & Rass, 2018), deploy remotely controlled infected machines, exfiltrate data (Zimba et al., 2020), and normally target the internetworked computer user at the workplace (Nicho & McDermott, 2019). With 95% of cybersecurity breaches being caused by human error (Forum, 2022), an SD approach can unravel the interaction of sociotechnical variables leading to the breach, as APT vulnerabilities are a major issue for managers in information security due to the combination of technical and nontechnical factors (Nicho & Khan, 2018).

IS security is a major concern for businesses that depend on information technology, as it is not easy to identify the dynamic increase in sociotechnical variables leading to cybersecurity breaches. Hence, it is necessary to learn how to spot cyberthreats using innovative methods such as SD, which helps identify, understand, and analyze the interaction of multiple dynamic variables and create 'what if' scenarios in the information security domain. APT attacks have a high likelihood of success due to the deployment of innovative sociotechnical variables, leading to a potentially higher impact on the organizational networks. The authors thus investigated previous research on SD and APTs to assist managers in framing security policies that minimize the risk of security failures. The authors then used SD to select and analyze three cases of reported breach incidents and extract the relevant sociotechnical variables that play a major role in determining the security level of organizational networks.

The paper is structured as follows: First, the authors explain the dynamics of APTs followed by the application of SD to ISs. Then, in the methodology section, the authors illustrate the three simulation case studies. Next, the authors analyze the model simulation and discuss the results in the following section. The authors conclude the paper by suggesting future research steps to study and model the problem in the context of business.

2. RELATED WORKS

2.1 Advanced Persistent Threats (APT)

APT attacks (as opposed to normal/conventional cyberattacks) target IS systems and gradually collect critical information using social engineering, zero-day vulnerabilities, and related approaches (Ahn et al., 2014). The sophistication, persistence, and strategic goals of APTs distinguish them from more common cyberattacks (Alert, 2020). The key characteristics of APT are explained below:

1. **Social engineering**: Social engineering is the technique of persuading individuals to take certain activities or reveal sensitive information, frequently by taking advantage of their feelings, trust, or

ignorance. In a typical attack, however, this usually happens only once, and it lacks the persistence and depth of planning that distinguish APT attacks (Ahn et al., 2014).

2. **Zero-day vulnerabilities**: Zero-day vulnerabilities are vulnerabilities in software that have not yet been patched and are unknown to the vendor. Attackers may take use of these vulnerabilities to break into systems, steal information, or engage in other malicious activities. When compared to normal attacks, APT attackers are more likely to devote a large amount of effort to finding and exploiting these vulnerabilities (Alert, 2020).
3. **High profile targets and well-determined goals**: Advanced Persistent Threats (APTs) focus on specific high-profile targets with valuable intellectual property. Unlike cyberattacks with a broad impact, APTs target specific targets and remain undiscovered while searching for assets like trade secrets, intellectual property, or data related to national security for tactical advantage. In contrast, conventional attacks primarily target personal information or generically valuable data that can be used for financial gain, such as credit card information (Chen et al., 2014).
4. **Co-ordinated and professional**: APTs, often conducted by coordinated professional teams, may be linked to government or military cyber units or contracted as cyber mercenaries by governments and private firms. APT actors have access to substantial financial and technical resources, which enables them to carry out attacks for an extended period of time using zero-day malware and potent attack tools (Khalid et al., 2023).
5. **Persistent attacks**: APT malware stay undetected for extended periods of time in the compromised system, infiltrating extended networks through persistence and stealth. In contrast, conventional cyber threats are non-specific and move on quickly to another target if their initial attempt is unsuccessful (Mohamed, 2022).
6. **Stealthy techniques**: The stealth and evasive nature of APT malware allows them to remain undetected as they use minimal noise or emulate benign calls to achieve their objectives to avoid detection. They achieve this using zero-day exploits to bypass conventional intrusion detection systems. This approach is different from conventional cyberattacks, which often rely on more visible and aggressive tactics likely to generate alerts (Kumari & Prasad, 2021).
7. **Multiphase operations**: Unlike in a conventional one cyber-attack, APT follows a multiphase attack process (reconnaissance, initial breach, privilege escalation, and data exfiltration), deploying novel strategies at each phase that go unnoticed for extended periods of time, while conventional cyber threats are frequently opportunistic and short term (Mohamed, 2022). This gives attackers the opportunity to obtain confidential data, seize control of the targeted system, and spread laterally to other areas of the network (Abu Talib et al., 2022).
8. **Data driven**: The goal of APT attacks is often to steal sensitive data, such as intellectual property, financial information, and personally identifiable information, to conduct business espionage or disrupt operations, while conventional cyberattacks focus on financial gain. Conventional cyberattacks, unlike APTs, rarely inflict considerable harm to the systems or data they target (Hejase et al., 2020).
9. **Risk tolerance**: Conventional cyberattacks frequently take on a significant level of risk by targeting a huge number of possible victims, while APT attackers have a reduced risk tolerance due to the expense and extensive planning that go into an APT attack. APT attackers are more concerned with evasion and thus employ more sophisticated evasion methods. This enables them to avoid detection on a target network for a longer time frame (Maccari et al., 2019).

2.2 Advanced Persistent Threats in Cyberspace

APT attacks are characterized by the exploitation of an optimal mix of sociotechnical vulnerabilities in a target organizational IS network, making them an appropriate attack type for the application of SD. A threat vector is a path or a means by which a malicious hacker gains access to organizational network systems and in which an APT follows multiple paths to reach its goal (i.e., the data). APTs are attacks in which attackers possess sophisticated levels of expertise and significant resources that are used to achieve their objectives by using multiple attack vectors (Hunker & Probst, 2011). These attacks target large corporations and governments to steal information or compromise ISs (Hejase et al., 2020). APT malware stays embedded within the target systems and extracts information at a slow and undetected pace without bringing down the network. It is a highly advanced networked entity typical of organized groups, in which it conducts hostile cyberattacks against the target network (Vert et al., 2014). Using stealth techniques, APTs can continuously monitor, administrate, and steal specific targets in the long term while staying undetected. Since APTs pursue cyber objectives over an extended period while adapting to defenders' efforts to resist them (Chen et al., 2014), an SD approach is suitable for their analysis. Furthermore, since APTs launch attacks in multiple domains of the target IS network in multiple stages using packets that may look benign, they typically bypass most current intrusion detection systems (Aparicio-Navarro et al., 2018).

2.3 APT Attack Vectors

APT attack vectors that are specific tactics or strategies that attackers use to launch APT attacks (Kumar et al., 2022) include techniques such as spear-phishing, malware distribution, network exploitation, social engineering, backdoors, key loggers, video recording of victim activity, and remote administration tools (Stojanović et al., 2020). Frequently, these vectors are used to form a multiphase attack that enables attackers to gain and keep access to a target network while evading detection. Table 1 provides a list of APT attack with the corresponding definitions.

2.4 Cyberattack System Dynamics (CSD)

The authors' analysis of cyberattacks focusing on APTs and SD reveals the overlap of these two domains. A cyberattack is action taken to undermine the functions of a computer network (Hathaway et al., 2012). A system comprises multiple interacting parts; it can be either open or closed, and its parts can be either independent or a function of the greater system they occupy (Johnson, 2021). SD is a computer-aided strategy and policy design approach that uses simulation modelling for complex systems (Society, 2022).

Table 1. APT attack vectors

APT Vector	Activity	References
Spear-phishing	Email attacks that target specific individuals or a group of people in the organization.	(Al-Hamar et al., 2021; Kim et al., 2019)
Malware distribution	Use of malicious codes (malware) to log into a network or system without authorization.	(Sharma et al., 2023; Wang et al., 2022)
Network exploitation	The act of locating and using a system's or network's vulnerabilities to obtain unauthorized access.	(Jabar & Mahinderjit Singh, 2022; Yaacoub et al., 2022)
Social engineering	Manipulating a user to gain access to critical information in addition to using technology.	(Aldawood & Skinner, 2020; Chetioui et al., 2022)
Backdoors	Using malware to circumvent standard authentication mechanisms to get unauthorized access to a system.	(Alminshid & Omar, 2020; Nie et al., 2019)
Key loggers	Use of efficient surveillance tool to monitor the victim's typing and mouse movements.	(Khilosiya & Makadiya, 2020; Singh et al., 2019)
Video recording of victim activity	Using a computer's add-on hardware (such as integrated cameras or webcams) or software (like video call services) to record videos in order to collect data.	(Ohrimenco et al., 2021; Pranggono & Arabo, 2021)
Remote administration tools	These are used by attackers to access a distant computer, server, or network and connect to it.	(Singh et al., 2019; Stojanović et al., 2020)

2.5 System Dynamics Applications

Developed by Jay Forrester (1989) in the 1950s to help corporate managers model and understand industrial processes, SD is a method to mathematically model and understand complex sociotechnical problems. As SD is applied in policy analysis, modelling, and design in both public and private organizations (Sterman, 2002), the authors demonstrate the use of SD simulation to assist policymakers in designing effective sociotechnical ISs at the workplace to detect cues of APT attacks. SD is grounded in the notion of dynamic complexity, whereby systems are constantly changing, tightly coupled, governed by feedback, nonlinear, history-dependent, self-organizing, counterintuitive, and policy-resistant (Sterman, 2002). The mapping of the dynamic complexity of cyberattacks is illustrated in Table 2 to evidence the link between SD and APT attacks. SD has been used in many studies to model information security management and attacks (Nazareth & Choi, 2015; Yang & Wang, 2011).

SD runs through six phases: systems description, converting description to equations, simulating the model, designing alternative policies and structures, educating and debating, and implementing changes in policies (Forrester, 1994). The authors demonstrate the interaction of sociotechnical variables using the first three phases only, as the latter three focus on education and policy formulation, which are not in the realm of this paper. Hence, the authors first describe the systems by identifying the sociotechnical variables involved in the attack process followed by the development of the equations based on the identified variables. In the third phase, the variables are fed into Vensim software for simulation using a stock and flow diagram.

2.6 Integration of SD in Information Security

SD is relevant to the study of information security in organizational settings as it can supplement either quantitative or qualitative research on information security. SD can simulate the realistic state of variables and their intricate relationships to model the dynamic structure of cybersystems used in real world processes. Similarly, it has been used in project management to deal with unplanned changes (Love et al., 2002). As a seamless integration of multiple variables is required for APTs to successfully infiltrate a system, SD has been deployed to deal with the variables involved in integrating the different parts of supply chain systems (Özbayrak et al., 2007). SD has also been applied in the broader domain of information security management and the focused area of insider threats. The complex nature of IS threats and multiple meticulously integrated variables used by hackers have called for dynamic tools to

Table 2. Mapping of dynamic complexity to cyberattacks

Dynamic Complexity (SD)	Cyberattacks (APT)
Constantly changing	APT vectors constantly change and evolve their advanced techniques and methods to stay undetected (Ussath et al., 2016).
Tightly coupled (systems interact with one another)	The attacker maintains persistent connection to a command-and-control server, normally a domain name system, or DNS (Zhao et al., 2015).
Governed by feedback	Same as above (the infected systems provide constant feedback to the attacker) (Zhao et al., 2015).
Non-linear	Attacks happen at multiple planes (Giura & Wang, 2012).
History-dependent (irreversible)	APT attacks cause more permanent, significant, and irreversible damage (Huang & Zhu, 2018).
Self-organizing	APT attacks are organized, having a sequence of tactical actions with a common purpose (Ahmad et al., 2019).
Counter intuitive(Cause and effect are distant in time and space)	APT attacks remain undetected for months (Rot & Olszewski, 2017); threats in cyberspace are global in nature (Lehto, 2022).
Policy resistant	APT attack vectors bypass security mechanisms (Liu & Chen, 2019).

help decision-makers manage information security with limited resources. Trček (2006) advocated the use of SD via computer simulations due to the nonlinearity of cyberthreats. Behara et al. (2007) used SD to analyze the effect of organizational security investments in the attack stage of the information security life cycle and demonstrated the feasibility and validity of SD through multiple simulations. Kim et al. (2012) used SD to build a map to assist financial institutions in determining the priority of security control areas by analyzing the relationships between the Electronic Financial Transaction Act of Korea (which enhances the security and dependability of electronic financial transactions by establishing legal relationships) and South Korea's risk assessment standards. Nazareth and Choi (2015) demonstrated that the SD model is useful for evaluating alternative security management strategies through an investment and security cost lens, as it provides managers with guidance for security-related decision-making. Dutta and Roy (2008) developed an SD model similar to the authors' of the interaction between technical and behavioral IS security factors. This model captures delays associated with users' perception of security, users' compliance, and the mechanics of risk mitigation achieved by investments in security technology and user training. While assessing the efficacy of multiple defense layers through simulation, Yang et al. (2018) discovered that in order to attain a better level of protection against APTs, a combination of several tactics was required. Yaacoub et al. (2020) used SD to model the development of APT attacks over time by taking into account attacker tactics, network structure, and the efficacy of various security measures. Through multiple simulations, they identified seven crucial intervention points where alterations to security procedures or the adoption of new security measures could increase an organization's resistance to APT attacks (Yaacoub et al., 2020). Gunduz and Das (2020) designed a SD model simulation to examine how APT attacks affect critical infrastructure systems by taking into account attack frequency, system vulnerability, and the efficacy of various security controls. They discovered that a comprehensive defense strategy combining various security controls was required to reduce the risks posed by APTs to critical infrastructure systems (Gunduz & Das, 2020). Malenfant (2021) developed a SD model to evaluate the efficacy of various cyber defenses (intrusion detection and prevention, access control, and security training) against APT attacks in healthcare organizations by considering factors such as frequency and seriousness of attacks, the efficacy of various security controls, and the degree of user knowledge.

2.7 Integration of SD in Insider Threat

The rise of insider threats, namely cybersecurity threats posed by malicious insiders and unintentional errors made by internetworked employees, has called for the use of SD. In particular, Melara et al. (2003) used a stock and flow diagram to illustrate the cyberthreats posed by malicious insiders to an organization. As cyberattacks occur due to sociotechnical security overlook and violations, Martinez-Moyano et al. (2008) demonstrated through an SD simulation that a well-implemented system of formal controls can make a remarkable difference and help evaluate the effect of an attack. To create a generic model, Martinez-Moyano et al. (2008) used multiple insider threat cases to find what variables led to insider threats, aiming to improve organizational security and survivability through the suppression of dynamic triggers. The use of case studies in SD has not only broadened the understanding of the insider threat problem but has also led to identifying possible leverage points for threat mitigation (Greitzer et al., 2008). From a security education and training awareness (SETA) perspective, SD can be used to model and analyze insider threats to create interactive learning environments that assist managers in understanding the variables of the cyberattack problem and assessing insider threats based on simulations of policies and cultural, technical, and procedural factors that analyze the complex interactions within the IS (Cappelli et al., 2007). The SD simulation done by Gupta et al. (2021) to examine the effect of social engineering attacks on insider threats demonstrated that the degree of staff knowledge and training and quality of access control have a significant impact on the effectiveness of insider prevention techniques. Zhang et al. (2022) developed an SD model to assess the relationship between employee job satisfaction and insider danger. The simulations demonstrated the relevance of job satisfaction in reducing the insider threat and the added benefits of investments in employee satisfaction (Zhang et al., 2022).

3. METHODOLOGY

In this study, the authors discuss only the first three steps, namely description, model equations, and simulation, out of the six SD problem-evaluation stages previously indicated (Forrester, 1994). In the description stage, the cyberattack scenario is translated into a description employed in subsequent phases. Case studies, soft operations research (i.e., problem structuring methods and tools within SD), and systems thinking are all viable options for the description (Forrester, 1994). Because of the exploratory nature of this research, the authors chose case studies relevant to the real world and characterized by critical corporate challenges. Case studies are helpful tools for the exploratory phase of a research project, serving as a foundation for creating the formal tools required in surveys and experiments (Rowley, 2002). Case studies foster in-depth investigation that is often necessary for answering how- and why-related questions. For example, the Equinox data breach is an interesting case study that demonstrated how SD can be used to identify and analyze the impact of an APT in terms of variables related to organizational and technical vulnerabilities (Nicho & Fakhry, 2019). In Step 1, the authors selected three data breach models as case studies – the Equinox data breach, the Carphone data breach, and the Zomato data breach – to identify and analyze the effect of insider threats. In Step 2, the authors translated the level and rate equations of an SD model from the system description of the three data breaches. To frame a generic model for data breaches, the authors developed equations, illustrated in the discussion section, to assess the variables associated with technological and organizational vulnerabilities. During the simulation process, the authors identified the factors causing the breaches, entered them into the Vensim software, and simulated the three data breaches through Vensim software to obtain the findings.

4. CASE STUDIES

The authors chose three instances of data breaches, namely the Equinox data breach, the Carphone data breach, and the Zomato data breach, as case studies, with the aim of examining the impact of APT attacks. APT attacks are frequently exceedingly complicated and frequently use specialized malware, cutting-edge technologies, and intricate attack paths. Therefore, knowing the attack methodology, prevention, detection, and mitigation of APT attacks through SD can enhance security. APT strategies and approaches can be investigated in greater detail by choosing case studies that have common similarities with APT characteristics. Table 3 illustrates the alignment of APT characteristics with the selected case studies. All three case studies focused on individual targets with well-determined goals, persistent attacks, stealth techniques, and data-driven operations. Zomato and Carphone had coordinated and well-equipped attackers, while Equifax's attackers' coordination is unknown. Equifax and Carphone had multiphase operations, while Zomato's is unknown. All three data breaches had risk tolerance for the security breach, which means they had accepted the possibility of a security breach and were willing to accept residual risk.

4.1 Equifax Data Breach

Equifax Inc., one of the three largest consumer credit reporting companies in the United States, revealed a data breach in September 2017 that resulted in the exposure of 147 million people's personal data, including names, residential addresses, phone numbers, dates of birth, social security numbers, and license numbers. Although other businesses have experienced larger security breaches in the past, this one is unparalleled due to the sensitivity of the personal data kept by Equifax and the scope of the issue (Ng, 2018).

4.1.1 Root Cause

On March 10, 2017, hackers began the APT attack by searching for servers with Apache Struts vulnerabilities, about which US-CERT had issued a warning just two days before. The hackers

Table 3. APT characteristics were aligned with the selected case studies

APT Characteristics	Equifax	Carphone	Zomato
Social engineering	✓	✓	✓
Zero-day vulnerabilities	x	✓	✓
Individualized targets and well-determined goals	✓	✓	✓
Co-ordinated and well-equipped attackers	x	✓	✓
Persistent attacks	✓	✓	✓
Stealthy techniques	✓	✓	✓
Multiphase operations	✓	✓	x
Data driven	✓	✓	✓
Risk tolerance	✓	✓	✓

exploited this vulnerability and used privilege escalation techniques, and it took them two months to penetrate Equifax's dispute portal, namely the portal in which people could lodge claims. In Equifax's network, the malware sat unnoticed for 76 days, giving hackers free rein to move around and steal data. The report claims that the hackers grabbed the data piecemeal from 51 databases to avoid setting off any alerts (Graceful, 2017). The widely used enterprise platform Apache Struts, which has the CVE-2017-5638 Apache Struts vulnerability (allowing remote command execution), contained the vulnerability that attackers leveraged to gain access to Equifax's system.

4.2 Carphone Data Breach

In 2015, Carphone Warehouse reported a data breach that resulted in the loss and disclosure of private information belonging to 2.4 million consumers. The attack ran from July 21 until August 5, when it was found and stopped by Carphone Warehouse. Investigations revealed that the security breach had unlawfully disclosed over 3 million consumers' and about 1,000 workers' data to unauthorized parties. Along with staff employees' identities, phone numbers, postcodes, and automobile registration information, the theft included consumers' names, residences, dates of birth, marital statuses, and past payment card information (Saleem & Naveed, 2020).

4.2.2 Root Cause

Before breaking into the Carphone Warehouse's networks and collecting the personal data of 2.4 million customers, hackers used junk traffic as a ruse. To keep information security employees too busy to follow-up on alarms that would indicate an invasion early on or to trick them into reducing security controls like firewall limits, cybercriminals used DDoS attacks in conjunction with larger security breaches. The Information Commissioner's office claimed that the Carphone Warehouse had violated the Data Protection Act of 1998 by failing to take appropriate actions to protect data and adopting an insufficient approach to data protection. The data breach happened because the WordPress software, which was not updated and patched against vulnerabilities, allowed cyber attackers to obtain login information (Knight & Nurse, 2020).

4.3 Zomato Data Breach

Over 17 million user records, including hashed passwords and customer email addresses, were stolen after the database of Zomato was breached. While not much damage was caused to the hashes due to salting, the breach exposed multiple vulnerabilities. The organization learned about the incident only after the attacker put the data on sale on a dark web marketplace (Saleem & Naveed, 2020). Furthermore, as the passwords of Zomato's 120 million users had been salted, they had become unintelligible even if the hashes were translated (Appiah et al., 2020). Hence, it was not easy to revert the passwords to plain text because hashing had transformed them into incomprehensible strings of letters.

4.3.1 Root Cause

An outdated version of PHP was exploited by the attacker to target 000webhost. They acquired a database containing the hashed passwords and email addresses of almost 17 million people, which was eventually made public (Bush, 2016). Along with this, the malicious hackers used the account information that had been leaked to access other websites, as they assumed that some users could have repeated their passwords. Password reuse allowed the attacker to access a Zomato employee's GitHub account, analyze the web app's source code repository for Zomato, and find a remote code execution vulnerability. The attacker exploited the vulnerability to gain remote access to Zomato's server (Patel & Kansara, 2018). An exfiltrated database containing the names, identities, emails, and password hashes of 17 million clients was located by the attacker (Saleem & Naveed, 2020).

5. RESULTS

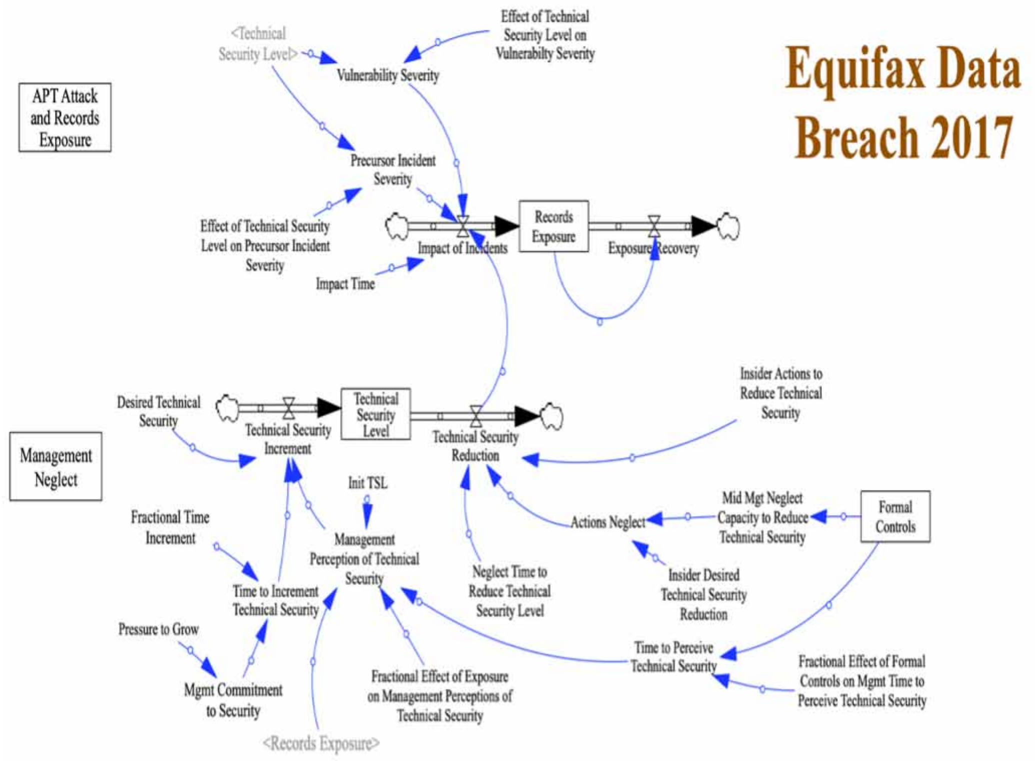
The case studies' analysis reveals that management's failure to promptly respond to threats by implementing the advised software patching, security measures, and appropriate system-wide scanning is a major contributing factor to APT attacks. Two sociotechnical subsystems (i.e., a lower and an upper subsystem) and the VENSIM-PLE program (vensim.com) were used to represent APT attacks with records' exposure and management's neglectful behavior. The upper subsystem displayed the development and effects of APT attacks; the lower subsystem showcased typical management behavior resulting in the implementation of security controls and a high level of technical security. The SD simulated system was further improved to include middle management actions that delayed the implementation of security measures.

5.1 Equifax Data Breach Model

Figure 1 illustrates the SD model of the Equifax data breach. The first subsystem exemplifies the three system variables that directly contributed to the disclosure of the records. The authors introduced a brief apparent loop to model the efforts to stop records exposure, and these variables were further demonstrated using cause-and-effect diagrams that systematically assessed record exposure and technical security. Conversely, the second subsystem modelled management behavior to implement an appropriate level of technical security and middle management actions to reduce the security level, totaling six variables: desired technical security, pressure to grow, management perception of technical security, mid-management actions, formal control reference, and fractional effect of formal control of management time to perceive technical security. The second subsystem consists of a key portion of the simulation model representing the higher management's overarching direction to raise security control levels. Implementation usually takes time due to a company's internal communications and logistics. This endeavour is thwarted by unfavourable actions that lower security control levels, namely middle management's negligence and failure to act promptly. These unfavourable activities caused a security gap that persisted for a long time and gave hackers access to more than 155 million personal records on many servers. The authors identified six socio variables and three technical variables that led to the data breach. The five socio variables include two management variables (middle management's negligence and failure to act promptly over confidence), two user variables (lower security control levels and pressure to grow), and one environment variable (multiple attack vectors). The two technical variables include junk traffic and irregular patching.

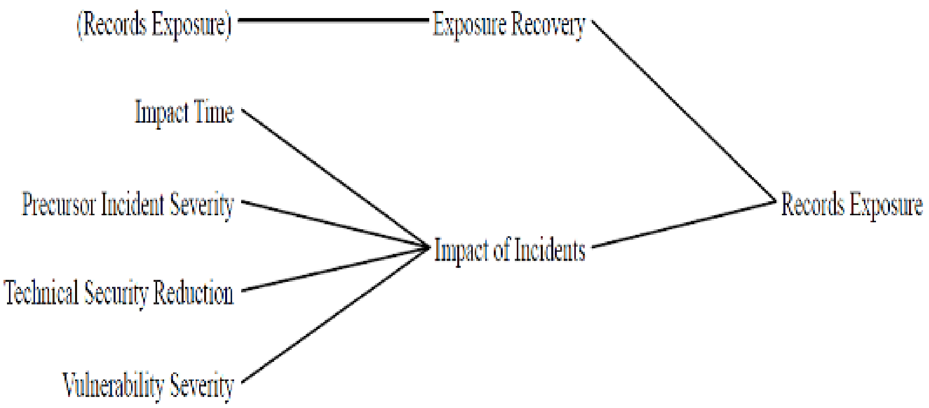
Figure 2 depicts the cause-effect diagram for record exposure. Records exposure is mostly based on the severity of the vulnerability and any prior event, which are steps taken by hackers to further lower the security level that eventually led to the data breach. The intensity or impact of this

Figure 1. System dynamics model of Equifax data breach



Equifax Data Breach 2017
APT Attack and Records Exposure
<Technical Security Level>
Effect of Technical Security Level on Vulnerabilty Severity
Vulnerability Severity
Precursor Incident Severity
Effect of Technical Security Level on Precursor Incident Severity
Impact of Incidents
Records Exposure
Exposure Recovery
Impact Time
Management Neglect
Desired Technical Security
Technical Security Increment
Technical Security Level
Technical Security Reduction
Insider Actions to Reduce Technical Security
Init TSL
Management Perception of Technical Security
Fractional Time Increment
Time to Increment Technical Security
Neglect Time to Reduce Technical Security Level
Actions Neglect
Mid Mgt Neglect Capacity to Reduce Technical Security
Formal Controls
Insider Desired Technical Security Reduction
Pressure to Grow
Mgmt Commitment to Security
Fractional Effect of Exposure on Management Perceptions of Technical Security
Time to Perceive Technical Security
Fractional Effect of Formal Controls on Mgmt Time to Perceive Technical Security
<Records Exposure>

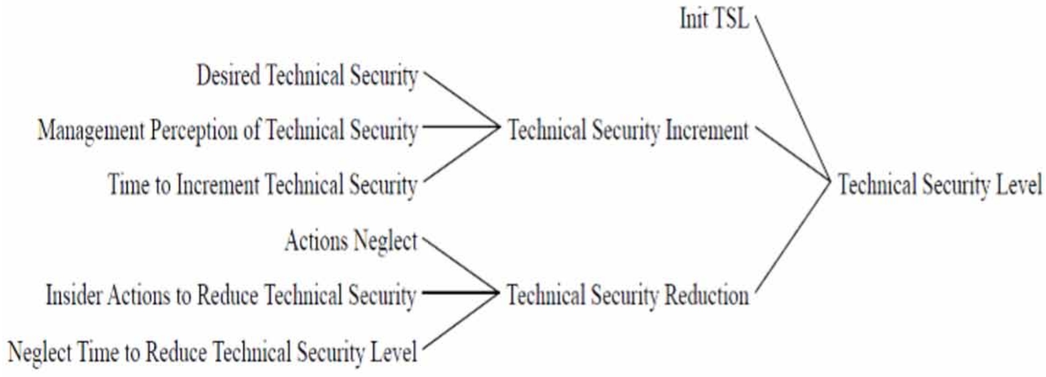
Figure 2. Records exposure cause-effect diagram



occurrence is also impacted by the current security levels. The model had a provision for an impact time constant, which indicated that data exposure and copying would take some time to complete.

Figure 3 depicts the cause-effect diagram for technical security. Management's perspective on technical security, commitment to security, and desired technical security level play a prominent role in implementing technical security, as seen in Figure 3. In general, competition and pressure to expand a business influence management's commitment to security and management may become

Figure 3. Technical security level cause-effect diagram


Init TSL
Desired Technical Security
Management Perception of Technical Security
Time to Increment Technical Security
Technical Security Increment
Technical Security Level
Actions Neglect
Insider Actions to Reduce Technical Security
Neglect Time to Reduce Technical Security Level
Technical Security Reduction

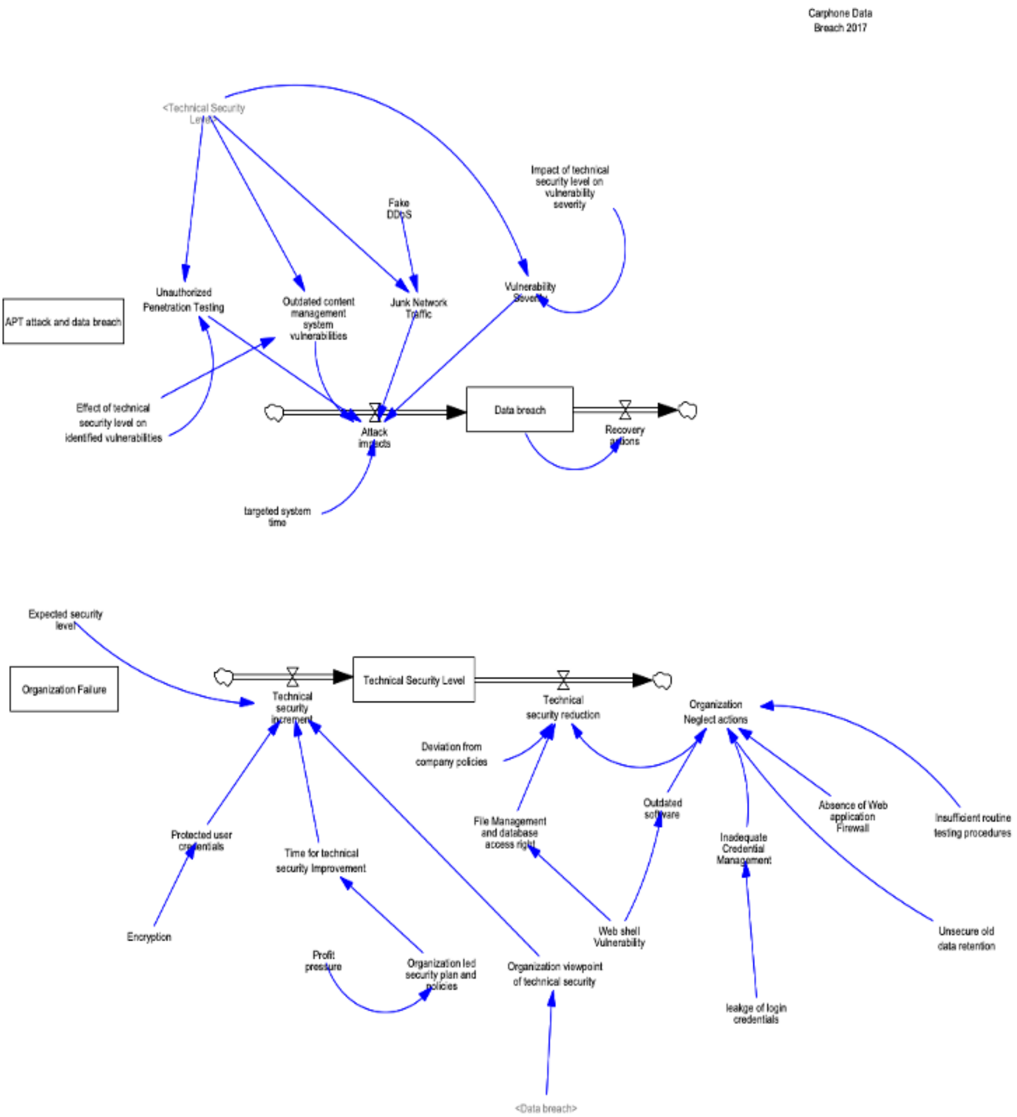
less devoted to security to facilitate faster business expansion. Nonetheless, a business's initial security level and recent history of security breaches can significantly influence management's view of technical security. A time constant representing how long it takes them to realize that they need to improve technological security effectively mitigates this. For example, attackers need only limited time to exploit a newly discovered vulnerability in operating systems (OS), while the OS sector may take time to release the corresponding update or patch. Additionally, it is evident that middle management had taken negative direct (e.g., carelessness) or indirect (e.g.,failure to act) measures.

5.2 Carphone Data Breach Model

Figure 4 illustrates the SD model of the Carphone data breach. The first sub system, as seen in Figure 4, provides an illustration of the three primary APT attack factors – outdated content management system vulnerabilities, unauthorized penetration testing, and ad-hoc network traffic – thus illustrating how they all worked together to cause a data leak. The severity of the vulnerability increases as more fictitious DDoS attacks add to the network load. The installation of an outdated online WordPress application had several vulnerabilities, one of which was an application vulnerability where the attacker uploaded web shells using this outdated software, giving them unrestricted access to the file system and the database exposing client data.

Nonetheless, the second subsystem, as seen in Figure 4, simulated technical vulnerabilities. The vulnerabilities affecting management were a lack of understanding of the need for IT security, overconfidence in security, and a lack of monitoring. Furthermore, managers disregarded strict security regulations, including patch management, penetration testing, and antivirus software updates, as they did not grasp the importance of security. Due to management's overconfidence, old transaction data, including credit card information, was kept on file without a reasonable justification. Despite being encrypted, the decryption keys were stored in plain text in the application's source code, making them easily accessible to hackers. Although the company's security policy called for annual testing, the policy was not followed, as there was insufficient oversight. The commonality of computer user errors as a source of APT assaults had been exposed by numerous breaches. Cybercriminals use DDoS assaults to distract security response staff so that they cannot investigate warnings that might point to an incursion right away or to trick them into lowering security precautions, such as firewall rules. Specifically, this case showed that the company lacked a system for identifying credential abuse. Additionally, a security breach occurred because 30 to 40 personnel had the same root password for several server operating systems. The hacker was also encouraged to penetrate the organizations' system through a number of attack vectors, including junk traffic produced by fake DDoS attacks and, exploitation of out-of-date content management. A vulnerability in the program caused by the absence of a web application firewall

Figure 4. Technical and APT attack vector model for carphone data breach


Carphone Data Breach 2017
<Technical Security Level>
Impact of technical security level on vulnerability severity
Fake DDoS
Unauthorized Penetration Testing
Outdated content management system vulnerabilities
Junk Network Traffic
Vulnerability Severity
APT attack and data breach
Effect of technical security level on identified vulnerabilities
Attack impacts
Data breach
Recovery actions
targeted system time
Expected security level
Organization Failure
Technical security increment
Technical Security Level
Technical security reduction
Organization Neglect actions
Deviation from company policies
Outdated software
File Management and database access right
Absence of Web application Firewall
Insufficient routine testing procedures
Inadequate Credential Management
Protected user credentials
Time for technical security Improvement
Encryption
Web shell Vulnerability
Unsecure old data retention
Profit pressure
Organization led security plan and policies
Organization viewpoint of technical security
leakge of login credentials
<Data breach>

also precluded direct network traffic monitoring and filtering. In addition, bogus DDoS attacks fooled security experts by creating erroneous network traffic to exploit network vulnerabilities.

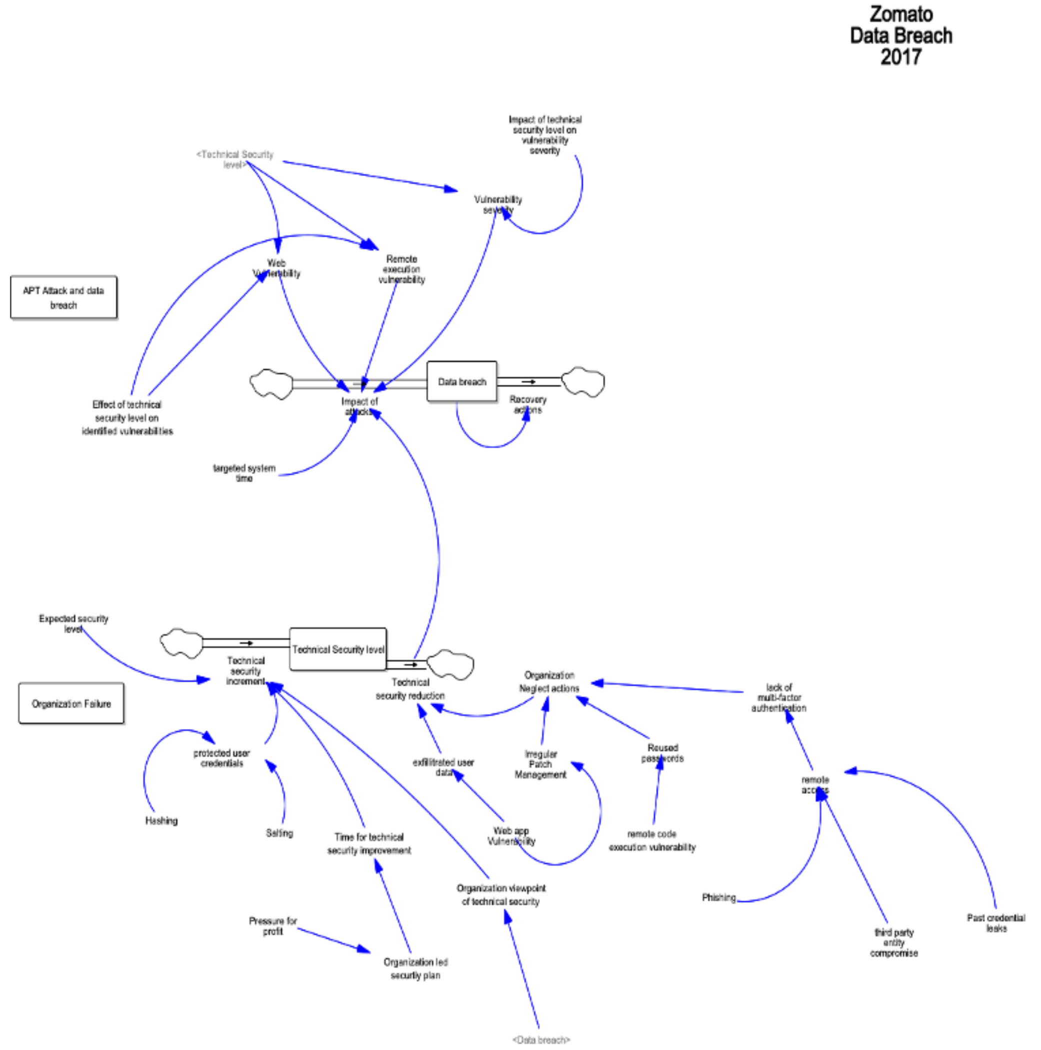
Six social and three technical variables that led to the data breach were identified. The six socio factors are divided into three management variables (overconfidence, lack of monitoring, and deviation from organizational policies), two user variables (weak security controls, poor credential management), and one environmental variable (multiple attack vectors). The three technical variables are junk traffic, irregular patching, and the absence of a firewall.

5.3 Zomato Data Breach Model

Figure 5 illustrates the SD model of the Zomato data breach. The three primary APT attack vectors – web vulnerabilities, third-party entity compromise, and remote execution vulnerabilities – relate to the first subsystem illustrated in Figure 5. Businesses frequently permit both employees and third parties to connect remotely to the company network by utilizing a variety of remote desktop capabilities. These tools support multifactor authentication and require valid credentials for connection. However, due to a lack of multifactor authentication, the attackers can remotely access corporate computers using phishing, third-party entity compromise, and past credential breaches (old data passwords).

The second subsystem, as seen in Figure 5, simulated the technical flaws that led to the Zomato data breach. The main causes of the data leak were improper patch management, reused passwords, and a lack of multifactor authentication. The online hosting service used an outdated version of PHP, which gave attackers access to vulnerable web apps. As demonstrated by the Zomato incident, employees' password reuse can result in severe breaches. Most users frequently use the same passwords for different internet accounts, often with few or no changes. Businesses frequently permit employees and third parties to connect remotely to the company network through various remote desktop capabilities. These tools support multifactor authentication and require valid credentials for connection.

Figure 5. Technical and APT attack vector model for Zomato data breach


Zomato
Data Breach
2017
Impact of technical security level on vulnerability severity
<Technical Security level>
Vulnerability severity
APT Attack and data breach
Web Vulnerability
Remote execution vulnerability
Data breach
Recovery actions
Impact of attacks
Effect of technical security level on identified vulnerabilities
targeted system time
Expected security level
Technical Security level
Technical security increment
Technical security reduction
Organization Failure
Organization Neglect actions
lack of multi-factor authentication
protected user credentials
exfilitrated user data
Irregular Patch Management
Reused passwords
remote access
Hashing
Salting
Time for technical security improvement
Web app Vulnerability
remote code execution vulnerability
Organization viewpoint of technical security
Phishing
Pressure for profit
Organization led securtiy plan
third party entity compromise
Past credential leaks
<Data breach>

Four social and three technical variables that led to the data breach were identified. The four socio factors are divided into two management variables (lack of monitoring and deviation from organizational policies), one user variable (lack of multifactor authentication), and one environmental factor (multiple attack vectors). The three technical variables are phishing, third-party entity compromise, and past credential breaches.

6. DISCUSSION

This section illustrated the equations that the authors developed based on the variables identified in the previous section. In the first phase, the authors transformed the real environment into a description, which the authors employed in later phases. The authors used stock and flow diagrams to illustrate the system. Stocks are entities (e.g., network security) that can rise or fall, whereas flows are things that cause stocks to rise or fall. In the authors' generic model for attack and recovery actions, the stock variable was data breaches, whose increase rate was controlled by the flow variable attack impact, which was decreased by the flow variable recovery actions. Similarly, in a generic model for the organization perspective, the stock variable is the technical security level, whose rate of increase is controlled by the flow variable technical security increment actions, whereas the rate of decrease is controlled by the flow variable technical security decrement actions. The authors used three case studies to address data breaches and provide a preliminary description of attack scenarios.

In Step 2, the authors began formulation of a simulation model. Specifically, the authors translated system description to the level and rate equations of an SD model. Writing equations in Step 2 highlights any errors and omissions in the first description that need to be fixed. In a generic model for data breaches, attack impact and recovery actions determine the rates at which quantity is added to or subtracted from the stock variable data breach. The net flow is the derivative of the total stock relative to time, as shown in Equation 1. Therefore, if a hacker's attack impact can counterfeit existing recovery actions of a system, the chance of data breaches is high:

$$d\left(data\ \ breach\right) / \ dt = attack\ \ impact\left(t\right) - recovery\ \ actions\left(t\right) \tag{1}$$

In a generic model for the organization side, technical security reduction and technical security increment are the rates at which quantity is added to or subtracted from the stock variable technical security level. The net flow is therefore the derivative of the total stock relative to time, as shown in Equation 2. Hence, if there is an upper hand in the technical security measures, the technical security level increases, and the chance of data breaches decreases:

$$d\left(technical\ \ security\ \ level\right) / \ dt = Technical\ \ security\ \ increment\left(t\right) - Technical\ \ security\ \ reduction \tag{2}$$

The simulation of the model could start once the equations from Step 2 met the logical requirements for an operational model, including having all variables defined with none defined more than once, no simultaneous equations, and consistent units of measurement.

When the authors analyzed 22 technical variables for the three data breach models, they found that the four variables that were the root cause of data breaches were irregular patch management, deviation from company security policies, managements' negligence in performing regular testing, and insider actions, as seen in Table 4. Table 4 provides an overview of the overlap of variables across the three cases. From these statistics, the authors simulated a generic SD model that outlines the main reasons causing data breaches from the organization and the technical sides.

The generic model of the attacker side and the anticipated recovery actions is shown in Figure 6. The generic model was created using a combination of existing academic literature, case study

Table 4. List of variables used in system design for representing factors of data breaches

Factors for Data Breach	Equifax Data Breach	Carphone Data Breach	Zomato Data Breach
Profit pressure	✓	✓	
Unauthorized penetration testing		✓	
Irregular patch management	✓	✓	✓
Junk network traffic		✓	
Fake DDoS		✓	
Deviation from company policies	✓	✓	✓
Unauthorized access	✓	✓	
Different web vulnerabilities	✓	✓	
Inadequate credential management		✓	✓
Absence of web application firewall		✓	
Unsecure old data retention			✓
Insufficient routine testing procedure		✓	✓
Remote code execution vulnerabilities			✓
Third party entity compromise			✓
Mid management negligence	✓	✓	✓
Insider actions	✓	✓	✓
Precursor incident severity	✓		
Past credential leakage			✓
Insecure remote access			✓
Lack of multifactor authentication			✓
Reused passwords			✓
Formal control reference	✓		

analysis, and round-robin discussions among the coauthors. The fundamental framework (or main causal loop) of the model is based on dynamic interactions between attack impact and recovery actions, which are influenced and modified by elements like attacker goals and defensive strategies. The two stock variables that have been shown to be important in visualizing the data breach in all three case studies are the attackers' goals and the defensive strategies.

In all case studies, the authors identified the attackers' goals and defensive strategies as the stock variables needed to demonstrate the recovery actions that can prevent future data breaches. The impact of the attacks depended on the attackers' strategies and the severity of various vulnerabilities existing in the system. The attackers' strategies were based on the attack threshold, previous system defense measures, and the timing of launching attacks. The recovery actions were planned based on the defensive strategies existing in the system, which were determined by measures such as testing, threshold defense value, time to defend, and average security loss due to the attack. Table 5 lists the elements influencing the stock variables.

The common vulnerabilities from the organization side are shown in Figure 7. The factors enhancing the network's security were the proper management of users' credentials, the organizations' IS security culture, and annual security policies planned by managers. Due to profit pressure, organizations often fail to follow these policies and to implement annual testing, which offers

Figure 6. General model for attack and recovery actions

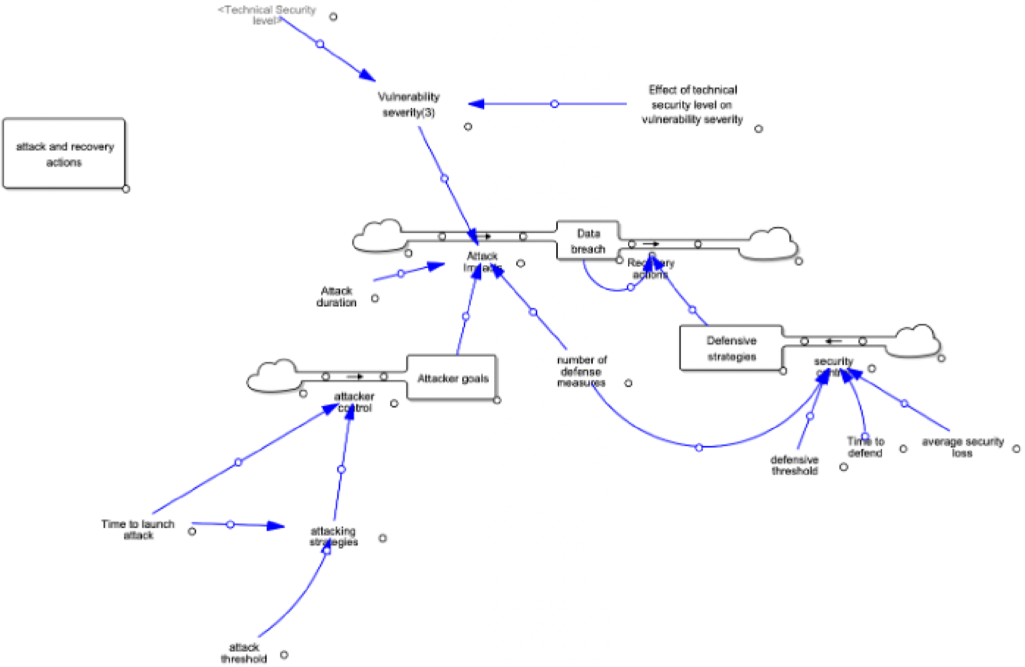


Table 5. Variables for system design of recovery actions

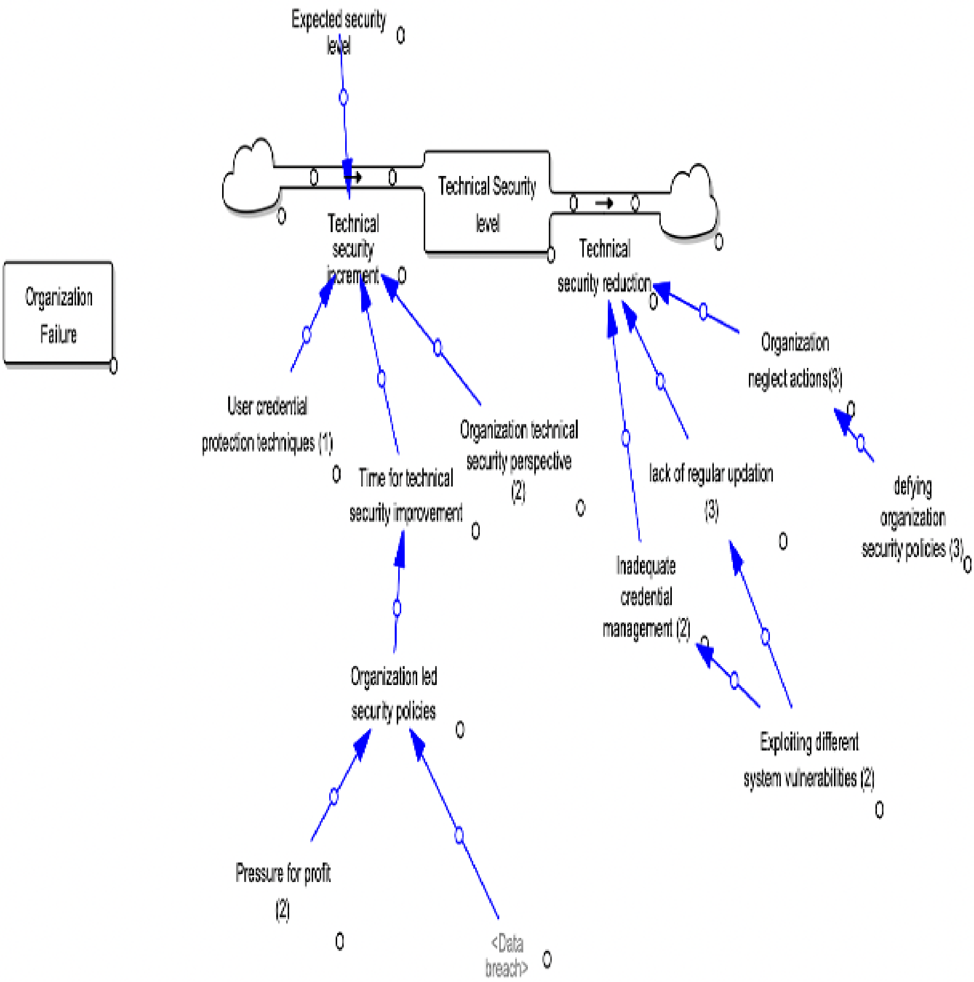
Stock Variables	Factors which lead to increase in stock variables	Factors which lead to decrease in stock variables
Attacker's goal	Time to launch attack, attacking strategies, attack threshold	Number of defense measures, security control
Recovery actions	Defensive threshold, time to defend cyberattacks, average security loss, defensive measures	Attack impact, attack duration, vulnerability severity

attackers the chance to intrude. Additionally, employees' and managers' overconfidence, leading to the irresponsible handling of users' credentials, also leads to data leakage. Insufficient routine testing, irregular patching, and lack of monitoring are the other factors contributing to technical security reduction, which help attackers launch attacks. The number in the brackets represents the occurrence of these variables among the three data breaches that the authors analyzed.

7. CONCLUSION

An attack taking the form of an APT is dynamic, as it involves the interaction between attack and defense variables (i.e., flows) and stock variables (i.e., organizational security). The authors used three cases of data breaches due to APTs to study the dynamics of the variables leading to the breaches and identified 22 variables related to either attackers or hacked organizations. Four variables were common to all three organizations: irregular patching, deviations from the company's policies, middle management negligence, and insider actions. Through this generic model, the authors were able to identify seven variables corresponding to strategies to breach data and 10 variables corresponding

Figure 7. General model for technical security level in an organization


Expected security level
Technical Security level
Technical security increment
Technical security reduction
Organization Failure
User credential protection techniques (1)
Time for technical security improvement
Organization technical security perspective (2)
lack of regular updation (3)
Organization neglect actions(3)
defying organization security policies (3)
Inadequate credential management (2)
Organization led security policies
Exploiting different system vulnerabilities (2)
Pressure for profit (2)
<Data breach>

to the organizations' vulnerabilities in terms of technological security. However, due to the dynamic nature of APT attacks, as the attack vector moves laterally and vertically across organizational networks, independent variables can be dependent, and dependent variables can be independent.

This study is the first to apply SD to APTs. Specifically, the authors modelled cyberattacks using SD using multiple case studies, which has practical implications. First, the authors' simulations can provide managers with insights into the dynamics of the threats and general sociotechnical cues to evaluate cyberthreats and predict cyberattacks. Second, the authors' contribution can allow managers to lessen damages by mitigating or eliminating the specific sociotechnical cues should a cyberattack occur. Third, the authors' model not only provides four generic IS vulnerabilities, namely irregular patching, deviations from the company's policies, middle management negligence, and insider actions, to improve cybersecurity but also provides a visual dashboard to analyze the complex interaction of variables leading to data breaches. Fourth, the authors' model can be used to evaluate the attack and defense effects of both attack vectors and organizational security measures. Managers can formulate policies and effective SETA programs that align with industry standards and regulations based on this model. Finally, a "what if" scenario can be built to understand the effect of the stock and flow diagram on the sociotechnical variables that affect a data breach and evaluate corresponding defensive and recovery initiatives.

The authors' research paves the way for the following research opportunities: First, since the authors used only the three phases of Forrester's (1989) SD process as a theoretical lens, extending the research into the subsequent three phases can highlight recommended and mandatory security policies for controlling the identified flows. Second, as APT attacks are dynamic (as they use multiple attack vectors), future researchers could create a robust generic model by considering all data breaches involving all APT attack vectors. Third, the role of the 'internetworked computer user' being a critical factor in any APT attacks, a convergent focus on this domain is a critical area of research from a behavioral perspective (since 'user' has been defined in the literature as the weakest link).

CONFLICT OF INTEREST

The authors of this publication declare there are no competing interests.

FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. Funding for this research was covered by the authors of the article.

REFERENCES

Abu Talib, M., Nasir, Q., Bou Nassif, A., Mokhamed, T., Ahmed, N., & Mahfood, B. (2022). APT beaconing detection. *Systematic Reviews*.

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, *86*, 402–418. doi:10.1016/j.cose.2019.07.001

Ahn, S.-H., Kim, N.-U., & Chung, T.-M. (2014). Big data analysis system concept for detecting unknown attacks. 16th International Conference on Advanced Communication Technology. ACM.

Al-Hamar, Y., Kolivand, H., Tajdini, M., Saba, T., & Ramachandran, V. (2021). Enterprise credential spear-phishing attack detection. *Computers & Electrical Engineering*, *94*, 107363.

Aldawood, H., & Skinner, G. (2020). An advanced taxonomy for social engineering attacks. *International Journal of Computer Applications*, *177*(30), 1–11. doi:10.5120/ijca2020919744

Alert, C. (2020). *Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations*. CISA.

Alminshid, K. A. A., & Omar, M. N. (2020). A framework of APT detection based on packets analysis and host destination. *Iraqi Journal of Science*, 215-223.

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys and Tutorials*, *21*(2), 1851–1877. doi:10.1109/COMST.2019.2891891

Aparicio-Navarro, F. J., Kyriakopoulos, K. G., Ghafir, I., Lambotharan, S., & Chambers, J. A. (2018). Multi-stage attack detection using contextual information. *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM),* Appiah, G., Amankwah-Amoah, J., & Liu, Y.-L. (2020). Organizational architecture, resilience, and cyberattacks. *IEEE Transactions on Engineering Management*, *69*(5), 2218–2233.

Behara, R., Huang, C. D., & Hu, Q. (2007). *A system dynamics model of information security investments*.

Bush, D. (2016). How data breaches lead to fraud. *Network Security*, *2016*(7), 11–13. doi:10.1016/S1353-4858(16)30069-1

Cappelli, D. M., Desai, A. G., Moore, A. P., Shimeall, T. J., Weaver, E. A., & Willke, B. J. (2007). *Management and education of the risk of insider threat (MERIT): Mitigating the risk of sabotage to employers' information, systems, or networks*. Carnegie Mellon University.

Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal.

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. *Procedia Computer Science*, *198*, 656–661.

Dutta, A., & Roy, R. (2008). Dynamics of organizational information security. *System Dynamics Review*, *24*(3), 349–375. doi:10.1002/sdr.405

Forrester, J. W. (1994). System dynamics, systems thinking, and soft OR. *System Dynamics Review, 10*(2-3), 245-256.

Georgantzas, N. C., & Katsamakas, E. G. (2008). Information systems research with system dynamics. *System Dynamics Review*, *24*(3), 247–264. doi:10.1002/sdr.420

Giura, P., & Wang, W. (2012). A context-based detection framework for advanced persistent threats. *2012 International Conference on Cyber Security*. Graceful Security. https://www.gracefulsecurity.com/equifax-breach-

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. *IEEE Security and Privacy*, *6*(1), 61–64. doi:10.1109/MSP.2008.8

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094. doi:10.1016/j.comnet.2019.107094

Gupta, S., Bhattacharya, A., & Gupta, H. (2021). Analysis of social engineering attack on cryptographic algorithm. *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*. Research Gate.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 817–885.

Hejase, H. J., Fayyad-Kazan, H. F., & Moukadem, I. (2020). Advanced persistent threats (apt): An awareness review. *Journal of Economics and Economic Education Research*, *21*(6), 1–8.

Huang, L., & Zhu, Q. (2018). *Analysis and computation of adaptive defense strategies against advanced persistent threats for cyber-physical systems*. Decision and Game Theory for Security: 9th International Conference, GameSec 2018, Seattle, WA, USA.

Hunker, J., & Probst, C. W. (2011). Insiders and insider threats: An overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, *2*(1), 4–27.

Jabar, T., & Mahinderjit Singh, M. (2022). Exploration of mobile device behavior for mitigating advanced persistent threats (APT): A systematic literature review and conceptual framework. *Sensors (Basel)*, *22*(13), 4662. doi:10.3390/s22134662 PMID:35808159

Johnson, L. (2021). *What is a system?* Student Works.

Khalid, M. N. A., Al-Kadhimi, A. A., & Singh, M. M. (2023). Recent developments in game-theory approaches for the detection and defense against advanced persistent threats (APTs): A systematic review. *Mathematics*, *11*(6), 1353. doi:10.3390/math11061353

Khilosiya, B., & Makadiya, K. (2020). Malware analysis and detection using memory forensic. *Multidiscip. Int. Res. J. Gujarat Technol. Univ*, *2*(2), 106.

Kim, A. C., Lee, S. M., & Lee, D. H. (2012). Compliance risk assessment measures of financial information security using system dynamics. *International Journal of Security and Its Applications*, *6*(4), 191–200.

Kim, M., Dey, S., & Lee, S.-W. (2019). Ontology-driven security requirements recommendation for APT attack. *2019 IEEE 27th international requirements engineering conference workshops (REW),* (pp. 150-156). IEEE.

Knight, R., & Nurse, J. R. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, *99*, 102036. doi:10.1016/j.cose.2020.102036

Kumar, R., Kela, R., Singh, S., & Trujillo-Rasua, R. (2022). APT attacks on industrial control systems: A tale of three incidents. *International Journal of Critical Infrastructure Protection*, *37*, 100521. doi:10.1016/j.ijcip.2022.100521

Kumari, M. A., & Prasad, K. N. (2021). A behavioral study of advanced security attacks in enterprise networks. 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS). IEEE.

Lehto, M. (2022). APT cyber-attack modelling: Building a general model. *International Conference on Cyber Warfare and Security.* IEEE.

Liu, C.-H., & Chen, W.-H. (2019). The study of using big data analysis to detecting APT attack. *Journal of Computers*, *30*(1), 206–222.

Love, P. E., Holt, G. D., Shen, L. Y., Li, H., & Irani, Z. (2002). Using systems dynamics to better understand change and rework in construction project management systems. *International Journal of Project Management*, *20*(6), 425–436. doi:10.1016/S0263-7863(01)00039-4

Maccari, M., Polzonetti, A., & Sagratella, M. (2019). Detection: Definition of new model to reveal advanced persistent threat. *Proceedings of the Future Technologies Conference (FTC) 2018, 2.* Springer. doi:10.1007/978-3-030-02683-7_22

Malenfant, T. (2021). *Impact of ransomware attacks on healthcare Utica College*.

Martinez-Moyano, I. J., Rich, E., Conrad, S., Andersen, D. F., & Stewart, T. R. (2008). A behavioral theory of insider-threat risks: A system dynamics approach. [TOMACS]. *ACM Transactions on Modeling and Computer Simulation*, *18*(2), 1–27. doi:10.1145/1346325.1346328

Melara, C., Sarriegui, J. M., Gonzalez, J. J., Sawicka, A., & Cooke, D. L. (2003). A system dynamics model of an insider attack on an information system. *Proceedings of the 21st International Conference of the System Dynamics Society*. Research Gate.

Mohamed, N. (2022). State-of-the-Art in Chinese APT attack and using threat intelligence for detection: A survey. *Journal of Positive School Psychology*, 4419–4443.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*(1), 123–134. doi:10.1016/j.im.2014.10.009

Ng, A. (2018, September 7). How the Equifax hack happened, and what still needs to be done. *Cnet*.

Nicho, M., & Fakhry, H. (2019). Applying system dynamics to model advanced persistent threats. *Proceedings of the 2019 International Communication Engineering and Cloud Computing Conference.* ACM. doi:10.1145/3380678.3380682

Nicho, M., & Khan, S. N. (2018). A decision matrix model to identify and evaluate APT vulnerabilities at the user plane. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).* ACM.

Nicho, M., & McDermott, C. D. (2019). Dimensions of ‘socio’vulnerabilities of advanced persistent threats. *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM).* ACM.

Nie, D., Yu, H., Lu, X., & Cui, C. (2019). *A method to defense APT based on dynamic ID transformation.* Artificial Intelligence and Security: 5th International Conference, ICAIS 2019, New York, NY, USA.

Ohrimenco, S., Borta, G., & Cernei, V. (2021). Estimation of the key segments of the cyber crime economics. *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T).* IEEE.

Özbayrak, M., Papadopoulou, T. C., & Akgun, M. (2007). Systems dynamics modelling of a manufacturing supply chain system. *Simulation Modelling Practice and Theory*, *15*(10), 1338–1355. doi:10.1016/j.simpat.2007.09.007

Patel, N., & Kansara, K. B. (2018). UBM–UVM approach for preventing insider data theft from cloud storage. *2018 5th International Symposium on Emerging Trends and Technologies in Libraries and Information Services (ETTLIS).* ACM.

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), e247. doi:10.1002/itl2.247

Rot, A., & Olszewski, B. (2017). *Advanced persistent threats attacks in cyberspace. Threats, Vulnerabilities, Methods of Protection. FedCSIS*. Position Papers.

Rowley, J. (2002). Using case studies in research. *Management Research News*, *25*(1), 16–27. doi:10.1108/01409170210782990

Saleem, H., & Naveed, M. (2020). SoK: Anatomy of data breaches. *Proceedings on Privacy Enhancing Technologies. Privacy Enhancing Technologies Symposium*, *2020*(4), 153–174. doi:10.2478/popets-2020-0067

Sharma, A., Gupta, B. B., Singh, A. K., & Saraswat, V. (2023). A novel approach for detection of APT malware using multi-dimensional hybrid Bayesian belief network. *International Journal of Information Security*, *22*(1), 119–135. doi:10.1007/s10207-022-00631-5

Singh, S., Sharma, P. K., Moon, S. Y., Moon, D., & Park, J. H. (2019). A comprehensive study on APT attacks and countermeasures for future networks and communications: Challenges and solutions. *The Journal of Supercomputing*, *75*(8), 4543–4574. doi:10.1007/s11227-016-1850-4

System Dynamics Society. (2022). *What is a systems dynamics*. System Dynamics Society.

Sterman, J. (2002). *System dynamics: Systems thinking and modeling for a complex world*. System Dynamics Society.

Stojanović, B., Hofer-Schmitz, K., & Kleb, U. (2020). APT datasets and attack modeling for automated detection methods: A review. *Computers & Security*, *92*, 101734. doi:10.1016/j.cose.2020.101734

Trček, D. (2006). Using systems dynamics for human resources management in information systems security. *Kybernetes*.

Ussath, M., Jaeger, D., Cheng, F., & Meinel, C. (2016). Advanced persistent threats: Behind the scenes. *2016 Annual Conference on Information Science and Systems (CISS)*. ACM. doi:10.1109/CISS.2016.7460498

Vert, G., Gonen, B., & Brown, J. (2014). A theoretical model for detection of advanced persistent threat in networks and systems using a finite angular state velocity machine (FAST-VM). *International Journal of Computer Science and Application*, *3*(2), 63. doi:10.14355/ijcsa.2014.0302.01

Wang, Q., Yan, H., Zhao, C., Mei, R., Han, Z., & Zhou, Y. (2022). APT attribution for malware based on time series shapelets. *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE. doi:10.1109/TrustCom56396.2022.00108

World Economics Forum. (2022). The global risks report 2022. WEF.

Xu, J., Liu, Z., Wang, S., Zheng, T., Wang, Y., Wang, Y., & Dang, Y. (2022). Foundations and applications of information systems dynamics. *Engineering (Beijing)*. doi:10.1016/j.eng.2022.04.018

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, *21*(1), 1–44. doi:10.1007/s10207-021-00545-8 PMID:33776611

Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, *77*, 103201. doi:10.1016/j.micpro.2020.103201 PMID:32834204

Yang, L.-X., Li, P., Yang, X., & Tang, Y. Y. (2018). A risk management approach to defending against the advanced persistent threat. *IEEE Transactions on Dependable and Secure Computing*, *17*(6), 1163–1172. doi:10.1109/TDSC.2018.2858786

Yang, S.-C., & Wang, Y.-L. (2011). System dynamics based insider threats modeling. *International Journal of Network Security & its Applications*, *3*(3), 1–14. doi:10.5121/ijnsa.2011.3301

Zhang, G., Zhang, X., & Wang, Y. (2022). Perceived insider status and employees' innovative behavior: The role of knowledge sharing and organizational innovation climate. *European Journal of Innovation Management*. doi:10.1108/EJIM-03-2022-0123

Zhao, G., Xu, K., Xu, L., & Wu, B. (2015). Detecting APT malware infections based on malicious DNS and traffic analysis. *IEEE Access : Practical Innovations, Open Solutions*, *3*, 1132–1142. doi:10.1109/ACCESS.2015.2458581

Zhu, Q., & Rass, S. (2018). On multi-phase and multi-stage game-theoretic modeling of advanced persistent threats. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 13958–13971. doi:10.1109/ACCESS.2018.2814481

Zimba, A., Chen, H., Wang, Z., & Chishimba, M. (2020). Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics. *Future Generation Computer Systems*, *106*, 501–517. doi:10.1016/j.future.2020.01.032

Mathew Nicho is currently working as an Associate Professor for Research in Cyber Security at the Research and Innovation Centre, Rabdan Academy (UAE Ministry of Interior). Prior to this he was an Associate Professor at the College of Technological Innovation at Zayed University, Dubai, United Arab Emirates teaching and researching in the information security domain since 2017. He has also taught at the University of Dubai (UAE), and Auckland University of Technology (New Zealand). He obtained his PhD and Masters from Auckland University of Technology, Auckland, New Zealand. His teaching and research are in the socio and technical aspects of cyber-attacks, advanced persistent threats vulnerabilities and mitigation; and IT governance. His research outputs have appeared in journals and conferences namely Communications of the Association of Information Systems, Information and Computer Security, International Journal of Information Security and Privacy, Lecture Notes in Computer Science, and conferences namely Hawaii International Conference on System Sciences, International Conference on Mathematical Methods, Models and Architectures for Computer Network Security), IFIP International Conference on New Technologies, Mobility and Security(to name a few).

Christopher McDermott is a Lecturer in Human-centred security at Robert Gordon University. His research focuses on the human factors of cybersecurity, privacy and trust where he considers questions at the intersection between humans and digital technology. In particular, exploring cyber psychology and behaviour to understand attacks that exploit humans: phishing, social engineering and security perception. He is also a leading advocate for security by design.

Hussein Fakhry is currently an Associate Professor in the College of Technological Innovation at Zayed University, Dubai Campus. He received PhD in Intelligent Control Systems & Roboticsfrom the University of Waterloo, Canada. Since then, he assumed different academic and administrative positions at University of Windsor, Cairo University and University of Dubai. Dr. Fakhry has extensive professional experience and capacity in teaching and training in the areas of Project Planning & Management, Computer Networks Planning & Management, Systems Analysis & Design, Database Design, Data warehousing Analysis & Design, Expert Systems, Decision Support Systems, IS Strategy Planning, Business and IT alignment, Strategic Management Modeling using System Dynamics, Modeling and Simulation of the Supply Chains, and Operations Research Models. Moreover, Dr. Fakhry developed extensive proficiency and expertise in academic programs planning and design, and accreditation standards and documentation following the international ABET standards (USA). Furthermore, Dr. Fakhry's research interests are in Information Systems Research using System Dynamics- Information Systems Security- E-Commerce and E-Business- Decision Support Systems- Applications of Artificial Intelligence- and Assessment of Academic Programs.

Shini Girija is a research assistant at Zayed University. She completed Masters in Engineering in Computer Science from Kerala University in India.Her focus as a research assistant includes using different machine learning methods on IoT devices, using blockchain in Intrusion Detection System in Industrial IOT devices, identifying vulnerabilities in Advanced Persistent Threats, Emotion Recognition methods, and aligning cyber security curriculum with the industry. She taught graduate and undergraduate students in universities on subjects namely Computer programming in Java and C#, Computer Networks, High Performance Microprocessors, Algorithm Design and Multimedia design, Internet of things, Security in Computing. She has expertise in machine learning especially deep learning methods coding platforms such as TensorFlow and Pytorch. She also has adequate knowledge of advanced computer programs namely C#, python, Java, HTML, MySQL, PHP and Azure cloud deployment. Her teaching philosophy takes the experiential learning approach of Kolb and Gibbs which she used extensively for facilitating rather than teaching. Her teaching methodologies include tutorials, projects, workshops, demonstrations, and discussion.