THE ROLE OF MANAGEMENT DECISIONS IN CREATING CYBER-SECURITY VULNERABILITIES

by

KIERAN EDWARD FLETCHER

B.S., Georgia Institute of Technology 2002

M.S., National Intelligence University, 2019

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment of the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2023

The role of management decisions in creating cyber-security vulnerabilities

Kieran Fletcher *Middle Georgia State University, kieran.fletcher@mga.edu*

Abstract

This paper employs literature analysis to develop a theory on the role of management in facilitating cyber-attacks on their own company via thematic analysis. Special attention was paid to phishing vulnerabilities and countermeasures, as well as their potential implementations. Policies that impact a workforce's susceptibility to phishing are also evaluated. The role of data system maintenance policies is also accessed. It was determined that prompt application of patches and human resources policies are key to cyber-defense. Human resources policies must avoid overworking employees, and encourage employees to report successful phishing attacks. Anti-phishing training was found to be of limited value.

Keywords: policy, management, cybersecurity, phishing, human resources, patches, updates

Introduction

Cyber-security is first and foremost a management function (Panko & Panko, 2015, p. 141). The cyber domain now connects to every aspect of modern life, including commerce (Aljeaid, et al, 2020). Information Technology (IT) is critical to every aspect of modern industry from finance to customer relations management. When enterprise IT systems are compromised it can have severe finical consequences for a company (Parenty & Domet, 2020 p. 1-5). Senior leaders must take responsibility for developing corporate cyber-security policies. Two major policy areas were studied, system security updates or patches, and phishing. Historically, unpatched vulnerabilities have contributed to globally damaging cyber-attacks (Collier, 2017). Phishing is by far the most common vector used in cyber-attacks. Phishing is a social engineering attack that uses a fraudulent email or webpage to elicit sensitive information or install malware (Kara, 2021). There are two major direct countermeasures for phishing training and simulation. Simulations are more effective but more difficult to carry out (Baillon, et al, 2019). Current human resource policies should limit employee vulnerability to phishing (Martínez-Costa, et al, 2019). However, their implementation is suspect (Abramson, 2022). The purpose of this study is to answer the following research question:

What management policies increase a firm's cybersecurity vulnerability?

Literature Review

The digital world

Internet adaptation has expanded annually, as of 2020 there were approximately five billion internet users globally (Jafar, et al, 2022). Technology has integrated itself into every aspect of modern life (Aljeaid, et al, 2020). Additionally, modern data systems are composed of complex subsystems, all of which must function correctly to provide critical services. A single defect in their underlying code may impact multiple systems (Zheng, 2009). Cyber-attacks now pose a threat to every segment of society (Zhang-Kennedy & Chiasson, 2021). Digital interconnectivity has increased the export of goods and services. In the process data, stored and transmitted in digital formats, has become the cornerstone of trade. This has reshaped industries and regulators alike (Louveaux, & Carter, 2022). These opportunities have not been without complications. Managers must maintain awareness of a cornucopia of emerging technology, they must access its potential utility, and weigh the opportunity cost of their integration into company operations. Corporations must now navigate new legal and ethical concerns, for example, data privacy rules. (Ciaramello, 2023).

Cyber-threats

The protection of digital assets and the infrastructure that hosts them is a critical concern in the modern business world (Parenty & Domet, 2020 p. 2-5). A cyber-attack may attempt to steal data or render it inaccessible, destroying it or holding it for ransom (Parenty & Domet, 2020 p. 1, 44). A cyber-attack may exploit technical vulnerabilities, human error, or both (Parenty & Domet, 2020 p. 27-28). Cyber-threats must be addressed as a management issue, central to business operations. Relegating cyber-security as a purely technical challenge is a critical mistake (Panko & Panko, 2015, p. 141-145). Phishing is the most common form of cyber-attack in use today (Kara, 2021). Cyber-threats are becoming more pervasive. Industry responses are not improving fast enough to meet the challenge; this is driving up the cost of cyber-security insurance. Insurers are expected to increase their rejection rate for cyber-attack claims and may insist on successful attribution of an attack before paying. The attribution of a cyber-attack to a specific actor is a particularly daunting task and is often impossible. Companies will be forced to rethink and significantly improve their cyber-security posture once insurance no longer mitigates losses caused by cyber-attacks (Yehezkel, 2023).

System updates

Modern data systems are incredibly complex, so the components will inevitably contain defects. An attacker can often exploit these defects to disable or improperly access the system. The companies which make the subsystems in a data system will issue updates or patches to remedy these vulnerabilities as they are discovered (Arora, et al, 2008). Applying patches often comes at the expense of system accessibility as the patch is installed (Jernigan, 2010). A global ransomware campaign is crippling organizations that continue to use outdated versions of VMWare ESXi hypervisor (Montalbano, 2023). VMWare is used to virtualize computers; this allows multiple unique instances of servers to operate on single physical machine. This significantly reduces the operating costs of running a data center (VMWare, 2023). As a result, instead of an attacker compromising a single machine, when they breach an ESXi system they gain the ability to usurp control over all Virtual Machines (VM) hosted by the ESXi host. In this attack, malicious actors are using ransomware to encrypt the host's data stores and all data related to their host VMs, then demanding approximately $23,000 to decrypt them (Montalbano, 2023).

Phishing

A phishing attack uses a misleading email to trick the recipient into installing software or visiting a fraudulent webpage. Phishing emails are designed to impersonate an email from a legitimate source, like the target's bank or employer. The goal of a phishing attack is to either steal sensitive information or install malware using the victim's credentials (Baillon, et al, 2019). Phishing exploits the human component of a data system, a user or an administrator, to bypass technical security measures humans are often the weakest point in a data system (Yanakiev, & Polimirova, 2020). Phishing attacks cause around nine billion dollars in damage every year (Sarno, et al, 2022). Early in 2023, the city of Oakland, California was at the grips of a ransomware attack. Fortunately, emergency services were not impacted by the attack. The city had to decide if it will pay the undisclosed ransom, which could range from tens of thousands of dollars to half a million dollars, or roll impacted systems back to their last uninfected backup. The investigation into the source was ongoing as of the time of writing but cyber-security experts believe the attack was initiated via a phishing email (Brinkley, 2023).

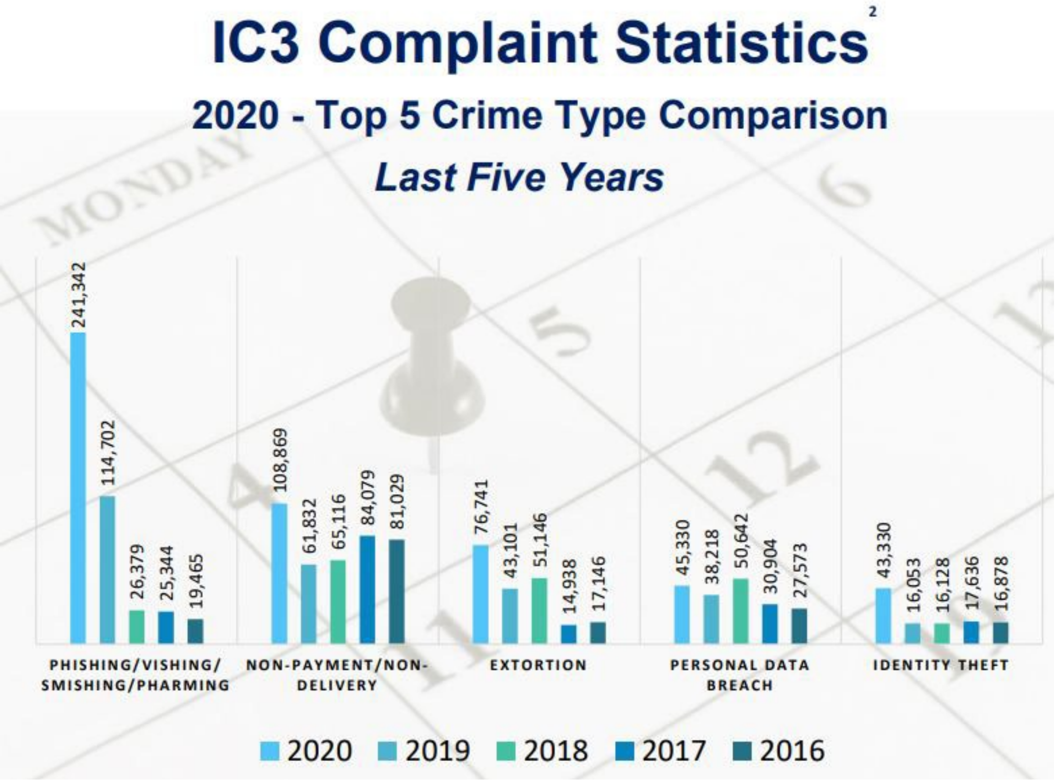

Figure 1: Criminal complaints registered with the FBI in 2020.
More phishing attacks were reported than any other form of cyber-crime (FBI, 2021).
Image source (FBI, 2021).

Phishing defense

Cyber-security is a 150-billion-dollar industry (Oxford Analytica,2022). Cyber-security has become so integral to modern life that governments have begun to legislate cyber-security standards for industry and agencies alike (Wallis, et al, 2021). Cybersecurity, including phishing countermeasures, tends to incorporate both technical defenses, for example, anti-virus software, and end-user training. The effectiveness of user training is the subject of debate (Kluge & Eckhardt, 2021). Data systems and their technical defenses require constant updating, as the cyber-threat environment is constantly evolving (Martinez, et al, 2022). Phishing is one of the most pervasive forms of cyber-attack., It has impacted roughly sixty-five percent of organizations in the United States. Anti-phishing training is the cornerstone of most organizations' phishing countermeasures (Sumner, et al, 2021). The human factor, employees, are a critical factor in cyber-defense (Allage, 2022). A prompt effective response can limit the damage inflicted by a phishing attack. The online forum Reddit was breached in February of 2023. An employee was deceived by the phishing attack and supplied the fraudulent webpage with their user id, password, and Multi-Factor Authentication (MFA) token. The attackers initiated an illicit login before the token could refresh. They were able to access some internal Reddit business intelligence systems. However, the employee who responded to the phishing email self-reported and Reddit was able to revoke the stolen credentials, before any user information was compromised. In contrast, a 2018 attack on Reddit was able to extract users' email addresses and a backup of encrypted passwords. In this case, the human factor was both the weak point in Reddit's security and the key to limiting the damage (Hope, 2023).

Challenges to the study of phishing defense

Technical countermeasures must adapt to changes in the cyber-threat environment, making them intrinsically reactive (Martinez, et al, 2022). Anti-phishing training is difficult to design and implement because the effectiveness of a particular training format will vary based on the number of participants, their perceptions, their level of experience with information technology, and demographics (Sumner, et al, 2021). Phishing is difficult to study in an academic setting as informed consent and other requirements for ethical human subjects research will influence the results of a study (Bardsley-Marcial & Johnson, 2022). Case studies revealed that real-world phishing awareness campaigns can be nullified by planning errors and implementation limits set by senior leadership. These factors undermine the effectiveness of the campaign (Rizzoni, et al, 2022). Additionally, poorly planned human resources policies, such as inadequate staffing, can render an organization's workforce more susceptible to phishing attacks (Jalali, et al, 2020).

Organizational policies

Human Resource Management (HRM) encompasses personnel center business functions, such as staffing. Historically, HRM has tended to focus on driving employees to structure their lives around career development, though modern philosophy emphasizes a work-life balance (Martínez-Costa, et al, 2019). Employers should seek a balance where employees have enough work to avoid boredom and enough free time for innovation (Gaskell, 2018).

Failure to adhere to this guidance could make management complicit in successful cyber-attacks against their organizations. Stress and time pressure are cyber-security risks, as they render employees more vulnerable to phishing attacks (Canfield, & Fischhoff, 2018). Policies that overwork employees directly increase a company's vulnerability to cyber-attack (Rizzoni, et al, 2022).

Methodology

Existing literature will be analyzed with thematic analysis, which will explain how leadership decisions can adversely impact a company's resistance to phishing attacks. Case studies and other relevant scholarly works will be analyzed to identify management-level decisions and policies that increase their organization's susceptibility to phishing attacks. Articles will be peer-reviewed and no more than fifteen years old, relevant corporate publications, or sourced from reputable news outlets.

Data analysis

The principles of thematic analysis will be applied to identify themes and leadership decisions that will adversely impact an organization's cyber-security posture. These themes will be organized and developed as the research progresses. Policies that increase a firm's vulnerability to cyber-attack will be identified.

Results

Concerning the research question, "What management policies increase a firm's cybersecurity vulnerability?" the results indicate four management policies that can undermine a firm's cyber-security.

Overview

Three major trends were noted in the literature, and one potentially damaging policy was inferred. The first one centered on the importance of system updates, there are risks when an organization fails to apply updates. However, applying an update also incurs a cost to the business. Management must balance cyber-security with operational needs (Jernigan, 2010). The prevalence of phishing as a vector for cyber-attacks and its use of social engineering makes anti-phishing training critical for an effective cyber-security policy (Schweigert, & Johnson, 2021). The techniques employed in phishing attacks are constantly evolving management must revise their training or simulation programs to reflect the current state of the threat (Sumner, et al, 2022). Selecting the correct workforce education program, conventional training or simulation requires that management consider the potential effectiveness of the program and how it would align with organizational culture, applicable laws, and labor agreements (Rizzoni, et al, 2022).

The third trend, workforce fatigue, was once the direct result of obsolete management policies (Smith, 2022; Martínez-Costa, et al, 2019). Overworking employees cripples their effectiveness and erodes their health (Carmichael, 2015). The majority of workers in the United States are overworked and are operating under a great deal of stress (Liu, ,2021). Finally, it was noted that the damage inflicted by a successful phishing attack can be limited if the employee who was phished promptly reports that they were tricked and facilitated an attack (Hope, 2023).

System updates

Modern data systems are complex, and vulnerabilities in these systems represent substantial cyber-security risks. Unpatched vulnerabilities can result in the compromise of sensitive data, loss of access to a data system, or the modification or deletion of data (Arora, et al, 2008). In May 2017, the WannaCry ransomware program rampaged across the globe by exploiting EternalBlue, a known vulnerability in the windows operating system (Trautman & Ormerod, 2019, p. 505). Ransomware encrypts data on an infected system, denying access to the data. The attacker demands payment in exchange for decrypting the data, which restores its availability (Berger, 2017, p. 20-21). WannaCry infected over 200,000 computers across 150 countries (Collier, 2017). The May 2017 WannaCry outbreak inflected billions of dollars in damage (BBC, 2017). However, the attack should have failed. WannaCry should not have been able to infect a single system. Microsoft issued a patch for the EternalBlue vulnerability two months before the May attack (Microsoft, 2017).

Cyber-security training

Cyber-security training, including anti-phishing training, is considered a cornerstone of effective cyber-defense (Miller, et al, 2020). A typical cyber-security training program presents trainees with information about cyber threats and then tests the trainees' knowledge retention and ability to apply this knowledge (Kävrestad, et al, 2022). Cyber-security training is often a reoccurring requirement for all employees of an organization (Venables, 2021). The goal of this training is to mitigate the system the risks posed by users of a data system (Yanakiev, & Polimirova, 2020). Phishing attacks are a major vector an attacker can use to exploit the human component of a data system training programs must evolve as the threat does (Kara, 2021; Kävrestad, et al, 2022). There is evidence that despite regular training employees are still highly susceptible to cyber-attacks, with roughly of those surveyed half falling victim (Segal, 2022).

There are some limitations to the current standard for counter-phishing training. The approach is not optimal, and training is less effective than simulation (Baillon, et al, 2019). Individuals taking training are aware that they are being tested, additionally, poorly designed training may simply teach trainees to avoid rather than analyze suspicious emails (Martínez-Costa, et al, 2019). Training cannot simulate the employees' day-to-day environment, with competing concerns and other distractions. When they are in training, they can focus exclusively on identifying the phishing attacks in the test (Kluge & Eckhardt, 2021).

A phishing simulation sends phishing attacks to an organization's employees without warning. Employees do not know they are being tested. After the exercise employees are given feedback on their performance. When tested employees who have been through simulation are less likely to click on or provide information to a phishing webpage, than those with conventional training. It should be noted that employees who have not gone through training or a simulation are the most likely to be deceived by the phishing attack. Combining training and simulation does not provide a meaningful improvement in performance over the exclusive use of simulations (Baillon, et al, 2019). A phishing simulation can be used to access the effectiveness of a training program (Sutter, et al, 2022).

A phishing simulation is not as easy to arrange as a conventional training regime. First, the timing of a simulation must be carefully planned to prevent employees from deducing that a test is underway. Secondly, management must consider the secondary effects of an accurate phishing simulation, employee trust in the organization may be harmed. A phishing simulation will also increase the workload of the IT support staff (Rizzoni, et al, 2022). Additionally, a realistic simulation would require a company to send phishing emails to its employees that either promise a reward for carrying out the email's instructions or threaten retribution if ignored (Sumner, et al, 2021). This could violate labor agreements or even local laws (Rizzoni, et al, 2022).

Employee fatigue

The digital age has enabled collaboration on a global scale, experts in different fields and time zones can communicate in real time. This enables better decisions by providing a more comprehensive perspective (Akther, et al, 2022). With this new capability came a new threat, the data systems that facilitate this communication and process vast collections of information are subject to attack. Companies must establish policies to protect their digital infrastructure (Georg-Schaffner & Prinz, 2021). The digital age also ushered in an age of global competition in many sectors of the economy necessitating comprehensive corporate policies (Thakur, 2022). The digital age promoted rapid evolution in cyber-security policy. Initially, cyber-security was viewed as a domain of the information technology department. This view grossly underestimated the importance of cyber-security and the impact of data system compromises. Current philosophy considers cyber-security to be the responsibility of an organization's senior leaders
(Panko & Panko, 2015, p. 141).

Human Resource Management (HRM) is a critical component of organizational policy, impacting every aspect of a business from productivity to cyber-security. Employee well-being is at the heart of modern HRM (Demo, et al, 2020). Working excessively long hours reduces an employee's job satisfaction and mental health (Kuroda & Yamamoto, 2018). It can even cause or exacerbate chronic medical conditions (Wong, et al, 2019).

From a cyber-security perspective, a large workload increases susceptibility to phishing attacks (Yeng, et al, 2022). Employees suffering from fatigue will have a degraded ability to identify the subtle differences between a well-developed phishing email and a legitimate message (Rizzoni, et al, 2022). A large workload and time pressure induce stress which increases phishing vulnerability. Additionally, attempting to work on multiple projects simultaneously splits an employee's attention increasing the likelihood that they will be deceived by a phishing attack (Canfield, & Fischhoff, 2018).

The risks to both the company and employee born of overwork and stress are clear, current management philosophy addresses this, in theory. In practice, most employees are overworked and under considerable stress (Deloitte, 2018).

TA summary of the critical findings is shown in Table 1.

Table 1: A summary of the critical findings

Software updates	Management may be negligent if they delay too long between patches, or ignore critical patches. The advent of dynamic updating will limit the cost of applying patches, making it gross neglect to leave a system unpatched (Microsoft, 2022). Until they adopt technologies like dynamic updates, companies must consider both the cost of applying a patch and the potential expense of delaying installation (Brooks, 2023).
Cyber-security training	Even the most effective counter-phishing training program have a 15%-20% failure rate, in a company with one thousand users which is one-hundred and fifty to two hundred successful attacks (Baillon, et al, 2019). Even aggressive training regiments are ineffective, managers would be better off seeking technical solutions, like MFA, to limit the damage caused by an attack (Alammari & Albahr, 2022). Relying on cyber-security training is dangerous given the high failure rate (Parenty & Domet, 2020 p. 17-19).
Employee fatigue	Overworking employees is a widespread act of negligence (Rizzoni, et al, 2022). The risks are clear, putting employees under stress, especially undue time pressure, greatly increases susceptibility to phishing. Operating while understaffed is dangerous (Canfield, & Fischhoff, 2018).
Measured reaction when an employee is deceived by a phishing email	In a large corporation, it is inevitable that one or more employees will be deceived by a phishing attack and unwittingly facilitate a system breach (Parenty & Domet, 2020 p. 17-19). Rapid detection of the incursion is critical if the company hopes to mitigate the damage. Company policies must encourage employees who fall for a phishing attack to come forward (Hope, 2023). Punitive responses to employee mistakes could dissuade employee self-reporting allowing a breach to persist.

Discussion and Conclusion

An organization's patch cycle and cyber-security training policies should both be driven by cost-benefit analysis. Patching data systems often requires a loss of functionality that can either reduce productivity or missed orders from customers (Jernigan, 2010). The potential expense in data integrity and system availability created by an unpatched security vulnerability can be extreme (BBC, 2017). For now, organizations must balance system availability with security, but technology may change this equation. The development of dynamic software updating could enable patching without a loss of availability (Hayden, et al, 2014). The adoption of cloud-based computing has the potential to eliminate loss of service during a patch cycle, removing the cost of updating data systems (Microsoft, 2022). At present there is often the possibility that a vulnerability will be exploited before a patch can be deployed, generally, this would simply be bad luck. But in the event of a publicized critical patch or in an organization with an excessively long patch cycle, it could rise to the level of managerial negligence. The damage inflicted by the WannaCry attacks illustrates the importance of keeping computer systems updated. It should be noted that both hardware and software will require regular updates to operate securely (Ashok, et al, 2018).

The development of an appropriate cyber-security training program is a similar exercise opportunity-cost analysis. A simulation will better prepare staff to detect phishing attacks but can inflict substantial damage on employee morale, and may be constrained by laws or labor agreements (Baillon, et al, 2019; Rizzoni, et al 2022). In either case, the program must be updated regularly to remain valid (Sumner, et al, 2022). Training must be repeated but not so frequently that it induces training fatigue (Sutter, et al, 2022). There is some debate as to the utility of cyber-security training, as every program has a failure rate, and it only takes one successful phishing attack to compromise a system (Parenty & Domet, 2020 p. 17-19).

Technology may offer a solution, in the case of attacks that compromise login credentials, usernames, and passwords, Multi-Factor Authentication (MFA) can limit the utility of stolen credentials (Alammari & Albahr, 2022). One example of MFA is a one-time code sent via text message that must be entered to complete a log-in. (Neagle, 2017). This system is used to access GALILEO from the MGA Library's webpage. Additionally, the prompt reporting of successful phishing -attacks by the employees who were deceived can limit the harm caused by the attack (Hope, 2023). Another option is the use of Explainable Artificial Intelligence (XAI) to improve human effectiveness in the detection of phishing emails. XAI highlights anomalies in an email that are designed to deceive a human. For example, XAI could highlight domain names that may appear legitimate when given a cursory glance but are spelled slightly differently from the real URL (Kluge & Eckhardt, 2021).

Workplace HRM policies have failed (Abramson, 2022). The ideal workplace, where employee well-being is central, and work-life balance is key has not been successfully implemented (Martínez-Costa, et al, 2019; Ro, 2021). Excessive stress and overwork are normal, as they affect more than half of employees. Some sources attribute this to the COVID-19 pandemic (Abramson, 2022). However, major news outlets have been reporting similar numbers since 2001, long before the COVID-19 outbreak (ABC News Network, 2001). Managers have failed to implement effective measures to counter stress and overwork, the literature did not reveal whether they do not know how to create a model work environment or if they simply have never tried (Telford, 2022; Gaskell, 2018). Instead, they have created environments that are ideal targets for phishing attacks (Rizzoni, et al, 2022). The problem has persisted for over two decades, at this point damage incurred by a phishing attack should be attributed to senior management regardless of who opened the email (ABC News Network, 2001).

Areas for future research

Future research should attempt to determine the optimal workload to enable employees to integrate cyber-security into their normal routines. A comparative analysis of the success rates of phishing attacks in different work environments could serve to establish baseline metrics. Also, the impact of policies that are tolerant of self-reported employee cyber-security policy deviations is worthy of study. Such policies may enable companies to limit the damage sustained due to cyber-attacks.

Previous research advocated for anti-phishing training while noting its failure rate. New and innovative approaches to anti-phishing training are needed to increase the effectiveness of training. Additionally, research is required to develop technology to help employees identify malicious emails. Technologies that can detect and mitigate breaches in data systems should also be researched.

References

ABC News Network. (2001, May 16). *Study: U.S. Workers Burned Out.* ABC News. Retrieved February 10, 2023, from https://abcnews.go.com/US/story?id=93295&amp;page=1

Abramson, A. (2022, January 1). *Burnout and stress are everywhere*. Monitor on Psychology. Retrieved February 10, 2023, from https://www.apa.org/monitor/2022/01/special-burnout-stress

Akther, N., Al Mamun, M., Azad, M., Kalam, A., & Sorwar, G. (2022). *Review of Human Resource Management (HRM) Literature: A bibliometric Analysis* (1981-2019). DLSU Business & Economics Review, 32(1).

Alammari, A., & Albahar, M. (2022). *Exploring and Adoption of Two Authentication Factors: Formation of Competence*. ASEAN Journal of Psychiatry, 23(4), 1–5.

Allage, A. (2022, July 12). Council post: *Why employees violate cybersecurity policies*. Forbes. Retrieved January 2, 2023, from https://www.forbes.com/sites/forbesbusinesscouncil/2022/07/11/why-employees-violate-cybersecurity-policies/?sh=37caade1d986

Aljeaid, D., Alzhrani, A., Alrougi, M., & Almalki, O. (2020). *Assessment of end-user susceptibility to cybersecurity threats in Saudi Arabia by simulating phishing attacks*. 11(12), 1–18. https://doi.org/10.3390/info11120547

Arora, A., Telang, R., & Xu, H. (2008). *Optimal policy for software vulnerability disclosure*. Management Science, 54(4), 642–656. https://doi.org/10.1287/mnsc.1070.0771

Ashok, A., Steenkiste, P., & Bai, F. (2018). *Vehicular cloud computing through dynamic computation offloading*. Computer Communications, 120, 125–137. https://doi.org/10.1016/j.comcom.2017.12.011

Baillon, A., de Bruin, J., Emirmahmutoglu, A., van de Veer, E., & van Dijk, B. (2019). *Informing, simulating experience, or both: A field experiment on phishing risks*. *PLOS ONE*, *14*(12). https://doi.org/10.1371/journal.pone.0224216

Bardsley-Marcial, B., & Johnson, R. (2022*). COMMON FACTORS IN SUSCEPTIBILITY TO PHISHING.* International Journal of Information, Business and Management, 14(4). B

BBC. (2017, December 19). *Cyber-attack: US and UK blame North Korea for WannaCry*. BBC News. Retrieved February 5, 2023, from https://www.bbc.com/news/world-us-canada-42407488

Berger, B. (2017). *WannaCry Exposes Defense Supply Chain Vulnerabilities*. National Defense, 102(764), 20–21

Brinkley, L. (2023, February 14). *Expert explains how city of Oakland may have become victim of ransomware attack*. ABC7 San Francisco. Retrieved February 15, 2023, from https://abc7news.com/city-of-oakland-ransomware-attack-hackers-phishing-scam/12810409/

Brooks, C. (Ed.). (2023, January 23). *Business cost keeping software updated*. business.com. Retrieved February 6, 2023, from https://www.business.com/articles/speed-of-technology-the-business-cost-of-keeping-your-software-updated/

Canfield, C. I., & Fischhoff, B. (2018). *Setting Priorities in Behavioral Interventions: An Application to Reducing Phishing Risk.* Risk Analysis: An International Journal, 38(4), 826–838. https://doi.org/10.1111/risa.12917

Carmichael, S. G. (2015, August 19). *The research is clear: long hours backfire for people and for companies*. Harvard Business Review. Retrieved February 8, 2023, from https://hbr.org/2015/08/the-research-is-clear-long-hours-backfire-for-people-and-for-companies

Ciaramello, A. (2023, February 14). Council post: Challenges of leading in a Digital age. Forbes. Retrieved February 17, 2023, from https://www.forbes.com/sites/forbesfinancecouncil/2023/02/14/challenges-of-leading-in-a-digital-age/?sh=7408380f2203

Collier, R. (2017). *NHS ransomware attack spreads worldwide*. Canadian Medical Association Journal, 189(22). https://doi.org/10.1503/cmaj.1095434

Deloitte (2018). Workplace Burnout Survey: Deloitte Us. Deloitte United States. Retrieved February 8, 2023, from https://www2.deloitte.com/us/en/pages/about-deloitte/articles/burnout-survey.html

Demo, G., Costa, A. C. R., Coura, K. V., Miyasaki, A. C., & Fogaça, N. (2020). *What do scientific research say about the effectiveness of human resource management practices? Current itineraries and new possibilities*. Revista de Administração Unimep, 18(3), 138-158.

FBI. (2021, March 17). IC3 releases 2020 internet crime report. FBI. Retrieved February 15, 2023, from https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

Gaskell, A. (2018, May 1). *What does overwork do to our productivity?* Forbes. Retrieved February 7, 2023, from https://www.forbes.com/sites/adigaskell/2018/05/01/what-does-overwork-do-to-our-productivity/?sh=17fd861e4b9f

Georg-Schaffner, L., & Prinz, E. (2021). *Corporate Management Boards' Information Security Orientation: An analysis of cybersecurity incidents in dax 30 companies*. Journal of Management and Governance, 26(4), 1375–1408. https://doi.org/10.1007/s10997-021-09588-4

Hayden, C. M., Saur, K., Smith, E. K., Hicks, M., & Foster, J. S. (2014). *Kitsune: Efficient, General-Purpose Dynamic Software Updating for C*. ACM Transactions on Programming Languages and Systems, 36(4), 1–38. https://doi.org/10.1145/2629460

Hope, A. (2023, February 14). *Reddit confirmed a security breach after a sophisticated phishing attack.* CPO Magazine. Retrieved February 15, 2023, from https://www.cpomagazine.com/cyber-security/reddit-confirmed-a-security-breach-after-a-sophisticated-phishing-attack/

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). *Why employees (still) click on phishing links: An investigation in Hospitals*. Journal of Medical Internet Research, 22(1). https://doi.org/10.2196/16775

Jafar, M. T., Al-Fawa'reh, M., Barhoush, M., & Alshira'H, M. H. (2022). *ENHANCED analysis approach to detect phishing attacks during COVID-19 crisis*. Cybernetics and Information Technologies, 22(1), 60–76. https://doi.org/10.2478/cait-2022-0004

Jernigan, J. (2010). *Demystifying Medical Equipment Software: Updates vs. Upgrades.* Biomedical Instrumentation & Technology, 44(6), 495–497. https://doi.org/10.2345/0899-8205-44.6.495

Kara, İ. (2021). *DON'T BI DON'T BITE THE BAI TE THE BAIT: PHISHING A T: PHISHING ATTACK FOR IN CK FOR INTERNET BANKING (E-BANKING)*. Journal of Digital Forensics, Security and Law, 16.

Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R., & Furnell, S. (2022). *Evaluation of contextual and game-based training for phishing detection*. Future Internet, 14(4). https://doi.org/10.3390/fi14040104

Kluge, K., & Eckhardt, R. (2021). *Explaining the Suspicion: Design of an XAI-based User-Focused Anti-Phishing Measure.* Wirtschaftsinformatik 2021 Proceedings, 1–17. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1197&context=wi2021

Kuroda, S., & Yamamoto, I. (2018). *Why do people overwork at the risk of impairing mental health?* Journal of Happiness Studies, 20(5), 1519–1538. https://doi.org/10.1007/s10902-018-0008-x

Liu, J. (2021, June 15). U.S. workers are among the most stressed in the world, New Gallup report finds. CNBC. Retrieved February 5, 2023, from https://www.cnbc.com/2021/06/15/gallup-us-workers-are-among-the-most-stressed-in-the-world.html

Louveaux, C., & Carter, R. (2022, May 11). *The impact of digitalization on the Global Marketplace in 2022. The Impact of Digitalization on the Global Marketplace in 2022* | U.S. Chamber of Commerce. Retrieved February 15, 2023, from https://www.uschamber.com/on-demand/technology/digital-economy-the-global-competition-to-write-the-rules

Martinez, S., Gransart, C., Stienne, O., Deniau, V., & Bon, P. (2022). Soren, how dynamic software update tools can help cybersecurity systems to improve monitoring and actions. *JUCS - Journal of Universal Computer Science*, *28*(1), 27–53. https://doi.org/10.3897/jucs.66857

Martínez-Costa, C., Mas-Machuca, M., & Olivella, J. (2019). *Staffing policies of leading professional service firms.* Intangible Capital, *15*(1), 38. https://doi.org/10.3926/ic.1370

Microsoft. (2017, March 14). *Microsoft Security bulletin MS17-010 - critical.* Microsoft Learn. Retrieved February 5, 2023, from https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Microsoft. (2022, November 28). *Eliminate downtime through versioned service updates* - azure DevOps. Azure DevOps | Microsoft Learn. Retrieved February 6, 2023, from https://learn.microsoft.com/en-us/devops/operate/achieving-no-downtime-versioned-service-updates

Miller, B., Miller, K., Zhang, X., & Terwilliger, M. G. (2020). *Prevention of phishing attacks: A three-pillared approach*. Issues In Information Systems, 21(2), 1–8. https://doi.org/10.48009/2_iis_2020_1-8

Montalbano, E. (2023, February 7). *Ongoing vmware esxi ransomware attack highlights inherent virtualization risks.* Dark Reading. Retrieved February 15, 2023, from https://www.darkreading.com/cloud/ongoing-vmware-esxi-ransomware-attack-virtualization-risks

Neagle, C. (2017). *New Year's Resolution: Improve Your Password*s. Journal of the Missouri Bar, 73(1), 32–33.

Oxford Analytica (2022). *Cybersecurity of US firms is improving but unevenly*, Expert Briefings. https://doi.org/10.1108/oxan-db267823

Panko, R. R., & Panko, J. L. (2015). *Business Data Networks and security* (10th ed.). Pearson.

Parenty, T. J., & Domet, J. J. (2020). *A leader's guide to cybersecurity: Why boards need to lead-and how to do it.* Harvard Business Review Press.

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). *Phishing simulation exercise in a large hospital*: A case study. DIGITAL HEALTH, 8, 1–13. https://doi.org/10.1177/20552076221081716

Ro, C. (2021, May 19). *How overwork is literally killing us*. BBC Worklife. Retrieved February 10, 2023, from https://www.bbc.com/worklife/article/20210518-how-overwork-is-literally-killing-us

Sarno, D. M., McPherson, R., & Neider, M. B. (2022). *Is the key to phishing training persistence? Developing a novel persistent intervention.* Journal of Experimental Psychology: Applied, 28(1), 85–99. https://doi.org/10.1037/xap0000410

Schweigert, C. T., & Johnson, R. A. (2021). *Testing the susceptibility of employees to phishing emails*. International Journal of Information, Business and Management, 13(3).

Segal, E. (2022, July 27). *Why companies should not count on all employees to guard against cyberattacks*. Forbes. Retrieved January 7, 2023, from https://www.forbes.com/sites/edwardsegal/2022/07/26/why-companies-should-not-count-on-all-employees-to-guard-against-cyberattacks/?sh=316cb9a51e1e

Smith, M. (2022, October 6). *50% of workers are burned out and 'productivity paranoia' could be making it worse: 'people are just worn down*'. CNBC. Retrieved February 8, 2023, from https://www.cnbc.com/2022/10/06/microsoft-50-percent-of-people-are-burned-out-at-work.html

Sumner, A., Yuan, X., Anwar, M., &McBride, M. (2021). *Examining factors impacting the effectiveness of anti-phishing trainings*. Journal of Computer Information Systems, 62(5), 975–997. https://doi.org/10.1080/08874417.2021.1955638

Sutter, T., Bozkir, A. S., Gehring, B., & Berlich, P. (2022). Avoiding the hook: Influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception. IEEE Access, 10, 100540–100565. https://doi.org/10.1109/access.2022.3207272

Telford, T. (2022, October 31). *U.S. workers have gotten way less productive. no one is sure why*. The Washington Post. Retrieved February 10, 2023, from https://www.washingtonpost.com/business/2022/10/31/productivity-down-employers-worried-recession/

Thakur, A. (2022). *Strategic Human Resource Management and Organizational Citizenship Behavior: A Critical Review of the Relationship in the Presence of Employee Diversity*. International Management Review, 18.

Trautman, L. J., & Ormerod, P. C. (2019). Wannacry, Ra*nsomware, and the Emerging Threat to Corporations*. Tennessee Law Review, 86(2), 503–556.

Venables, A. (2021). Modelling cyberspace to determine cybersecurity training requirements. Frontiers in Education, 6. https://doi.org/10.3389/feduc.2021.768037

VMware. (2023). *What is ESXi: Bare metal hypervisor: ESX. VMware.* Retrieved February 15, 2023, from https://www.vmware.com/products/esxi-and-esx.html

Wallis, T., Johnson, C., & Khamis, M. (2021*). Interorganizational Cooperation in Supply Chain Cybersecurity: A cross-industry study of the effectiveness of the UK implementation of the NIS directive.* Information & Security: An International Journal, 48(1), 36–68. https://doi.org/10.11610/isij.4812

Wong, K., Chan, A. H. S., & Ngan, S. C. (2019). *The effect of long working hours and overtime on Occupational Health: A meta-analysis of evidence from 1998 to 2018*. International Journal of Environmental Research and Public Health, 16(12). https://doi.org/10.3390/ijerph16122102

Yanakiev, Y., & Polimirova D. (2020). *Exploring the Role of the Human Factor in Cybersecurity: Results from an Expert Survey in Bulgaria*. Information & Security: An International Journal. 44, 39-50.

Yehezkel, S. (2023, February 15). *The cost of cybersecurity insurance is soaring–and state-backed attacks will be harder to cover. it's time for companies to take threats more seriously*. Fortune. Retrieved February 15, 2023, from https://fortune.com/2023/02/15/cost-cybersecurity-insurance-soaring-state-backed-attacks-cover-shmulik-yehezkel/

Yeng, P. K., Fauzi, M. A., Yang, B., & Nimbe, P. (2022). *Investigation into phishing risk behaviour among healthcare staff.* Information, 13(8), 392. https://doi.org/10.3390/info13080392

Zhang-Kennedy, L., & Chiasson, S. (2021). *A systematic review of multimedia tools for cybersecurity awareness and Education*. ACM Computing Surveys, 54(1), 1–39. https://doi.org/10.1145/3427920

Zheng, J. (2009). Cost-sensitive boosting neural networks for software defect prediction. *Expert Systems with Applications*, *37*(6), 4537–4543. https://doi.org/10.1016/j.eswa.2009.12.056