Motivating Employees and Organizations to Adopt a Cybersecurity-Focused Culture

Ron Fisher
Idaho National Laboratory

Celia Porod
Idaho National Laboratory

Sydney Peterson
Idaho National Laboratory

We explore the reality of cyber risk faced by organizations, along with the lack of preparedness that continues to become apparent with each successful cyber-attack. Sources project continued growth and evolution of cyber-attacks; they will become more frequent and more sophisticated. To prepare for and mitigate these risks, we propose creating a cybersecurity-focused culture throughout all organizations. The greatest vulnerability, the employees, can also become the greatest defense when properly trained and informed. We review numerous studies that provide outcomes focused on enhancing cybersecurity culture to provide a list of recommended activities for organizations looking to strengthen their cybersecurity posture.

Keywords: cybersecurity, culture, employee motivation, cybersecurity training

INTRODUCTION

The way individuals and organizations view cybersecurity today is quite interesting; most people know there is a need to ensure cybersecurity measures are in place within their personal lives and their organizations, but there is uncertainty on what actions to take to be cyber-safe. Our physical world and cyber world are highly interconnected creating significant interdependent relationships. As stated by the U.S. Department of Homeland Security (DHS), "our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace" (DHS, 2019). To live our lives as we currently do today, and to move forward with continued technological advancements, we need both our physical and cyber worlds to be functioning properly, which requires appropriate defenses to mitigate risks and deter attacks. The greatest defense against both physical and cyber-attacks remains the same: people.

Organizations today are faced with complex challenges due to the evolving risk environment and the interconnectedness of systems, both cyber and physical. As technology continues to advance, telecommuting and remote work are becoming an integral part of the modern office; however, this shift in the workforce poses additional risks. Thus, ensuring effective cybersecurity measures are in place requires implementation and adoption of policies and procedures, along with an organizational shift to a culture that prioritizes cybersecurity at all levels. This cultural shift is dependent upon the individuals within the organization and their willingness to change their behavior to enhance their cybersecurity. Effective change in organizational culture cannot take place without behavioral changes occurring among individual employees; to change culture, individuals must sustainably change their behavior.

In this paper, we present background information on cyber vulnerabilities to frame the issue, followed by an overview of security, culture change, and employee motivation, with the conclusion focused on real-world application of what organizations can do to enhance their cybersecurity as well as resources that are available to them. With the recent increase in remote employees, we also touch on some of the potential risks related to teleworking. This paper does not aim to provide a single solution for enhancing cybersecurity; it merely presents near-term actions that organizations can take to strengthen their cybersecurity, such as leveraging available checklists and resources, and long-term actions that address the greater culture challenges.

THE REALITY OF CYBER VULNERABILITY

Global reliance on the Internet continues to grow. By 2022, there will be an estimated 6 billion Internet users, which is only 2 billion less than the estimated world population (Morgan, 2019). The more Internet users there are, the more human and digital targets exist for cyber-attacks (Morgan, 2019). Clearly stated by DHS Cybersecurity and Infrastructure Security Agency (CISA) (2019a), "as Americans become more reliant on modern technology, we also become more vulnerable to cyberattacks such as corporate security breaches, spear phishing, and social media fraud." More Internet users and greater technology reliance calls for stronger cybersecurity measures and increased cybersecurity posture among organizations.

Even with this incredible dependence on the Internet, there are still individuals and organizations that lack urgency and commitment to ensure appropriate cybersecurity measures are in place to protect valuable information across personal and professional domains. In 2018, Verizon published the Verizon Data Breach Investigations Report (DBIR) which indicated there were over 53,000 incidents and 2,216 confirmed data breaches over a 12-month period. The total volume of cyber events increased almost fourfold between January 2016 and October 2017 (Cisco Annual Cybersecurity Report, 2018). As stated by the Former Cisco CEO John Chambers, "There are two types of companies: those that have been hacked, and those who don't yet know they have been hacked" (Cisco).

When reviewing data of U.S. publicly traded companies who submitted Securities and Exchange Commission (SEC) filings, only 2.8 percent of companies identified cyber risk as one of their business risk concerns in 10-K filings for 2017 (Fisher, Wood, Porod, and Greco, 2020). Similarly, a global survey conducted about attitudes and opinions on information technology (IT) security by Kaspersky Lab (2017) determined that only 14 percent of survey participants regard cyber threats in their top three risks; survey participants included 1,300 senior professionals from small business to enterprise level across 11 countries. Results from the Kaspersky Lab (2017) study highlighted the following for the study participants:

- 91 percent had been affected by attacks in the last year;
- 45 percent were under-prepared for dedicated cyber-attacks;
- 17 percent had lost financial information as a result of attacks;
- 57 percent had banned access to social networks due to potential security risks; and,
- 30 percent had still not fully implemented anti-malware software.

Data such as this indicates that organizations may not be prepared for cyber-attacks, especially if they do not identify cyber risk as a business risk in formal reporting. In the U.S. alone, malicious cyber activity cost the economy an estimated $57 billion to $109 billion in 2016 (The Council of Economic Advisers, 2018). It is estimated that cybercrime will continue to rise, costing nearly $5.2 trillion globally over the next five years (Accenture, 2019). On average, the cost of cybercrime is $13 million for sophisticated attacks per organization (Accenture, 2019).

In 2016, the top five industries identified as being at-risk for cyber-attacks included the following: (1) healthcare; (2) manufacturing; (3) financial services; (4) government; and (5) transportation (Morgan, 2016). Although most media attention is focused on large companies following the disclosure of a cyber incident, Verizon's DBIR stated that 58 percent of victims are categorized as small businesses (Verizon, 2018). Without proper cybersecurity measures in place, many small businesses go out of business within six months of being victimized by cyber-attacks (Steinberg, 2019). According to IBM (2018), cyber-attacks do not only have financial implications for organizations, but they can also result in the following consequences:

- Damage brands and reputations;
- Erode and even decimate customer loyalty;
- Result in loss of intellectual property;
- Put companies out of business;
- Invite regulatory penalties;
- Impair security for governments and states; and,
- Increase potential for future attacks.

Not only is it important for organizations to have cyber risk mitigation measures in place, but it is also key to have plans developed and reviewed regularly to minimize negative impacts to operations before, during, and after an attack. In a study conducted by Fisher, Norman, and Klett (2017), a review of 6,148 critical infrastructure facilities identified that only 11 percent reported having cybersecurity plans in place. Cybersecurity plans address cybersecurity or information technology continuity, which are critical to ensuring organizations can carry out their missions following a cyber-attack whether operations are partially or fully disrupted (Fisher, Norman, Klett, 2017). Our ever-expanding increased interconnectedness has created a complex external risk environment that is more difficult for organizations to manage (Fisher, Norman, Klett, 2017). It is important to ensure employees within all levels of the organization are effectively trained on a regular basis to encourage the implementation of successful cybersecurity measures. Ensuring appropriate plans and procedures are in place for responding to and recovering from an attack are critical to maintaining or regaining operability of key cyber assets and systems.

Overview of Cyber Threats: Internal and External

The security equation is made up of three components: people, process, and technology; "any security manager who is not attending to people, process, *and* technology is inviting a major, and perhaps disastrous incident" (Batteau, 2011). Perhaps the most critical component of that security equation, and the greatest cyber vulnerability in organizations today, is people or employees, as they are the users of the technology and the implementers of the processes. Employees could be the gateway for an attack to take place in unintentional ways, or they could be the attackers, stealing valuable information and data from the company for malicious purposes.

External attacks, such as phishing schemes, hacking, password theft, malware, and data mishandling, are common, but so are insider threats/attacks. External attacks often target employees to gain access to an organization's operating systems, business sensitive information, protected data, and more. Table 1 below outlines some of the most common cyber-attacks and their descriptions as identified by Cisco.

TABLE 1
WHAT ARE THE MOST COMMON CYBER ATTACKS?

Malware	Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms.
Phishing	Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email.
Man-in-the-middle (MitM)	MitM attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction.

Denial-of-service	A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth.
Structured Query Language (SQL) Injection	An SQL injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.
Zero-day exploit	A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented.
DNS Tunneling	DNS tunneling utilizes the DNS protocol to communicate non-DNS traffic over port 53.

CISCO

Beyond external attacks, insider threats continue to be a great vulnerability that every single organization faces. As stated by DHS CISA:

> "*All organizations are vulnerable to the threat that insiders may use their access to compromise information, disrupt operations, or cause physical harm to employees. To mitigate this threat, organizations are encouraged to establish and maintain a comprehensive insider threat program that protects physical and cyber assets from intentional or unintentional harm*" (DHS CISA, 2019b).

According to the National Insider Threat Task Force, an insider is defined as, "any person with authorized access to an organization's resources to include personnel, facilities, information, equipment, networks, or systems" (DHS CISA, 2019b). The National Insider Threat Task Force defines insider threat as:

> "*the risk an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of propriety information and technology; damage to company facilities, systems or equipment, actual or threatened harm to employees; or other actions that would prevent the company from carrying out its normal business practice*" (DHS CISA, 2019b).

A highly publicized example of a successful insider attack is that of Edward Snowden. While employed as a government contractor, he successfully downloaded and leaked thousands of intelligence documents requiring the Pentagon to spend billions of dollars to overcome the damage (NBC News, 2014). As a National Security Agency (NSA) contractor, Snowden had access to certain classified information, but he was able to persuade 20-25 coworkers to give him their logins and passwords by telling them they were needed for him to do his job as computer systems administrator (NBC News, 2014). In April 2012, Snowden began downloading documents describing the government's electronic spying programs, successfully downloading and leaking thousands of documents (NBC News, 2014).

In addition to malicious insider threat, there is also the risk of employee negligence. A 2018 State of the Industry Report by Shred-it (2018) found that 96 percent of American consumers think employee negligence contributes to breaches. The same report stated that half of C-Suites say human error or accidental loss by an insider caused a data breach, indicating that in the world of information security "the biggest obstacle U.S. companies face is their own staff" (Shred-it, 2018). However, findings also indicated that "most U.S. businesses do not offer adequate data security training to their staff" (Shred-it, 2018). Only 78 percent of participants reported training their staff on information security procedures and policies at least once a year (Shred-it, 2018). Organizations are also experiencing a shift in their workforce, with more employees participating in teleworking and open-concept offices. Both put businesses at a greater risk caused by human error (Shred-it, 2018).

Organizations need to ensure mitigation measures are in place for both internal and external cyber-attacks, as well as plan for what needs to take place when a cyber-attack is occurring or has occurred. The evolution of the workforce causes some challenges, but organizations can equip their employees to become their greatest defense against cyber-attacks. This can be accomplished through training, encouraging ownership in cybersecurity processes and procedures, and engraining cybersecurity as part of organizational culture.

MOVING THE BAR ON CYBERSECURITY

For organizations to improve their cybersecurity measures, there needs to be a reprioritization; cybersecurity needs to become a top priority for organizations from leadership through all levels of employees. As presented by de Bruijn and Janssen (2017) there exists a paradox: information security risks are on the rise, but people seem to feel less worried about the matter. De Bruijn and Janssen (2017) stated:

> *"Although cybersecurity is one of the most important challenges faced by governments today, the visibility and public awareness remains limited. Almost everybody has heard of cybersecurity, however, the urgency and behaviour of persons do not reflect high level of awareness."*

The lack of compliance with specified policies or expected behaviors when it comes to cybersecurity may be due to people not being aware of (or not perceiving) the risks or, they do not know (or fully understand) the "correct" behavior (Bada, Sasse, and Nurse, 2015). Bada, Sasse, and Nurse (2015) identify three key areas of focus for people to adopt secure online behavior: (1) they need to accept that the information is relevant; (2) they need to understand how to respond; and, (3) they need to be willing to carry out these actions in the face of many other demands. Ultimately, the focus of shifting organizational culture to embrace, adopt, and fully implement cybersecurity policies and procedures is reliant on peoples' abilities to change their behaviors.

As defined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), cybersecurity, or cyberspace security, is defined as "preservation of confidentiality, integrity, and availability of information in the cyberspace" (ISO, 2012). It is the protection of the interests of a person, society, or nation, including their information and non-information-based assets that need protection from the risks relating to their interaction with cyberspace (Reid and Van Niekerk, 2014). Cyberspace is defined as, "the complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" (ISO, 2012). And finally, cybercrime is defined as "criminal activity where services or applications in the cyberspace are used for or are the target of a crime, or where the cyberspace is the source, tool, target, or place of a crime" (ISO, 2012).

Moving the bar on cybersecurity is reliant upon the people within the organization. This means all people, from the C-Suite through all levels of employment. Every individual within an organization is part of the cyber defense, helping to mitigate and prevent attacks so that their organizations' missions can continue to be carried out daily.

Historic Perspective on Security: Reactive Vs. Proactive

To understand security culture in general, it is helpful to learn from the past by looking at historical incidents and the historical reactive culture verses the necessary proactive culture moving forward. From the beginning of civilization, humans have had to defend themselves from various threats to ensure survival. Historical events like the ones outlined below provide insight into key components for not only surviving attacks but maintaining our way of life, through increasing awareness, preparing for both manmade and natural incidents, and understanding approaches for response and recovery.

Since the time of the Roman Empire and ancient Egypt, great nations and societies have often viewed themselves as impenetrable to potential external threats. This is similar to the mindset seen today of "it won't happened to me." As history has demonstrated, this belief often leads to complacency with respect to security posture, which ultimately resulted in the demise of once-great nations and societies. Lessons learned from these and other historic examples serve as important reminders to leading nations today. The

United States, for example, had not considered itself highly vulnerable to a homeland attack until 1941, when the Japanese attacked Pearl Harbor. The Nation rallied after Pearl Harbor, instituting protective measures to mitigate vulnerabilities; a strong sense of patriotism, driven by normative beliefs in protecting the homeland, motivated changes at all levels (i.e., citizens, communities, organizations, government) that were instituted in a collaborative and holistic manner. As a result, the security posture of the Nation rapidly improved.

Since Pearl Harbor, other threats to the homeland, such as the Russian missile crisis, have followed this same pattern. In recent history, the terrorist attacks of September 11, 2001 (9/11), served as a new reminder of the vulnerabilities to the homeland. Immediately after 9/11, a patriotic spirit rapidly developed within the Nation to fight terrorism. For a brief period, security was ingrained into the culture. However, over time, the motivation to ensure appropriate security measures are in place has declined. For example, after 9/11, security line delays were readily accepted by air passengers. Today, there are public complaints against airport body scanners and security pat downs; people view them as more of a hassle and less of the critical security measure that they are.

Certainly, the lack of succinct information sharing and communication concerning ongoing threats and acceptable protective measures is part of this problem. For example, the Homeland Security Advisory System (HSAS) established in 2002 in response to the terrorist attacks to "provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts" (Homeland Security Presidential Directive [HSPD]-3, 2002) is criticized for "lack of public confidence in the system" (HSAC, 2009). In the years since 9/11, it is reported that current threats are greater, more complex, and more diverse than before (Bergen and Hoffman, 2010). The evolving terrorist threat requires a sustainable and ongoing protective posture that has not previously been observed in the United States.

Similar to physical security measures, cybersecurity measures are necessary in order to deter attacks, as well as prevent or minimize the amount of information and data that can be accessed by an attacker. As mentioned above, there seems to be a common thought shared among individuals and organizations alike, that "it won't happen to me" when it comes to topics like cyber-attacks. For example, the 2017 data breach at Equifax comprised information of 148 million Americans; a congressional report blamed the breach on "a culture of complacency" at the credit reporting company (Johnson, 2018). It was identified that the lack of an adequate security program contributed to the breach, after Equifax failed to fully patch every impacted system when an Apache Struts software flaw was detected in March 2017 (Johnson, 2018). There was also a lack of network traffic monitoring at Equifax, with the attack carrying on for 76 days. The suspicious activity was detected only after Equifax executives updated an expired security certificate, triggering the incident response effort (Johnson, 2018).

The number of Internet users will continue to increase, while simultaneously increasing cybercrime targets. This reality is the reason that cybersecurity needs to be an ongoing, proactive effort. Cyber systems and networks relied upon by organizations are not impenetrable and need to be treated as such. Individuals and organizations can no longer wait for something to happen to then act.

Cyber Is the Greatest Manmade Threat

The cyber threat is real – "no threat facing America has grown as fast, or in a manner as difficult to understand, as the danger from cyberattacks" (The Heritage Foundation, 2020). Paul Martini, co-founder of iBoss, stated, "Without shooting a single bullet or missile, you can shut down an entire country or nation" in reference to the current cyber threat faced worldwide (Brown, 2020). Martini also stated that "private-sector corporations, which include banking, health care, and energy services, would be the primary targets… it's not just the lights, it's also the Internet which shuts down communication systems" (Brown, 2020). There will likely be a continued increase in the number of cyber threats and cyber-attacks that occur in many years to come. In 2018, Daniel Coats, the former Director of National Intelligence, addressed the U.S. Senate Select Committee stating:

> "*We face a complex, volatile and challenging threat environment. The risk of interstate conflict is higher than any time since the end of the Cold War – all the more alarming*

> *because of the growing development and use of weapons of mass destruction by state and nonstate actors. Our adversaries, as well as the other malign actors, are using cyber and other instruments of power to shape societies and markets, international rules and institutions, and international hotspots to their advantage*" (Garamone, 2018).

In 2019, the World Economic Forum's Global Risks Report listed out the top ten risks by likelihood. This report ranked cyber-related risks as the top manmade risks behind weather and climate, as demonstrated in Table 2 below:

TABLE 2
WORLD ECONOMIC FORUM TOP 10 RISKS BY LIKELIHOOD 2019

1	Extreme weather events (e.g. floods, storms, etc.)
2	Failure of climate-change mitigation and adaptation
3	Major national disasters (e.g. earthquake, tsunami, volcanic eruption, geomagnetic storms)
4	**Massive incident of data fraud/theft**
5	**Large-scale cyberattacks**

Myers and Whiting, 2019

Even with the understanding of the severity of the threat that cyber-attacks pose, the constantly changing threats and vulnerabilities in the cyber domain have left the U.S. unprepared (The Heritage Foundation, 2020). According to The Heritage Foundation (2020), nation-state hackers are the most serious threat to the U.S, specifically Russia and China in terms of cyber threat sophistication. Organizations must prepare for attacks through planning, training, and cultural shifts to adopt the protective cybersecurity posture discussed earlier.

THE SECURITY RISKS OF TELEWORKING

Teleworking, also known as telecommuting, is defined as employees and/or contractors' working away from the traditional office or organizational facilities via external networks through computers and telecommunication technologies such as Virtual Private Networks (VPN) to maintain a link to the office and access internal organizational resources (Autry, 2019; Yang et al., 2013). As teleworking becomes more common, the risks associated with working away from the office could increase as well. In 2010, the U.S Government introduced the Telework Enhancement Act "requiring government agencies to have a coherent policy in teleworking and concrete roles in the management of teleworking" (Brown et al., 2016; US OPM, 2017).; a posture that can serve as a model for nongovernment organizations to follow when establishing and/or modifying telecommuting policy, procedures, training, and implementation.

It is imperative that organizational leaders work with teleworkers to develop adequate training and policies to mitigate risks. Employees must have security and threat awareness training to overcome the security misconceptions that can arise when working from home, such as the belief that a "home network is too small to be at risk" (Autry, 2019). For example, due to the breach of a teleworkers home computer, the United States Postal Service (USPS) "suspended all remote work at one of its locations because of a breach of the employee database" compromising 800,000 workers (Weiss, 2014).

Much of the literature around teleworking has centered three data security risks: disclosure, modification, and destruction of data. The disclosure of data to unauthorized parties either intentionally or unintentionally is of great concern for teleworkers as the proximity to nonorganizational personnel is heightened in a home office environment. Personal devices and hardcopy information data can be used or stolen unwittingly (Yang, 2013). Furthermore, the proximity and likelihood of nonorganizational personnel engaging with data can possibly lead to the modification or destruction of materials. The home office work environment should be considered a threat containing "potentially unsecured, malware-infected, and compromised devices" (Perkins, 2018; Souppaya & Scarfone, 2016a) with unprotected wireless connections and communication channels, illuminating a larger obstacle facing organizations participating in telecommuting. The uncertainty of home office conditions makes securing an environment out of the scope of managements control. Providing employees with "laptops or desktops as well as creating secure configurations using the business' policies and procedures [can] help mitigate some of the home office risks" (Autry, 2019). Providing technology for employee use is not enough when data security relies so heavily on the compliance and behavior of teleworkers; organizations need to adopt a cybersecurity-focused culture that all employees abide by.

Personnel security risks require a prioritization by both leadership and employees at all levels, maintaining a level of personal responsibility and liability when working with organizational data. Should teleworkers disengage from personal responsibility "to follow the principles of management objectives… they can easily endanger the success of teleworking" (Autry, 2019). Two behavioral theories can be applied to better understand the necessity of employees opting into compliant behaviors and habits, Control Balance Theory (CBT) and Theory of Neutralization (ToN). CBT "is a general theory of deviance with constructs identified as constraints, control balance, situational provocation, and violation motivation to understand criminal behaviors" (Moody et al., 2018). When applied to cybercrime to understand deviance, it is "found that anonymity and deindividualization created by the reduction of the usual constraints increased the likelihood of computer crime" (Williams 2008). Removal from the office environment or constraints can create a relaxed state where employees disconnect from the organization's security measures out of complacency. This goes hand-in-hand with Theory of Neutralization, when employees "create rationalized reasons for making exceptions to rules, policies, or laws and violating the accepted norm" (Moody et al., 2018). Once employees have rationalized a behavior, acts against compliance can become the new standard or norm.

Appropriate training that accounts for these behavioral theories can help mitigate risks that arise from teleworking at the individual employee level. Adopting an organizational cybersecurity-focused culture at all levels can extend beyond technological capabilities and into individual responsibility, where the greatest security threat exists.

THE NEED FOR CHANGE: APPLYING ORGANIZATION DEVELOPMENT THEORY

For organizations to drive this culture change and prioritize cybersecurity throughout all levels, there needs to be a basic understanding of organization development theory as it pertains to culture change. Organization development (OD) theories and practices can make a significant positive contribution to cybersecurity by supporting a more proactive approach to risk assessment and management within organizations. In a world of uncertainty posed by constantly evolving cyber vulnerabilities and threats, it is important not only to respond effectively to crisis, but to better prepare our cyber systems to anticipate and adapt to such events. OD is a system-wide application and transfer of behavioral science knowledge to the planned development, improvement, and reinforcement of the strategies, structures, and processes that lead to organization effectiveness (Cummings and Worley, 2008: 1-2). OD examines the humanistic side of all organizational interactions and involvement by understanding the external environment, motivating change, increasing trust, and improving knowledge management. OD solutions are offered as next steps in motivating employee and organizational behavior to adopt a cybersecurity-focused culture.

Culture is the foundation for change, encompassing the ability to either promote or obstruct organizational transformation (Cummings and Worley, 2009). Culture is usually defined as the social or normative glue that holds an organization together. It expresses the values or social ideals and the beliefs that organization members come to share (Smircich, 1983). Discussed by Cummings and Worley (2009), culture is a process of social learning. According to Edgar Schein (1985), culture is the most difficult organizational attribute of change, outlasting organizational products, services, founders, leadership, and all other physical attributes of the organization. Schein's organizational model illuminates culture from the standpoint of the observer, who is described by three cognitive levels of organizational culture: artifacts and behaviors, exposed values, and basic underlying assumptions. At the first and most cursory level of Schein's model are organizational characteristics that can be seen, felt, and heard by the uninitiated observer

(Schein, 1985). This level is known as the organization's artifacts. Schein states that "[t]his is the observable level of culture and consists of behavior patterns and outward manifestations of culture perquisites provided to executives, dress codes, level of technology utilized and the physical layout of workspaces" (Schein, 1985: 14). Artifacts and behavior inform what a group is doing, but not why. Examples of artifacts and behaviors are the facilities, offices, furnishings, visible awards and recognition, dress code, and how each person interacts with each other and with organizational outsiders.

The following level deals with the imperceptible at first glance. Values underlie and, to a large extent, determine behavior, but unlike behaviors, they are not directly observable (Schein, 1985). Norms are expressions of values or unwritten rules that allow members of a culture to know what is expected of them in a wide variety of situations, including how to coordinate their interactions with others (Hatch, 2006). Values express preferences for certain behaviors or certain outcomes, while norms express behaviors accepted by others. Values and norms, once transmitted through the organization, establish the permanence of the organization's culture. Leaders at the senior executive level are often the source for the generation and re-infusion of an organization's ideology, articulation of core values, and specification of norms (Schein, 1985). At this level, company slogans, mission statements, and other operational creeds are often expressed, and local and personal values are widely articulated within the organization.

To profoundly understand culture, one most delve into the deepest level, the point of assumptions and beliefs. Schein (1985) contends that underlying assumptions grow out of values, until they become standardized and fall from consciousness. The deeper level of basic assumptions and beliefs includes: learned responses to the group's problems of survival in its external environment and its problems regarding internal integration; these learned responses are shared by members of an organization, are expressed in its unconscious operations, and tend to be overused in an organization's view of itself and its environment (Schein, 1985). That external environments affect organizational cultures is obviously related to the claim that organizations, in general, are affected by their environments (Gordon, 1991). These are the rudiments of culture that are unseen and not cognitively identified in everyday interactions between organizational members. Numerous yet unspoken rules exist outside of the conscious knowledge of the organization's members. Those with sufficient experience to understand this deepest level of organizational culture usually become acclimated to its attributes over time, thus reinforcing the invisibility of its existence. Schein (1985) found it remarkable that culture at this level was the underlying and driving element often missed by organizational behaviorists at the time. [It likely has been studied since he uncovered the phenomenon in 1985.]

Such change is deep, in that it entails shifts in the behaviors, beliefs, and values of members, and pervasive, in that it affects subsystems throughout the organization. If organizational members are to make sense of the organizational changes and to develop the new patterns of interaction necessary to achieve intended outcomes, knowledge must be transferred effectively by the designers of the change so that the "receiving units" are able to faithfully appropriate the "intentions of the change" (Poole and DeSanctis, 1994). Successful learning depends not only on formal, planned, organizational implementation activities but also on the capabilities of the existing and emergent social networks (Tenkasi and Mohrman, 2003).

Strong, willing leadership can serve as a precursor to organizational culture change. Culture may be invested deeply in the early stages of organizational development—tracks that may have been laid by strong founders and carried on down through time by top executives. Clear lines are defined as to what matters in the organization, processes by which things are accomplished and completed, and the mechanisms for handling problems. The investment of leadership transpires to the attitudes and beliefs of management and employees, creating a strong, aligned culture (Cummings and Worley, 2009); when employees see leaders prioritizing and participating in cyber-security activities, it influences employees own involvement (Huang 2019).

In terms of cybersecurity, this is where a great deal of change is needed: switching from a reactive to a proactive culture. The goal needs to be to reduce the vulnerabilities of complex, interconnected organizations and increase their resilience in order to increase their effectiveness and viability. Most organizations today are connected to other infrastructure in some way, especially in terms of cyber assets and systems. As eluded to earlier, "our increased interconnectedness, increased reliance on information technology and telecommunications, and globalization have created a more complex external risk environment" (Fisher, Norman, Klett, 2017).

In 2018, the National Initiative for Cybersecurity Education Working Group (NICE) developed a guidebook titled "Cybersecurity is Everyone's Job" as a resource for all organizations and all levels of employees. As stated in the introduction:

> *"We are the greatest vulnerability in any organization. In this era of persistent cyber threats, an organization will be secure only with the active participation of everyone... Each member of the group, from the newest employee to the chief executive, holds the power to harm or to help, to weaken or strengthen, the organization's security posture."* (NICE, 2018)

The guidebook specifically calls out "building a cyber-secure culture" in hopes to help organizations establish a successful cybersecurity posture (NICE, 2018). A cyber-secure culture is essential if organizations would like to build a resilient workforce (NICE, 2018). There are five key areas of consideration for building a cyber-secure culture described below:

- **Mindset.** *When we build awareness into the organizational culture, we increase our ability to address cyber risks.* (NICE, 2018)
- **Leadership.** *Leadership is the most important factor to influencing awareness and mindset. Leaders must embrace cybersecurity education, awareness and best practices.* (NICE, 2018)
- **Training and Awareness.** *Once leaders foster a cyber-secure culture, the next step is to implement employee awareness training. These programs build an understanding of risks, and—most importantly—provide specific steps for mitigating them.* (NICE, 2018)
- **Performance Management.** *For real cultural change to occur in cybersecurity preparedness, individual performance goals must align with the goals of the organization.* (NICE, 2018)
- **Technical and Policy Reinforcement.** *Just as physical access controls reinforce the mental awareness of a physical perimeter, so can password policies, multifactor authentication and mobile device management solutions reinforce security culture.* (NICE, 2018)

Considering, addressing, and implementing these five areas within an organization can help to form and then drive a cybersecurity-focused culture.

Motivating Employee Behavior Change Through Awareness and Training

Most organizations have some type of cybersecurity training programs for their employees. However, just because an organization requires cybersecurity training does not mean that employees are actively implementing the learned material in their daily jobs, or that they are adhering to organizational cybersecurity policies and procedures. Often, functionality trumps security, meaning that employees will "circumvent security in order to focus on meeting deadlines, making tasks easier, and speeding interaction with colleagues" (Pfleeger, Sasse, Furnham, 2014).

An environment of mindfulness must be created, both individual and collective, to increase awareness of what could go wrong and an understanding of the actions that could mitigate those effects (Pfleeger, Sasse, Furnham, 2014). This approach to security behavior takes a psychological approach rather than a technological approach, advocating understanding of the issues and problems from a user's perspective, and then determining how messages about behavioral change can be most effective (Pfleeger, Sasse, Furnham, 2014). Although technological approaches and solutions are helpful and beneficial in a multitude of ways, they are not as powerful as culture change, driven by the change in individual behaviors of employees. Kirsch and Boss (2007) support this as well, stating that their research results emphasized "the need for managers to focus on behavioral solutions in addition to technical ones in the context of information security." To enable good security behavior, we must be able to provide good motivators, and to do so, we must understand what employee's value and why (Pfleeger, Sasse, Furnham, 2014). It is also up to leadership and management to help drive security as a key issue in an organization, as research results showed "that managerial attention is needed to craft meaningful information security policies and to motive individuals to follow them" (Boss and Kirsch, 2007).

As articulated by Assante and Tobey (2011), "cybersecurity, by its very nature, is people – both defenders and attackers – engaged in a contest of playing out on a field of information systems and technology. Just as in any contest of this kind, success lies in identifying talent and continually developing and conditioning teams of professionals." Employees need to be trained more than once a year on cybersecurity policies and procedures for their organization. Cybersecurity should become a part of their daily routine – a key aspect of the organizational culture – continually growing, expanding, and improving employee abilities to defend against cyber-attacks.

Research conducted by McBride, Carter, and Warkentin (2012) for DHS looked at how individual personality traits shape cybersecurity policy violation intentions, specifically the Big Five Traits (openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism). The effort focused on establishing "statistically significant relationships between individual differences such as various personality profiles and policy violation intention motivations" to establish guidelines for protection protocols customized to meet the needs of diverse employees (McBride, Carter, and Warkentin, 2012). The research also looked at the role of sanctions on non-compliance and the employees' inherent nature to protect themselves from threats. Their results proposed three levels of cybersecurity training within organizations, with the ultimate goal being to develop customized protocols to help organizations achieve level three cybersecurity training (McBride, Carter, and Warkentin, 2012). These levels include the following, outlined in Table 3:

TABLE 3
PROPOSED TRAINING STRATEGY

Level One	*This is the status quo. Currently, most organizations provide one training protocol to all employees. The protocol may include a discussion of security threats (if you don't follow this policy you may lose your data) and/or organizational sanctions (if you don't follow this policy you will be reprimanded).* ***However, this approach does not account for individual differences.***
Level Two	*A few organizations may utilize a training protocol that leverages the direct effects of personality factors and/or the seven situational factors. For example, a training protocol in an organization where the culture emphasizes the importance of following the rules, may indicate the importance of following the cybersecurity policy and highlight the consequences of noncompliance.* ***This approach may incorporate a few individual differences, but it does not account for the interactions between diverse individual factors.***
Level Three	*This represents the next step for research on cybersecurity compliance training development. This approach would explore the combined effects of the Personality Factors and/or the seven situational factors. It would take into account how various personality traits interact with individual perceptions of security threats and sanctions. The results of this study can be used to develop a set of employee profiles that categorize organizational employees based on their personality types and perceptions of cybersecurity threats and sanctions. In order for organization to implement these customized training elements to organizational employees, individual employees would need to complete a brief questionnaire before beginning a training program that assesses his Big Five personality traits and his perceptions of cybersecurity threats and organizational sanctions. Then, based on his responses and the findings, a set of customized training protocols could be developed to target diverse profiles of individuals.* ***As a result, each employee would receive cybersecurity training that targets his specific personality traits and unique cybersecurity perceptions.***

McBride, Carter, and Warkentin, 2012

What works for one employee in terms of training, may not work for another. For employees to learn and implement necessary skills and strategies as part of cybersecurity training programs, various approaches may be needed to reach all employees.

Similarly, work by He and Zhang (2019) focused on recommendations for successful cybersecurity training and awareness programs for organizations, stating that "to improve employees' security behavior, there is an urgent need to explore the most common issues in existing security training and awareness programs and to investigate ways in which organizations can make the training more successful." He and Zhang present a variety of best practices based on their research, outlined below in Table 4:

TABLE 4
BEST PRACTICES FOR IMPLEMENTING SUCCESSFUL CYBERSECURITY TRAINING PROGRAMS

Attributes	Best Practices
Accountability	*Emphasize how destructive lack of knowledge and negligence could be; instead of highlighting who failed the assessment, highlight who did the right thing; forward suspicious emails to IT or report an unsuccessful penetration attempt; accountability does not mean that the company focuses on punishing those who do not comply; it should reward those who do. Ensure that cybersecurity is a part of every employee's performance goals.*
Fun	*Entertain: begin your training sessions with few relevant but scary cybersecurity statistics; find engaging content; create entertaining literature; incorporate funny and relatable scenarios to keep your employees' attention, while helping them understand why cybersecurity is vital; gamify the security awareness training program, so that points are amassed; use a leaderboard or prizes; turn a mundane training into a game.*
Hands-on	*Have a point of contact or a shared email box where employees can forward suspicious links; hold a contest among employees to see who can spot the most phishing emails; similar activities can target mobile devices or laptops by asking employees to download unauthorized software; include role-playing and testing.*
Interactivity	*Tell some stories; encourage employees to ask questions and to share experiences; encourage employees to share the material with their friends and family; ask employees questions related to their specific industry, operational area, and even job type; ask what they have experienced and what they did about it; persuade employees to share what they have learned; roleplay phishing or other security scenarios; use stories and videos.*
Just-in-time Training	*Create material for training employees as they join the company; when employees fall for test emails, tell them that they failed and that they need to read materials or watch a video on what key points they missed.*
Personalization	*Conduct social engineering testing such as the spear phishing test; use examples from real life and cases/ scenarios from recent current events, real security incidents, breaches, and ransomware; ask questions about employees' personal cybersecurity concerns related to their email, social media and smartphone use.*
Reinforcement	*Run assessments and micro-trainings at regular intervals; be aware of new and emerging threats; send out regular email blasts about threats; create a monthly newsletter or blog to keep security on the employees' minds; quiz your staff throughout the year to see who is paying attention.*
Relevancy	*Provide curricula tailored to the roles and responsibilities of the individuals partaking in the curriculum; provide department/application-specific advice to explain why, in*

	simple terms that your employees will understand; develop progressive topic driven modules that have been customized for specific roles.
Reward	*Give out incentives like candy or gift cards when someone answers a question posed to the group; rewards can be simple gift cards or a more complex points program which can be redeemed for prizes.*

He and Zhang, 2019

He and Zhang (2019) also propose four key recommendations for improved performance for enterprise cybersecurity training an awareness programs: (1) relating cyber awareness to employees' personal lives; (2) reinforcing security procedures and guidelines; (3) instilling a "relaxed alert" state of employees; and, (4) minimizing security fatigue for employees. The focus should be on creating a cyber-secure workforce, which can only be done by improving individual employee behavior through motivational techniques.

Checklists provided for guiding cybersecurity in organizations are a strong starting point, but as demonstrated in the research outlined here, there is much more beyond the basic implementation to enhance an organization's security posture and work towards a cyber-secure culture. Organizations should consider how people not only learn information, but how they implement what they have learned into their daily jobs. It is also important to encourage ongoing learning and engagement enterprise-wide to ensure cybersecurity sustainability and avoid a culture of complacency. From the reviewed research, the information below provides recommendations for moving beyond the basic cybersecurity checklists and driving towards a strong, sustainable cybersecurity-focused culture.

PREPARING FOR CYBER THREAT: NEAR-TERM AND LONG-TERM ACTION

There are various checklists readily available to organizations that provide ideas for enhancing cybersecurity within organizations simply found by searching the Internet, for example:

- DHS Office of Science and Technology Cybersecurity Resources: https://www.dhs.gov/science-and-technology/cybersecurity-resources
- DHS CISA Insider Threat Mitigation: https://www.cisa.gov/insider-threat-mitigation
- Federal Communications Commission Cybersecurity and Network Reliability: https://www.fcc.gov/general/cyber-security-and-network-reliability, and Cybersecurity for Small Business: https://www.fcc.gov/general/cybersecurity-small-business

These checklists and resources provide a solid foundation for strengthening cybersecurity programs, focused on both external and internal threats. Often, these lists include employee training as a key aspect, along with policies and procedures, and planning, which are all critical for a strong cybersecurity program, as well as other resources to support organizations in maintaining operations and achieving their missions. However, following these checklists are not the only solution to a strong cyber defense.

In addition to leveraging pre-existing resources to strengthen cybersecurity programs and to drive organizations toward enhanced cybersecurity postures, we propose the three following long-term key actions: create a culture of cybersecurity awareness; motivate employees to change their behaviors through training and awareness programs; and, encourage employees to take ownership in their roles to prevent cyber-attacks.

Create a Culture of Cybersecurity Awareness

As explained by Smircich (1983), organizational culture expresses the values or social ideas and the beliefs that organization members come to share. For cybersecurity to become ingrained in the organization and prioritized by all, a culture of cybersecurity awareness must be created. Culture change is difficult, but the activities outlined below can help drive towards enterprise-wide culture change overtime to enhance cybersecurity posture.

- Ensure leaders are open and supportive of cybersecurity being an organizational priority in a way that is visible to employees. Strong, willing leadership can serve as a precursor to organizational culture change. The investment of leadership transpires to the attitudes and beliefs of management and employees, creating a strong, aligned culture (Cummings and Worley, 2009).

- Drive security as a key issue in the organization from the top-down; managerial attention is needed to craft meaningful information security policies and to motive individuals to follow them (Boss and Kirsch, 2007).
- Consider establishing a successful cybersecurity posture and culture by focusing on five key areas: mindset, leadership, training and awareness, performance management, and technical and policy reinforcement (NICE, 2018).

Motivate Employees to Change Their Behaviors

Nothing will change in an organization if employees are not willing, or able, to sustainably change their individual behaviors. Providing employees with the correct tools and resources to learn how to change their behaviors is key. Using a variety of approaches to do this can also increase the likelihood of success that employees will adopt the desired cybersecurity-focused behaviors.

- Take a psychological approach to cybersecurity training and awareness instead of a strictly technological approach (Pfleeger, Sasse, Furnham, 2014).
- Create an environment of mindfulness, both individual and collective, to increase awareness of what could go wrong and an understanding of the actions that could mitigate those effects (Pfleeger, Sasse, Furnham, 2014).
- Identify and utilize different ways to motivate employees throughout the organization to adopt and implement effective cybersecurity measures (Pfleeger, Sasse, Furnham, 2014).
- Explore the most common issues in existing security training and awareness programs and investigate ways in which organizations can make the training more successful (He and Zhang, 2019).

Encourage Employees to Take Ownership in Their Roles to Prevent Cyber-Attacks

Employees should be reminded that cybersecurity is everyone's job; there is no single entity responsible for cybersecurity within an organization. Every individual needs to embrace the mindset that their actions within the organization can either help or harm the entire institution.

- Consider developing different approaches to cybersecurity awareness and training, taking into account different personality traits and approaches to learning (McBride, Carter, and Warkentin, 2012)
- Minimize employee complacency, encourage proactivity within the organization. Examples such as the Equifax hack demonstrated the detriment that can occur when a culture of complacency exists (Johnson, 2018).

Addressing the long-term actions listed above, combined with the near-term actions called out in the various checklists mentioned can strike a successful balance in driving towards a cybersecurity-focused culture. Although there is no single solution to implementing strong cybersecurity within organizations, these actions can serve as a starting point to enhancing security posture through all employees in all organizations.

CONCLUSION

This initial research is only the first step in advancing cybersecurity culture within organizations. There is a great deal of work that can be conducted to help organizations advance their cybersecurity posture and build a stronger understanding of existing techniques, best practices, and resources moving forward. Our goal for future research is to focus on the cultural shift needed to address both the external and internal cyber threats faced by organizations through enhanced cybersecurity. One specific area of follow-on research that we hope to explore in greater detail is insider threat. This topic continues to gain attention as it is a threat faced by every single organization. Similar to the work conducted by McBride, Carter, and

Warkentin (2012) focusing on personality traits and tailored approaches to cybersecurity training, we would like to explore personality trait commonalities and behavioral indicators among historical insiders who carried out detrimental activities or attacks on their organizations. Our research aims to leverage artificial intelligence and machine learning to combat insider threat. We would also like to enhance the research surrounding the use of technological solutions in parallel with behavior techniques and approaches.

Our world is continually changing, with new threats and challenges arising each day, in both our personal and professional lives. We can mitigate these threats by building a cybersecurity-focused culture throughout the organization, at all levels so that all employees understand and accept that cybersecurity is a priority and they can serve as part of the cyber defense. Organizations can also leverage existing resources, such as checklists, trainings, and best practices to enhance their cybersecurity posture. Although employees are the greatest vulnerability, they are also the greatest defense to mitigating cyber-attacks when given the tools and resources needed. To effectively raise the bar on enhancing cybersecurity, we need to create a cybersecurity-focused culture to help mitigate the cyber-risks that plague organizations today.

REFERENCES

Accenture. (2019). *Ninth Annual Cost of Cybercrime Study*. Retrieved from https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Assante, M.J., & Tobey, D.H. (2011). Enhancing the cybersecurity workforce. *IT Professional*, *13*(1), 12-15.

Autry, T. (2019). *Secure IoT compliance behaviors among teleworkers* (Order No. 27544236). ProQuest One Academic (2313671125). Retrieved from http://ezproxy.neu.edu/login?url=https://search-proquest-com.ezproxy.neu.edu/docview/2313671125?accountid=12826

Bada, M., Sasse, A., & Nurse, J. (2015). *Cyber security awareness campaigns: Why do they fail to change behavior?* International Conference on Cyber Security for Sustainable Society. Bass.

Batteau, A.W. (2011). Creating a culture of enterprise cybersecurity. *International Journal of Business Anthropology*, *2*(2), 36-47.

Bergen, P., & Hoffman, B. (2010, September). *Assessing the terrorist threat, a report of the Bipartisan Policy Center's National Security Preparedness Group*. Bipartisan Policy Center.

Brown, C., Smith, P., Arduengo, N., & Taylor, M. (2016). Trusting telework in the federal government. *The Qualitative Report*, *21*(1), 87-101. Retrieved from https://nsuworks.nova.edu/tqr/

Brown, D. (2020). Cyberwar with Iran: How vulnerable is America? *USA Today*. Retrieved from https://www.usatoday.com/story/tech/2020/01/03/how-much-damage-could-iran-cyber-attacks-do/2803599001/

Cisco Annual Cybersecurity Report. (2018). *Cisco 2018 Annual Cybersecurity Report*. Retrieved from https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

Cisco. (n.d.). *What are the most common cyber attacks?* Retrieved from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Cummings, T., & Worley, C.G. (2008). *Organization development and change* (9th Edition). Minneapolis, MN: West Publishing Company.

Cummings, T.G., & Worley, C.G. (2009). *Organization development and change* (9th Edition, p.772). South Western Cengage Learning, Mason, Ohio, USA.

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7.

Dengler, R.A. (2006). *Fast-acting OD intervention for expedited organization culture change: A quantitative evaluation of a field experiment in a large utility undergoing an intentionally violent transformational change*. ProQuest. Retrieved November 19, 2010, from Dissertations and Theses database.

DHS CISA. (2019a). *Combating Cyber Crime*. Retrieved from https://www.cisa.gov/combating-cyber-crime

DHS CISA. (2019b). *Insider Threat Mitigation*. Retrieved from https://www.dhs.gov/cisa/insider-threat-mitigation

DHS. (2019). *Cybersecurity*. Retrieved from https://www.dhs.gov/topic/cybersecurity

Federal Communications Commission (FCC). *Cybersecurity for small business*. Retrieved from https://www.fcc.gov/general/cybersecurity-small-business

Fisher, C.J. (2000, Summer). Like it or not...culture matters. *Employment Relations Today*, pp. 43–52.

Fisher, R., Norman, M., & Klett, M. (2017). Enhancing infrastructure resilience through business continuity planning. *Journal of Business Continuity & Emergency Planning*, *11*(2), 63-172.

Fisher, R., Wood, J., Porod, C., & Greco, L. (2020). Evaluating cyber risk reporting in U.S. financial reports. *Journal of Cybersecurity*, *3*(3), 275-286.

Fligstein, N. (1991). The structural transformation of American industry: an institutional account of the causes of diversification in the largest firms. In W. Powell, & P. DiMaggio (Eds), *The New Institutionalism in Organizational Analysis*. Chicago, IL, University of Chicago Press.

Garamone, J. (2018). *Cyber tops list of threats to U.S., Director of National Intelligence Says*. U.S. Department of Defense (DOD) News. Retrieved from https://www.defense.gov/Explore/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/

Gordon, G.G. (1991). Industry determinants of organizational culture. *Academy of Management Review*, *16*(2), 396–415.

Hatch, M.J. (2006). *Organization theory* (2nd Edition). Oxford, NY: Oxford University Press.

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249-257.

Hoffman, T. (2004, June 15-17). *Why is the intelligence community so different (difficult?) to redesign?* Paper presented at the SOG-conference, University of British Colombia, Vancouver.

HSAC. (2009, September). *Homeland Security Advisory System: Task Force Report and Recommendations, Homeland Security Advisory Council*. U.S. Department of Homeland Security.

HSPD-3. (2002, March 2002). *Homeland Security Presidential Directive 3: Homeland Security Advisory System*, President George W. Bush, White House.

Huang, K., & Pearlson, K. (2019). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. *ScholarSpace*, *6400*.

IBM. (2018). *Learn about cyber attacks and how to defend against them*. IBM Services. Retrieved from https://www.ibm.com/services/business-continuity/cyber-attack

International Organization for Standardization (IS0). (2012). ISO/IEC 27032:2012 [ISO/IEC 27032:2012] *Information technology — Security techniques — Guidelines for cybersecurity*. Retrieved from https://www.iso.org/standard/44375.html

Johnson, D.B. (2018). *'Culture of cybersecurity complacency' blamed for 2017 Equifax hack*. FWC: The Business of Federal Technology. Retrieved from https://fcw.com/articles/2018/12/10/equifax-house-oversight-reports.aspx

Kaspersky Lab. (2017). *Ready or not: Balancing future opportunities with future risks, a global survey into attitudes and opinions on IT security*. Retrieved January 13, 2020, from https://media.kaspersky.com/documents/business/brfwn/en/The-Kaspersky-Lab-Global-IT-Risk-Report_Kaspersky-Endpoint-Security-report.pdf

Kirsch, L., & Boss, S. (2007). The last line of defense: Motivating employees to follow corporate security guidelines. *International Conference on Information Systems 2007 Proceedings*.

Kotter, J., & Heskett, J. (1992). *Corporate culture and performance*. New York: The Free Press.

Kuhn, A. (1974). *The logic of social systems*. San Francisco: Jossey-Bass.

March, J.G., & Olsen, J.P. (1989). *Rediscovering institutions: The organizational basis of politics*. New York: The Free Press.

McBride, M., Carter, L., & Warkentin, M. (2012). *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cyber Security Policies*. (Prepared by RTI International – Institute for Homeland Security Solutions under contract 3-312-0212782.)

Moody, G.D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*, 285-311.

Morgan, S. (2016). *Top 5 Industries at Risk of Cyber-Attacks*. Retrieved from https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#7cb238ff715e

Morgan, S. (2019). *2019 Official Annual Cybercrime Report*. Retrieved January 13, 2020, from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Myers, J., & Whiting, K. (2019*). These are the biggest risks facing our world in 2019*. World Economic Forum. Retrieved from https://www.weforum.org/agenda/2019/01/these-are-the-biggest-risks-facing-our-world-in-2019/

National Initiative for Cybersecurity Education Working Group (NICE). (2018). *Cybersecurity is everyone's job. National Institute of Standards and Technology*. Retrieved from https://www.nist.gov/system/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf

O'Toole, J., & Bennis, W. (2009, June). What's needed next: A culture of candor. *Harvard Business Review*.

Pearce, C.L. (2004). The future of leadership: combining vertical and shared leadership to transform knowledge work. *Academy of Management Executive*, *18*(1).

Perkins, B. (2018). *9 hidden risks of telecommuting policies*. Retrieved from https://www.cio.com/article/3261950/hiring-and-staffing/hidden-risks-of-telecommutingpolicies.html

Pfleeger, S.L., Sasse, M.A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Homeland Security and Emergency Management*, *11*(4), 489-510.

Poole and DeSanctis. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. *Organization Science*, *5*(2), 121–147.

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *2014 Information Security for South America*, pp. 1-7.

Schein, E.H. (1985). *Organizational culture and leadership.* San Francisco, CA: Jossey-Bass.

Shred-it. (2018). *State of the Industry Report, North America, Information security*. Retrieved January 13, 2020, from https://www.shredit.com/getmedia/b5de58fd-7e17-4d18-b718-9eca8d0665a6/Shred-it-2018-North-America-State-of-the-Industry.aspx

Smircich, L. (1983). Concepts of culture and organizational analysis. *Administrative Science Quarterly*, *28*, 339–358.

Souppaya, M., & Scarfone, K. (2016a). *Guide to enterprise telework, remote access, and bring your own device (BYOD) security*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

Steinberg, S. (2019). *Cyberattacks now cost small companies $200,000 on average, putting many out of business*. Retrieved January 13, 2020, https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

Taylor, C. (2017). *Fail to plan, plan to fail*. Retrieved from http://www.govtech.com/library/papers/Forrester-Report-How-to-Secure-Your-IoT-and-OTEnvironment-93957.html

Tenkasi and Mohrman. (2003). The role of networks in fundamental organizational change: A grounded analysis. *Journal of Applied Behavioral Science*, *39*(3), 301–323.

The Council of Economic Advisers. (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

The Heritage Foundation. (2020). *The growing threat of cyberattacks*. Retrieved from https://www.heritage.org/cybersecurity/heritage-explains/the-growing-threat-cyberattacks

Weiss, E. (2014). *Post office suspends telecommuting due to breach*. Retrieved from https://www.usatoday.com/story/tech/2014/11/12/us-postal-service-suspendstelecommuting-breach-vpn/18915317/

Widup, S., Spitler, M., Hylender, D., & Bassett, G. (2018). *2018 Verizon Data Breach Investigations Report*. Retrieved from https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report

Williams, K.S. (2008). Using tittle's control balance theory to understand computer crime and deviance. *International Review of Law, Computers & Technology*, *22*(1-2), 145-155. doi:10.1080/13600860801925086

Yang, H., Zheng, C., Zhu, L., Chen, F., Zhao, Y., & Valluri, M. (2013). *Security risks in teleworking: A review and analysis.*