Journal of Crime and Criminal Behavior
Vol. 2, No. 2, 2022, pp. 131-144
© ARF India. All Right Reserved
URL: www.arfjournals.com
https://doi.org/10.47509/JCCB.2022.v02i02.04

Cybercrime and the Nature of Insider Threat Complexities in Healthcare and Biotechnology Engineering Organizations

Darrell Norman Burrell[1], Calvin Nobles[2], Austin Cusak[3], Marwan Omar[4] and Lemie Gillesania[5]

[1]Marymount University, ORCID
[2]Illinois Institute of Technology. E-mail: cn8972@gmail.com
[3]Robert Morris University. E-mail: pogicusak@gmail.com
[4]Illinois Institute of Technology. E-mail: drmarwan.omar@gmail.com
[5]Capitol Technology University. E-mail: gillesanialemie@outlook.com
Corresponding author: darrell.burrell@yahoo.com

Abstract: This article explores the nature of cybersecurity professionals being insider threats to their own organization, as well as the general increase in harder-to-detect threats coming from an ever-widening acceptance of third-party insiders, which organizations, biotechnology engineering, and other healthcare organizations rely on. After examining the current and emerging literature on how individuals are motivated to engage in problematic workplace behaviors as a means of gaining their specific goal or need, the paper articulates malicious cybersecurity insider threat indicators, then provides best practices for reducing the risk of these threats in healthcare and biotechnology engineering organizations.

Received : 15 July 2022
Revised : 30 August 2022
Accepted : 15 September 2022
Published : 30 November 2022

TO CITE THIS ARTICLE:

Darrell Norman Burrell, Calvin Nobles, Austin Cusak, Marwan Omar and Lemie Gillesania (2022). Cybercrime and the Nature of Insider Threat Complexities in Healthcare and Biotechnology Engineering Organizations. *Journal of Crime and Criminal Behavior,* 2: 2, pp. 131-144. *https://doi.org/10.47509 /JCCB.2022.v02i02.04*

Introduction

Biotechnology engineering encompasses a large subset of life sciences industries. Biotech engineers may work in medical equipment manufacturing, pharmaceutical and medicine manufacturing, research and development, education, and many other areas where their scientific know-how is required. Cybersecurity in healthcare and biotechnology engineering involves protecting electronic information and assets from unauthorized access, use, and disclosure (Wilder, 2022). There are three goals of cybersecurity: protecting the confidentiality, integrity, and availability of information, but the designation of insiders cannot be defined simply by their employment status (Wilder, 2022). Healthcare organizations must look at insiders through application and data access entitlements. Healthcare and biotechnology engineering cybersecurity insider threats typically include employed- and non-employed staff, volunteers, vendor partners, contractors, and even patients who access their personal health records via online portals.

According to Wilder (2022), each of these individuals may expose sensitive data, which could also be identified as Spector and Fox's (2005) concept of Counterproductive Work Behaviors (CWBs) for any one of three reasons:

- *Accidental:* Unauthorized exposure of sensitive information is often the result of users lacking awareness of processes or best practices.
- *Negligence:* Users who knowingly disregard established policies due to negligence have various reasons, but their intent is not malicious.
- *Malicious:* Users who intentionally expose sensitive data for various reasons, whether for financial gain, espionage, or something else.

Counterproductive work behaviors (CWBs) are volitional behaviors that harm an organization's, its members' well-being, or both (Spector & Fox, 2005). CWB is a general term that covers a broad range of behaviors, such as sabotage, aggression, theft, and production deviance. Employers are concerned about cybersecurity insider threats because of the wide range of CWBs and their ability to undermine organizations' interests.

Sabotage in the workplace is a form of workplace violence that is seldom discussed (Spector & Fox, 2005). However, the effects of employee sabotage can span across many areas. Consider the costs incurred for hardware, software, and additional personnel to rebuild a company computer system after a virus that an employee intentionally uploaded has annihilated it. Consider having to pay for a lawsuit by an employee who was affected by an act of sabotage (whether it is physically, mentally, or reputation-wise) because the company did nothing to stop the act or reprimand the perpetrator. Furthermore, consider having to rebuild the morale and trust levels when an act of sabotage occurs. In broad terms, employee sabotage occurs when an employee intentionally inflicts damage on the organization or its members to undermine or disrupt the operation or profit of the organization in some way.

Healthcare Cybersecurity

The profession of cybersecurity only recently emerged from the larger Information Assurance field of IT Security and has ported over many practices that need refinement and customization (Lippert & Cloutier, 2021). Modern healthcare depends on protecting biotechnology engineering data and patient information, which cybersecurity provides. However, cybersecurity as a field is still establishing its norms, standards, and best practices (NAPA Workforce Report, 2022), meaning cybersecurity practitioners come with varying degrees of ethics and intentions. Therefore, while the medical profession went through its own process of professionalization starting in the 1840s to create the American Medical Association (Spidalieri, 2014), it remains reliant on a continuously expanding profession with no centralized association to confirm competence and ensure an appropriately higher standard of ethics is followed (p.16). This relationship has been further taxed by the increase of security threats and data breaches during the COVID-19 crisis, which enlarged the target on the Healthcare sector for both external criminals and insider threats (Alkinoon *et al.*, 2021).

As the healthcare and biotechnology engineering sectors become more reliant on remote workers, support staff using their own devices, and the realities of living/working through a pandemic, it has, by necessity, expanded the definition and roster of whom it allows to be an insider. Gelles (2016) shows that as more people and interactions move from brick-and-mortar offices to the increasingly interconnected online world, some workers gain a sense of anonymity because their behaviors are no longer observed. The social and external constraints are lessened, making their own internal constraints of integrity and morality more necessary. While there are many benefits to remote/telework, one downside is the increased difficulty of observant co-workers to impede, interrupt, or deter potential insider threats (p.44). Countering this effect requires biotechnology engineering and healthcare organizations to increase their ethical training and standards for their cybersecurity workforce since a skilled cybersecurity professional is usually in a high-trust position and could take advantage of their employer's lack of understanding in how they work and what they do (Dawson, 2018). In addition, with more insiders from different companies being let in, it becomes harder for biotechnology engineering and healthcare organizations to know what their contracted and sub-contracted companies hiring standards are, how they screen for mental health issues, and what internal reporting practices they use to notify the parent organization of their employees CWBs.

Cybersecurity Insider Threats

Many biotechnology engineering and healthcare organizations are becoming even more interconnected, meaning a quality cybersecurity insider threat program protects more than just the Healthcare organization where it is housed. However, quality programs and ethically trained professionals are often only prioritized once it is too late (Alkinoon *et al.*, 2021). For example, despite data breaches and ransomware attacks frequently being in the news, Fruhlinger (2020) found that 67% of surveyed medium/small U.S. businesses had some cybersecurity attack happen to them in 2019, yet 18% of decision-makers in those businesses still felt cybersecurity was a low priority. In addition, half of the total participants surveyed believed being attacked or attacked again was unlikely to happen to them.

The world needs to produce more cybersecurity professionals to counter threat actors using emerging technologies from outside while securing the increasingly blurred boundaries of what is owned inside each organization (Dobson, 2018). Those that do enter the profession often come from other careers first, with Frost & Sullivan (2017) estimating that 87% of our current cyber workforce moved into cybersecurity from a related field, with 30% of that being people lacking technical backgrounds. This means that while some higher education programs require courses of ethics and morality in their curriculum, many currently within and entering the cybersecurity career field lack the infusion of ethical, social, cultural, political, and economic perspectives needed to grapple with moral dilemmas and interpersonal pressures (Jacobs *et al.*, 2018).

Students and self-taught cybersecurity professionals learn dangerous hacking skills without understanding the seriousness of misusing those skills (Pike, 2013), leading to the engagement of CWBs early in a profession when the cybersecurity practitioner may not have the wisdom to resist risky behavior. Most cybersecurity professionals are committed to fully complying with rules, laws, and regulatory statutes established by their work, including published ethical frameworks (Pike, 2013). However, as part of the curriculum taught to students and learned through self-led training, cybersecurity professionals early on learn traditionally illegal computing skills as part of becoming security specialists. More than a few of those students were initially attracted to the field of cybersecurity because it can be fun to do quasi-legal things with their computers (Pike, 2013). The profession is thus mired in grey areas, requiring an increased emphasis on ethics and proper moral decision-making (p.68); otherwise, there is an increased possibility of a Healthcare organization having a highly-skilled, highly placed cybersecurity professional normalizing their personal CWBs.

Gelles (2016) supports this, saying that the growing interconnected nature of organizations opens the door to more and more insiders that have access to those organizations' information but lack loyalty to that organization's norms and values. These types of insiders also often gain access to their co-worker's information through social media, online profiles, online records, and internal company databases, allowing cyber-savvy insiders to more easily social engineer other employees (p.196). For a cybersecurity professional trained to use tools and tactics for gaining access and not leaving digital footprints, there is a higher potential for success in them engaging in CWBs to seek revenge on others whom they perceive have wronged them.

Workplace revenge

Bandura (2016) found that when a person begins a personal moral disengagement process, they begin to see their own CWBs as regular, leading them to view morally disengaged rule-breaking as ordinary. Without proper ethical training, they may end up justifying other common subconscious tactics for engaging in CWB, such as dehumanization of their target (organization and/or person), using euphemistic labeling, another type of moral justification that validates their thoughts and eventual actions to seek revenge on those who have wronged them (Bandura, 2002).

Historically, workplace violence and revenge were seen as separate issues within insider threat programs because they required a different type of investigation, usually not focused on counterintelligence or counterespionage (Gelles, 2016). However, all mitigation of insider threats is usually brought under one program. The CWB indicators leading to workplace revenge can be subtle and hard to identify from purely online means. This can be an even more complicated set of indicators to identify when the insider threat is a cybersecurity professional that can effectively mask their malicious CWB activity from non-cybersecurity trained insider threat analysts. Employees feeling undervalued and unfairly treated may become disgruntled towards an organization and an individual, to the point where they feel they are experiencing a crisis (p.165). That individual may seek revenge by trying to lash out at people, materials, or specific information as a perceived means to solve their crisis. Gelles (2016) says this chain of events is part of the commonly misunderstood myths of who is likely to be a violent/nonviolent insider threat because it can happen to anyone. There is no profile for a personality type being more likely to become an insider threat since it is not always the vocally disgruntled people that engage in revenge-type CWBs, and the moment of crisis often builds slowly over time. In such a state of crisis, the moral attentiveness helping a person distinguish between ethical and immoral behavior is strained (Shields & Funk, 2015), making it easier for those with high levels of access and skill to engage in revenge-type CWBs that can severely damage the person and/or Healthcare organization.

Problem Statement

The total cost of workplace insider threats is difficult to estimate precisely, but the available statistics are astonishing. According to the National Retail Federation (2017), employee theft accounted for 30% of inventory loss, which cost the U.S. retail economy $14.67 billion in 2016. In addition, less tangible forms of CWBs have tremendous costs: Cisco estimated that workplace incivility costs them $12 million a year. Their employees also respond to workplace incivility by decreasing work efforts and the quality of work (Porath & Pearson, 2013). This project seeks to explore the nature of cybersecurity insider threats and understand the emerging best practices to address them in biotechnology engineering and healthcare.

Method

This conceptual paper uses content from relevant and emerging literature in biotechnology engineering, healthcare cybersecurity, cybersecurity insider threats, and malicious workplace behavior to influence the world of practice. This will occur by researching and combining practical solutions dispersed in the literature and combining it into a comprehensive, coherent discussion focused on educating and incubating more research and discussion on the topic of cybersecurity insider threats. The value of this research is that are limited studies on complexities and responses to insider threats in cybersecurity in healthcare and biotechnology organizations. Most of the research in this field is focused on technical approaches and not approaches focused on the management of people.

Contexts and Theories

Cybersecurity insider threats are posed by individuals from within an organization, such as current or former employees, contractors, and partners (Georgiadou, Mouzakitis, & Askounis, 2021). These individuals can potentially misuse access to networks and assets to disclose, modify and delete sensitive information (Georgiadou, Mouzakitis, & Askounis, 2021) wittingly or unwittingly. Several significant insider threat examples include:

- Capital One had an information security breach that involved the theft of more than 100 million customer records, 140,000 Social Security numbers, and 80,000 linked bank details of Capital One customers, allegedly stolen by a single insider (Fazzini, 2019)
- A former Google executive was given an 18-month prison term for stealing design information on Google's self-driving car and providing them to his new employer, Uber (Statt, 2020).
- Facebook had to release an employee accused of exploiting the privileged information his position accorded him to stalk women online (Popken, 2018)
- An employee at Tesla allegedly sent company trade secrets and design information to third parties and sabotaged company systems (Kemp, 2018).

A psychological need to develop effective information security employees and cultures amid extreme vulnerabilities is essential to preserving conducive organizational social systems. These systems should support those who challenge corrupt behaviors or those that are cybersecurity experts who are dedicated to protecting organizational assets. Though ambiance for protecting organizational assets is more corrective than preemptive, a democratic responsibility of safeguarding trust and critical organizational information by every stakeholder in the organizational system is much needed. Robbins and Judge (2017) distill research to establish vital qualities which serve as cornerstones for trustworthy organizational cultures that can minimize insider threats, which are:

1. Determined and sustained commitment to the execution of ethical conduct and decision making
2. Inclusive interests and benevolence in correspondence between people
3. Skill or adeptness in executing all-inclusive interests into decisions.

With the growth of technology and new forms of cybercrime, it has become critically important that organizations understand the importance of embracing effective information security cultures, ethical cultures, moral reasoning, and ethical decision-making.

Rest (1979) framed the four-component moral reasoning model that challenges the CWBs of cybersecurity insider threat employees. The steps within this model are:

1. Moral Sensitivity, which helps to identify conflicts, looks at all interested parties, the consequences of CWBs, and any obligations to the subjects.
2. Moral Judgment includes forming a fair and honest perspective before action or inaction.
3. Moral Commitment includes reflecting on actions and behaviors' moral implications and consequences.
4. Moral Action includes deciding the best ethical and fair action to be taken in a way that understands the weight and impact of CWBs.

Goodman (2007) postulated that stricter supervision and accountability through effective leadership and management was the key to affecting the attitudes and behaviors of employees. To reduce CWBs and the growth of cybersecurity insider threats in the workplace, Goldman (2007) asserted it was not enough to have rules, regulations, and training. The enforcement of those regulations was vitally essential as having a straightforward course of action for all employees who break the rules. Millage (2005) offered, "Organizations need to evaluate what will work most effectively, including a closer look at the role workplace culture plays" (p. 13).

Although the functional approach to CWB, which suggests that CWBs serve specific needs or motives, is not entirely new, the motives underlying CWBs have yet to be examined extensively (Krischer *et al.*, 2010). There are a few examples of limited conceptual discussions and empirical studies. For example, using CWBs to get revenge has been proposed and discussed (Bies *et al.*, 1997; Folger & Skarlicki, 2005). Moreover, research has demonstrated that employees engage in production deviance and withdrawal to reduce emotional exhaustion (Krischer *et al.*, 2010). However, we need a systematic framework of CWB motives and comprehensive empirical studies examining CWB motives.

Motivations

Attempts to conceptualize the nature of human motives/motivation have been numerous. Given its multiple aspects and changing perspectives on the subject, definitions or even labels in this area have differed across time and researchers (Heckhausen, 2018). Because we examine the nature of one type of work behavior, CWBs, the definition of motivation in the workplace context was consulted and utilized.

Pinder (2008) defined work motivation as "a set of energetic forces that originate both within as well as beyond an individual's being, to initiate work-related behavior, and to determine its form, direction, intensity, and duration" (p. 11). This definition stresses motivation's energizing and directional aspects, which is consistent with our functional approach for CWBs. Moreover, the definition is compatible with our focus on the reasons and processes underlying CWBs. Examining the forces underlying CWBs may reveal more about the nature of CWBs and the processes leading to them. Therefore, based on work motivation and the functional approach, we define CWB motives as forces that initiate and direct counterproductive work behaviors. These forces can often be thought of as goals or needs, where individuals engage in CWBs to achieve specific goals or meet particular needs.

Vengeance

First, the vengeance or revenge motive is a popular notion that has received much attention in previous research. This popularity may be due in part to the incorporation of vengeance in narratives in the media surrounding workplace violence. However, violence is a rarely used form of revenge in the workplace (Tripp & Bies, 2009).

Although researchers have defined and named the vengeance motive differently, their core ideas are similar: vengeance or revenge is a response to perceived unfairness, injustice, or personal harm (e.g., violation of social order or norm). For example, Bies *et al.* (1997) outlined a thermodynamics model as the theoretical framework for understanding vengeance and revenge in organizations. From their point of view, vengeance is a response to "a perceived personal harm or violation of the social order" (p. 19). Folger and Skarlicki (2005) proposed the concept of Organizational Retaliatory Behaviors (ORB) and defined these as "a subset of ... negative [workplace] behaviors … used to punish the organization and its representatives in response to perceived unfairness" (Skarlicki & Folger, 1997, p. 435). These conceptualizations overlap substantially. Based on previous work, we define the vengeance motive for CWB as the goal to inflict damage, injury, discomfort, or punishment on the party judged responsible in response to perceived unfairness or personal harm by another party (Tripp & Bies, 2009, p. 3). An example of this from a cybersecurity insider threat perspective could be an employee not selected for a promotion who now feels the need to sell organizational trade secrets to a competitor out of vengeance for not being selected.

Furthermore, it is worth noting that vengeance or revenge is multifaceted. Bies *et al.* (1997) indicated that the conventional view considers revenge only in behavioral terms and evaluates it as a destructive and emotional act. Workplace violence is an excellent example of this characterization. However, the revenge motive could exist solely in cognitions as well. For instance, workplace injustice may spark the vengeance motive, but this is never acted on due to status differences between the parties. Folger and Skarlicki (2005) also argued that ORB could be dysfunctional and functional for organizations. ORB may hinder organizational goals but also hold people accountable for their wrongdoings. Moreover, retaliation could result from self-interest and a third party's reactions to others' misdeeds (e.g., refusing to help someone mean to other colleagues). To sum up, the revenge motive is multifaceted and captures various organizational behaviors and cognitions.

CWB activities that relate to information at risk of being compromised could include details about an organization's security practices, customer and employee data, login credentials, and sensitive financial records (Georgiadou, Mouzakitis, & Askounis, 2021). The nature of insider threats means that traditional preventative security measures are often ineffective (Georgiadou, Mouzakitis, & Askounis, 2021).

Insider Threats in Cybersecurity

Traditional security measures tend to focus on external threats and cannot always identify an internal threat from inside the organization (Georgiadou, Mouzakitis, & Askounis, 2021).

Types of insider threats include:

- A malicious insider is someone who maliciously and intentionally abuses legitimate credentials, typically to steal information for financial or personal incentives. Examples are workers who hold a grudge against a former employer or an opportunistic employee who sells secret information to a competitor. Malicious insiders have an advantage over other attackers because they are familiar with an organization's security policies and procedures and its vulnerabilities (Georgiadou, Mouzakitis, & Askounis, 2021).
- A careless insider is an innocent pawn who unknowingly exposes the system to outside threats. This is the most common type of insider threat, resulting from mistakes, such as leaving a device exposed or falling victim to a scam. For example, an employee who intends no harm may click on an insecure link, infecting the system with malware (Georgiadou, Mouzakitis, & Askounis, 2021).
- A mole is an imposter who is technically an outsider but has gained insider access to a privileged network. Someone from outside the organization poses as an employee or even joins the organization with a sinister agenda (Georgiadou, Mouzakitis, & Askounis, 2021).

Malicious Insider Threat Indicators

Anomalous activity at the network level could indicate an inside threat (Georgiadou, Mouzakitis, & Askounis, 2021). Likewise, if an employee is dissatisfied, holds a grudge, or starts to take on more tasks with excessive enthusiasm, this could indicate a significant threat (Georgiadou, Mouzakitis, & Askounis, 2021; Gheyas & Abdallah, 2016).

Trackable insider threat indicators are often captured by monitoring both insiders' behavioral and digital actions.

Behavioral Indicators

There are a few different behavioral indicators of an insider threat that should be closely monitored, including:

- A dissatisfied or disgruntled employee, contractor, vendor, or partner.
- Attempts to circumvent security.
- Constantly working off-hours.
- Displays resentment toward co-workers.
- The routine violation of organizational policies.
- Contemplating resignation or discussing new opportunities (Georgiadou, Mouzakitis, & Askounis, 2021; Gheyas & Abdallah, 2016).

Digital Indicators

There are a few different digital indicators of an insider threat that should be closely monitored, including:

- Signing into enterprise applications and networks at unusual times. For instance, an employee who, without prompting, signs into the network at 3 am may be cause for concern.
- A surge in the volume of network traffic. For example, an employee tries to copy large quantities of data across the network.
- Unusual spikes in network traffic.
- Access resources they usually do not or are not permitted to.
- An employee is accessing data that is not relevant to their job function.
- Repeated requests for access to system resources not relevant to their job function.
- Using unauthorized devices such as USB drives.
- Network crawling and deliberate search for sensitive information.
- An employee is emailing sensitive information outside the organization (Georgiadou, Mouzakitis, & Askounis, 2021; Gheyas & Abdallah, 2016).

Conclusions: Steps To Reduce the Risk of Insider Threats

Protecting critical assets, including systems, technology, facilities, and people, can be physical or logical. Intellectual property is another critical asset, including customer data for vendors, proprietary software, schematics, and internal manufacturing processes. It requires organizations to form a comprehensive understanding of their critical assets by asking and answering questions such as what critical assets they currently possess if they have appropriately prioritized them., and understanding the current state of each asset (Georgiadou, Mouzakitis, & Askounis, 2021; Gheyas & Abdallah, 2016).

Biotechnology engineering and other healthcare organizations must clearly document organizational policies, consistently enforce them, and prevent misunderstandings. Everyone in the organization should be familiar with security procedures and understand their rights concerning intellectual property (IP), so they do not share the privileged content they have created. (Georgiadou, Mouzakitis, & Askounis, 2021; Gheyas & Abdallah, 2016). To prevent sabotage, employers should ensure that all employees know the company's intolerance against sabotage and that violating this corporate policy would lead to disciplinary action, including termination and a lawsuit. The policy should be publicized and enforced to add further validity. In addition to a policy against sabotage, some employers have even included a provision in their employee handbooks that gives managers the right to inspect lockers, desks, and anything else that belongs to the company if they suspect employee sabotage.

However, a formal, written policy will only get a company so far. It is equally, if not more important, for employers to develop and practice fair employee relations, open lines of communication, and employee assistance programs so that employees are given a chance to express their feelings, ideas, and criticisms.

Increase visibility and deploy solutions to keep track of employee actions and correlate information from multiple data sources. For example, organizations can use deception technology to lure a malicious insider or imposter and gain visibility into their activities. (Georgiadou, Mouzakitis, & Askounis, 2021; Gheyas & Abdallah, 2016).

Promote culture changes ensuring security is not only about expertise but also about attitudes and beliefs. Organizations should educate their employees regarding security issues and improve employee satisfaction to combat negligence and address the drivers of malicious behavior (Georgiadou, Mouzakitis, & Askounis, 2021).

Insider Threat Detection Solutions

Insider threats can be more brutal to identify or prevent than outside attacks since they are invisible to traditional security solutions like firewalls and intrusion detection systems, which focus on external threats (Georgiadou, Mouzakitis, & Askounis, 2021). If an attacker exploits an authorized login, the security mechanisms may not identify the abnormal behavior (Georgiadou, Mouzakitis, & Askounis, 2021). Moreover, malicious insiders can more easily avoid detection if they are familiar with the security measures of an organization (Georgiadou, Mouzakitis, & Askounis, 2021; Gheyas & Abdallah, 2016).

Organizations should diversify their insider threat detection strategy to protect all assets instead of relying on a single solution (Georgiadou, Mouzakitis, & Askounis, 2021; Gheyas & Abdallah, 2016). An effective insider threat detection system combines several tools to monitor insider behavior, filter through many alerts, and eliminate false positives (Georgiadou, Mouzakitis, & Askounis, 2021; Gheyas & Abdallah, 2016).

References

Alkinoon, M., Choi, S. & Mohaisen, D. (2021). Measuring healthcare data breaches. In *International Conference on Information Security Applications, 13009,* 265-277. Springer. https://doi.org/10.1007/978-3-030-89432-0_22

Bandura, A. (2002). Selective moral disengagement in the exercise of moral agency. *Journal of Moral Education, 21*(2), 101-120. https://doi.org/10.1080/0305724022014322

Bandura, A. (2016). *Moral disengagement: How people do harm and live with themselves. Business Ethics Quarterly*, *26*(3), 426–429. https://doi.org/10.1017/beq.2016.37

Bies, R., Tripp, T., & Kramer, R. (1997). At the breaking point: Cognitive and social dynamics of revenge in organizations. In R. A. Giacalone & J. Greenberg (Eds.), *Antisocial behavior in organizations*, (pp. 18–36). Sage.

Dawson J., & Thomson R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology, 9 (744).* https://doi.org/10.3389/fpsyg.2018.00744

Dobson, S. (2018). Cybersecurity talent hard to find: Report. *Canadian HR Reporter, 31*(9), *3–18*. https://www.hrreporter.com/focus-areas/recruitment-and-staffing/cybersecurity-talent-hard-to-find-report/299496

Fazzini, K. (2019, June 30). The Capital One breach is unlike any other major hack, with allegations of a single engineer wreaking havoc. *CNBC*. Retrieved from: https://www.nbcnews.com/tech/social-media/facebook-investigating-claim-engineer-used-access-stalk-women-n870526

Folger, R., & Skarlicki, D. P. (2005). Beyond counterproductive work behavior: Moral emotions and deontic retaliation versus reconciliation. In S. Fox & P. E. Spector (Eds.), *Counterproductive work behavior: Investigations of actors and targets* (pp. 83–106). American Psychological Association. https://doi.org/10.1037/10893-004

Frost & Sullivan, (2017). Global Information Security Workforce Study: Benchmarking workforce capacity and response to cyber risk. *Center for Cyber Safety and Education*. https://www.iamcybersafe.org/s/gisws

Fruhlinger, J. (2020, March 9). Top cybersecurity facts, figures, and statistics. *CSO Online*. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Gelles, M. (2016). *Insider threat: Prevention, detection, mitigation, and deterrence*. Elsevier. http://dx.doi.org/10.1016/B978-0-12-802410-2.00015-0

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Detecting Insider Threat via a Cyber-Security Culture Framework. *Journal of Computer Information Systems, 62*(4), 706-716. https://doi.org/10.1080/08874417.2021.1903367

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big data analytics, 1*(1), 1-29. https://bdataanalytics.biomedcentral.com/articles/10.1186/s41044-016-0006-0

Goodman, D. (2007). *Enforcing ethics* (3rd ed.). Prentice-Hall.

Heckhausen, H. (2018). *Motivation and action*. (J. Heckhausen, Ed.). Springer. https://doi.org/10.1007/978-3-319-65094-4_2

Hung, T. K., Chi, N. W., & Lu, W. L. (2009). Exploring the relationships between perceived co-worker loafing and counterproductive work behaviors: The mediating role of a revenge motive. *Journal of Business and Psychology, 24*(3), 257-270. https://doi.org/10.1007/s10869-009-9104-6

Jacob, J., Wei, W., Sha, K., Davari, S., & Yang, T. (2018). Is the Nice Cybersecurity Workforce Framework (NCWF) Effective for a Workforce Comprising of Interdisciplinary Majors? *16th International Conference on Scientific Computing, pages 124-130.* https://par.nsf.gov/biblio/10095246

Kemp, T. (2018, July 19). What Tesla's Spygate Teaches Us About Insider Threats. *Forbes.* Retrieved from: https://www.forbes.com/sites/forbestechcouncil/2018/07/19/what-teslas-spygate-teaches-us-about-insider-threats/?sh=367702605afe

Krischer, M. M., Penney, L. M., & Hunter, E. M. (2010). Can counterproductive work behaviors be productive? CWB as emotion-focused coping. *Journal of occupational health psychology, 15*(2), 154-166. https://doi.org/10.1037/a0018349

Lee, J. S., Kwak, D. H., & Braustein-Minkove, J. R. (2016). Coping with athlete endorsers' immoral behavior: Roles of athletes identification and moral emotions on moral reasoning strategies. *Journal of Sports Management, 30*(2), 176-191. http://dx.doi.org/10.1123/jsm.2015-0341

Lippert, K. & Cloutier, R. (2021). Cyberspace: A digital ecosystem. *Systems 2021, 9*(3), 1-20. https://doi.org/10.3390/systems9030048

NAPA Workforce Report. (2022). A call to action: The federal government's role in building a cybersecurity workforce for the nation. *National Academy of Public Administration.* https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf

National Retail Federation. (2017, June 22). National retail security survey 2017. NRF. https://cdn.nrf.com/sites/default/files/2018-10/NRSS-Industry-Research-Survey-2017.pdf

Pinder, C. C. (2008). *Work motivation in organizational behavior.* Psychology Press. https://doi.org/10.4324/9781315734606

Pike, R. (2013). The "ethics" of teaching ethical hacking. *Journal of international technology and information management, 22*(4). https://scholarworks.lib.csusb.edu/jitim/vol22/iss4/4

Porath, C & Pearson, C. (2013, February). The price of incivility. *Harvard business review*, *91*(1-2), pp. 114–121. https://hbr.org/2013/01/the-price-of-incivility

Popken, B. (2018, May 1). Facebook fires engineer who allegedly used access to stalk women. *NBC News.* Retrieved from: https://www.nbcnews.com/tech/social-media/facebook-investigating-claim-engineer-used-access-stalk-women-n870526

Rest J. (1979). *Development in judging moral issues*. University of Minnesota Press.

Robbins, S., Judge, T. (2017). *Organizational Behavior.* Person.

Shields, D., & Funk, C. (2015). Predictors of moral disengagement in sport. *Journal of Sports & Exercise Psychology, 37*(6), 646-658. https://doi.org/10.1123/jsep.2015-0110

Skarlicki, D. P., & Folger, R. (1997). Retaliation in the workplace: The roles of distributive, procedural, and interactional justice. *Journal of Applied Psychology, 82*(3), 434. https://doi.org/10.1037/0021-9010.82.3.434

Spector, P. E., & Fox, S. (2002). An emotion-centered model of voluntary work behavior: Some parallels between counterproductive work behavior and organizational citizenship behavior. *Human Resource Management Review, 12*(2), 269–292. https://doi.org/10.1016/S1053-4822(02)00049-9

Spidalieri F. & Kern S. (2014). Professionalizing cybersecurity: A path to universal standards and status. *Pell Center for International Relations and Public Policy.* https://salve.edu/sites/default/files/filesfield/documents/Professionalizing-Cybersecurity.pdf

Statt, N. (2020, August 20). Former Google exec Anthony Levandowski sentenced to 18 months for stealing self-driving car secrets. *The Verge.* Retrieved from: https://www.theverge.com/2020/8/4/21354906/anthony-levandowski-waymo-uber-lawsuit-sentence-18-months-prison-lawsuit

Tripp, T. M., & Bies, R. J. (2009). *Getting even: The truth about workplace revenge--and how to stop it.* John Wiley & Sons.

Wilder, J. (2022, April 27). HHS Warns of Insider Threats in the Healthcare Sector. *Healthcare Innovation*. https://www.hcinnovationgroup.com/cybersecurity/data-breaches/news/21265719/hhs-warns-of-insider-threats-in-the-healthcare-sector