8-2021

CYBERSECURITY: CREATING A CYBERSECURITY CULTURE

Steven Edward Ogden
California State University - San Bernardino

CYBERSECURITY: CREATING A CYBERSECURITY CULTURE

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems Technology

by

Steven Ogden

August 2021

CYBERSECURITY: CREATING A CYBERSECURITY CULTURE

A Project

Presented to the

Faculty of

California State University,

San Bernardino

by

Steven Ogden

August 2021

Approved by:

Benjamin Becerra, PhD, Committee Chair, Information & Decision Sciences

Conrad Shayo, PhD, Committee Member

Jay Varzandeh, PhD, Dept. Chair, Information & Decision Sciences

ABSTRACT

Human error has been identified as one of the highest contributing factors to successful cyber-attacks and security incidents that result in data leaks and theft of sensitive information. Human error has been caused by employees not behaving securely when interacting with information systems. This culminating experience project investigated how a cybersecurity culture can be developed to address the human error problem. The research was based on several key questions that focus on influencing factors of human behavior and best practices that have been used to develop a cybersecurity culture so that employees engage in secure behaviors. Social Cognitive Theory was used to guide research focusing on environmental and cognitive factors that influence human behavior and best practices for developing a cybersecurity culture were identified through recent case studies. Key findings include: 1) environmental factors such as social-proximity, subjective norms, and descriptive norms, 2) cognitive factors such as self-efficacy, knowledge, and experience, and 3) several different best practices. Based on the results, this study provides recommendations to the US government for building a cybersecurity culture.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE:

INTRODUCTION

Purpose of Study

The government industry was one of three main industries where 95% of all records were breached (Milkovich, 2020). Cybercrime has drastically increased over the years and more so since the COVID 19 pandemic took hold in the United States in early 2020 (Monteith et al., 2021). During the first five months of 2020, the number of reported cybercrimes matched those during the entire year of 2019 (Monteith et al., 2021). The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) also tracks the number of reported cybercrimes and there was a notable difference between 2019 and 2020. There were 467,361 complaints and an estimated $3.5 billion in reported losses in 2019 as compared to 791,790 complaints and an estimated $4.1 billion in reported losses in 2020, nearly a 70% increase in complaints (Federal Bureau of Investigation, 2021). A recent report by Cyberedge Group (2021) concluded that an increasing number of organizations are suffering from successful cyberattacks over the last 5 years as shown in figure 1.

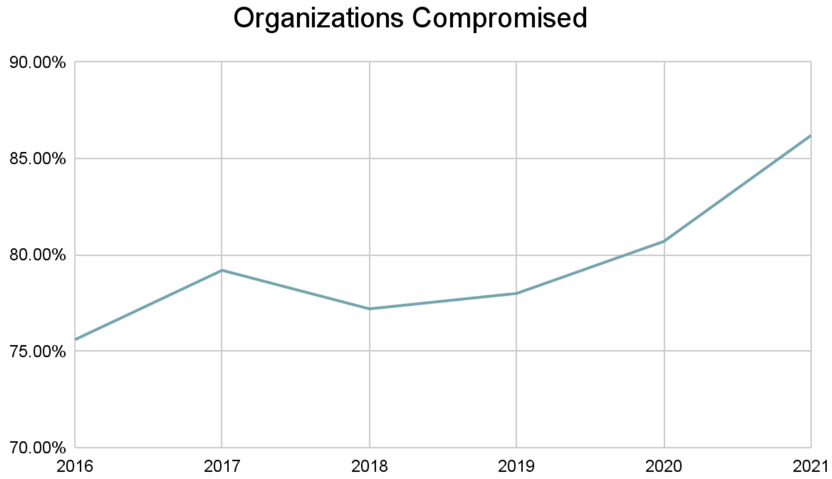

Figure 1.1 Percentage of Organizations Compromised from 2016-2021

Advancements in technology are being leveraged by criminals to commit cybercrime against all types of entities, especially the United States Federal Government (herein referred to as “government”), focusing on data destruction, stealing proprietary information, financial gain, and many others (Eggers, 2021; Olejarz, 2015). An understanding of why cyberattacks and cyber incidents are occurring is necessary before developing solutions to the problem.

Common themes have appeared that describe reasons why these events have been occurring so much in recent years that have been identified in recent publications: human error, environment complexity, and restricted information sharing, and insufficient budgets (Macak et al., 2020; Office of the Secretary of Defense, 2015; Sen, 2018; Ashford, 2017). The 2021 Cyberthreat Defense report also provided several of the most common reasons why organizations are unable to successfully defend their systems. Figure 2 shows that the main two reasons are: (a) Low Cybersecurity awareness, and (b) Lack of Skilled Personnel (Cyberedge Group, 2021).

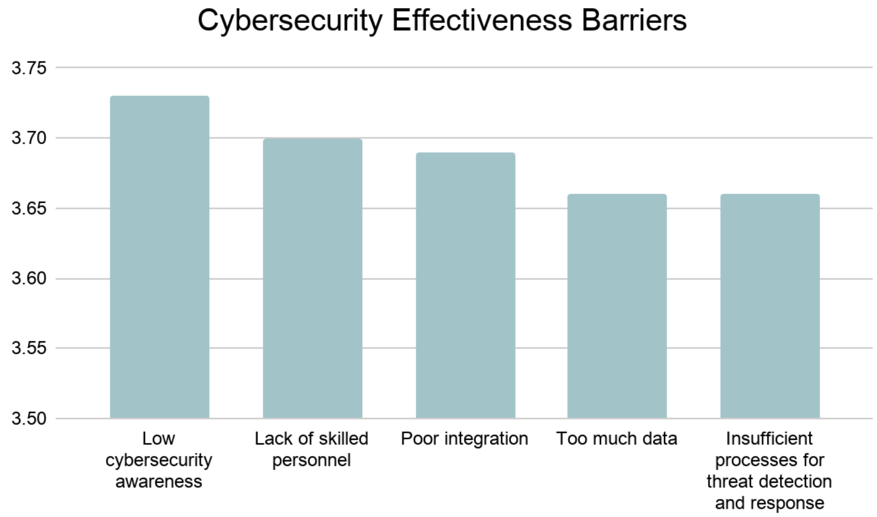

Figure 1.2 Cybersecurity Effectiveness Barriers

According to Bruce Schneier (2000), a cybersecurity expert, people are referred to as the weakest link in security and are repeatedly responsible for system failures. System failures can be caused by performing tasks incorrectly or by being the victim of a cyberattack that introduces malicious actors into the information system. The human problem has not made much progress since then and remains as the top threat to the government since 2014 (SolarWinds, 2020). A recent report to Congress concluded that the total number of cyber related incidents within the government caused by human error increased nearly 30% from fiscal years 2018 to 2019, accounting for nearly 50% of all cyber incidents (Executive Office of the President of the United States, n.d.). A significant increase in this category should be alarming as it indicates a serious problem with peoples' interaction with information systems. Human error is often a result of a lack of awareness, distractions, or natural psychological flaws and has been blamed for 95% of data breaches (Huseyin, 2019; Milkovich, 2020; Pollock, 2017).

Several recent events involving human error include the SolarWinds hack resulting from a poor password, Hillary Clinton's disclosure of classified information, and the 2016 presidential election hack via a phishing campaign (Datta, 2021; Temple-Raston, 2021; Fessler & Martin, 2017). Using a poor password can be argued as poor organizational policy; however, it could also be argued that if the administrator was aware of the vulnerability, the situation could have been avoided and the system less likely compromised if a stronger password was used (Scarfone & Souppaya, 2009). Several government agencies downloaded the compromised software from SolarWinds that ultimately compromised their networks allowing adversaries to infiltrate their systems (Whitaker, 2021). To this day, the SolarWinds hack is known to be one of the most complex and destructive hacks to have ever happened (Whitaker, 2021).

The disclosure of classified information from Clinton's email server was found not to be malicious but was a result of 38 individuals not properly securing classified information (U.S. Department of State, 2019). Had these individuals been aware that their actions were not complying with security policies, it is likely they would have used the appropriate methods to communicate sensitive information. Similar to the phishing emails used in the presidential election hack (Fessler & Martin, 2017), email recipients may not have been aware of the illegitimacy of the emails or how to identify them based on the detection difficulty (Steves et al., 2019). Moreover, in 2019, the United States Department of Agriculture (USDA) reported 36 improper use cases consisting of unauthorized software installations, viewing of forbidden content, and more (U.S. Department of Agriculture, 2019). Thus, collectively, this suggests that people that lack cyber awareness may have the tendency to engage in dangerous activities that pose a great risk to the organization.

Statistics and recent events demonstrate that people who lack cyber awareness may be a serious problem and can jeopardize the integrity and security of information systems. Employees throughout the entire organizational structure pose a risk, from line workers to senior leaders. Each employee can be targeted for cyberattacks or exercise poor cybersecurity practices that result in unwanted outcomes. Proofpoint (2019) reported that lower levels of management and front line workers were targeted more frequently with phishing attacks and email-based malware than senior leaders. However, in 2020, a study shows that top level executives are twelve times more likely to be pursued as a target rather than the average employee (Aon, 2020). Executives are high profile targets because they often have access to valuable company information but (Aon, 2020). As the literature highlights people as the weakest link and potentially being a top threat to cyber defense, the government will remain vulnerable if the human factor is not addressed and resolved (U. S. Government Accountability Office, 2021).

While there is no single solution for increasing cybersecurity and mitigating risks, the government should also focus on non-technical solutions, rather than just technical solutions, to have the best chances at success (Donalds & Osei-Bryson, 2020). Developing a cybersecurity culture has been recognized as the best approach to address human factors as the weaknesses within cybersecurity (Gcaza & Solms, 2017). Policy compliance is an aspect of cybersecurity culture that identifies acceptable behaviors detailing how employees shall interact with the organization's information system. Policy compliance has shown to reduce risk and minimize security-related incidents since individuals behave accordingly (Li et al., 2019; Veiga, 2016). Therefore, the objective of this project is to explore the importance of a cybersecurity culture and how it can be used to mitigate risks while focusing on policy compliance. The specific questions the project will focus on include:

- How can the government create a cybersecurity culture? What environmental and cognitive factors may have an influence on individuals to exercise compliant behavior?
- What are the best practices we can learn from? What challenges may the government be faced with when implementing cybersecurity culture best practices?

- Based on the best practices and challenges discovered, what recommendations can be made for the government?

Organization

This project is organized as follows: Chapter 2 will provide a background on cybercrime and cyberwarfare within the government along with challenges that the government is currently faced with. Chapter 3 will describe the methodology used for research. Chapter 4 will review the results. Chapter 5 will provide recommendations for the government, limitations, and a conclusion.

CHAPTER TWO:

CYBERCRIME IN GOVERNMENTS

Cybercrime and Cyber Warfare

Cybercrime is the act of carrying out criminal activities using technological devices, such as computers, as the primary instrument to attack other networks or information systems (Kierkegaard, 2005). Cybercrime is often performed by professionals within the industry, and they spend a lot of time organizing their activities before execution (Latto, 2020). Organized cybercrime involves learning more about the potential victim; what their weaknesses and vulnerabilities are. Gathering this type of information can increase the success of an attack and is a critical step to carry out. Cyber warfare is similar to cybercrime but it involves nation-states or international organizations that attack other nation's information systems. A term used to describe those who participate in cybercrime is cyber threat actors (CTAs). The following table will be used to define the different types of CTAs and their motivations to conduct cybercrime (Center for Internet Security, n.d.):

Table 1: List and Definitions of Cyber Threat Actors

CTAs	Definition	Motivation
Cybercriminals	Individuals or groups that are long-term threats conducting cyberattacks.	Focused more on financial gain than anything else.

Insiders	Employees or individuals that have access to information systems within an organization.	Financial gain but also have a vendetta to seek revenge on their employer or former employer.
Nation-state actors	A nation-state (i.e., Russia and China) or state-sponsored organizations that target other organizations to steal information or destroy assets.	espionage, political gain, economic gain, or military power
Hacktivists	Criminal hackers that share ideological values, usually seek to make a change.	Political or social ideologies
Cyberterrorists	Terrorist groups or individuals that have the same intention to cause massive damage or fear by using technology to carry out their actions.	Financial gain, political ideologies, or espionage.

CTAs use different methods to conduct criminal activities to include malware, hacking, identity theft, and scams (Michael & Sammons, 2017). There are several different categories of cybercrime: economic crimes, content-related offenses, intellectual property (IP) crimes, and privacy offenses (Kierkegaard, 2005). Economic crimes consist of traditional hacking, computer fraud, computer espionage and forgery, and computer destruction; content-related offenses include illegal content of child sexual abuse and racial statements; IP crimes include theft of copyrighted material, trade secrets, and violations of trademarks; and privacy offenses are an illegal collection of people's personal information to also include storage and distribution without proper consent (Kiener-manu, 2019; Kierkegaard, 2005). For example, the SolarWinds and presidential campaign hacks would be classified as an economic crime and Clinton’s disclosure of classified information would be considered a privacy offense. Research has shown that the government suffers from economic crimes and privacy offenses more than the other types.

The United States Government as a Target

The government is one of the largest organizations in the world with roughly 456 government agencies and departments that employ over two million civilian employees and nearly five hundred thousand active military members (Cancian, 2019; Jennings & Nagel, 2020). The number of employees greatly increases its threat landscape since employees remain one of the highest vulnerabilities and a desirable target for CTAs to exploit. Government agencies are known to have high-value assets, sensitive information, and large budgets that gain the attention of CTAs for obvious reasons given their motivations. For example, the Department of Defense (DoD) is one of the largest government entities possessing high-value assets such as military aircraft and critical infrastructure. According to Armerding (2019), a recent report released by the Government Accountability Office (GAO) determined that DoD weapon systems have critical vulnerabilities allowing adversaries to gain undetected control. Attacks on these assets have the potential to do damage similar to that of a nuclear weapon (Andres, 2017). While there are extreme risks for adversaries to attack the government, they believe the benefits outweigh the potential consequences which is why the government must take action to protect its infrastructure (Andres, 2017).

Michael McCaul said in a congressional hearing that government organizations are being attacked in several ways: cyber warfare, denying service to critical infrastructure, appropriating intellectual property, conducting spy operations, and accessing personally identifiable information (PII) (America is Under Cyber Attack, 2012). Nation-states are trying to advance their developments in an effort to strategically compete with the government's capabilities since they are behind in the competition (America is Under Cyber Attack, 2012). The government is not just a target for espionage and financial gain. Nation-state actors are not always in the game to steal information and cause damage; they have also been known to compromise systems just to demonstrate and inform the world of their capabilities (Sobers, 2020).

China, for instance, is a nation-state and implicated as one of the government's top threats as they seek to target their infrastructure for espionage and theft to advance their cyber and technological capabilities (Office of the Director of National Intelligence, 2021). The NSA has publicly announced that Chinese state-sponsored cyber actors are scanning and targeting government networks (Musto, 2020). A group of Chinese hackers were attributed to the cyberattack that was conducted on the Office of Personnel Management government agency (Fruhlinger, 2020). OPM is essentially the government’s human resource agency. As the human resource agency, they have personnel files for every government employee that consist of social security numbers, fingerprints, financial information, and more PII which is a form of sensitive information. The attack on OPM resulted in over twenty-one million records being breached. Such information may provide China with the ability to gain a better understanding of government operations and special programs. The data breach is suggested to place a target on American lives for extortion by the Chinese government to potentially conduct additional espionage missions (Gootman, 2016).

Russia, another nation-state, is considered a top threat to the government (Office of the Director of National Intelligence, 2021). They have highly advanced cyber capabilities that they utilize to collect intelligence from other governments and conduct offensive cyber operations (Bowen, 2021). The goal of Russia’s cyber warfare is thought as a means to avoid war while attempting to affect political and economic outcomes around the world (Connell & Vogler, 2017). Russia has been accused of conducting cyber warfare on government organizations for many years. The 2016 United States presidential election was hacked by Russia to influence the election outcomes and sabotage public trust in the democratic process (Connell & Vogler, 2017). Russia also stole emails and other sensitive documents that can provide intelligence for decision making but they are also known to commit espionage so they can leak the information to the public (Bowen, 2021; Connell & Vogler, 2017).

North Korea is known for attacking government networks in pursuit to steal and launder money to fund their development of nuclear weapons but also for espionage (Sanger & Perlroth, 2020). Since 2017, North Korea has increased their network activity nearly 300% and is known to have 7,000 cyber warriors to aggressively carry out their missions (Office of Information Security, 2021). They commonly use spearphishing attacks directed at DoD and Department of State employees attempting to steal sensitive information (Cluley, 2021; U.S. Department of Justice, 2021). More recently, North Korea has been accused of targeting COVID-19 vaccine developers to steal research data and has sent COVID-19 themed phishing emails to millions of people hoping to steal sensitive information and financial data (Office of Information Security, 2021). Reports indicate that North Korea has been able to steal more than $300 million dollars since from 2019 to late 2020 (Lederer, 2021). Government entities remain a top target for North Korea as well as other targets: aerospace, healthcare, and banking.

The government is becoming increasingly more dependent on technology which inherently creates more vulnerabilities as new technologies become integrated into their systems. Nation-states have demonstrated that they possess the cyber capabilities to hack some of the most secure systems by exploiting vulnerabilities. These exploitations have resulted in millions of dollars in damages and damage the integrity of our national security. Nation-states have proven they are motivated and determined to continue engaging in cyber warfare in their mission to boost military capabilities at the expense of the government. These attacks have the potential to cause serious damage which is why it is imperative that the government seeks new ways to mitigate these threats. National security can be greatly impacted if cyberattacks on government systems continue while not implementing a better solution (Executive Office of the President, 2018).

Current Challenges within the Government

Increasing cybersecurity within the government has been an ongoing challenge since 2008 when the Bush administration created the Comprehensive National Cybersecurity Initiative in an effort to address the cybersecurity gap. However, GAO initially identified cybersecurity as a risk in 1997 but the issue lacked attention for many years (U.S. Government Accountability Office, 2021). The initiatives were designed to increase cyber defense through counterintelligence, research and development, network technologies, sharing of information between entities, education, risk management, and deterrence strategies. In 2010, GAO provided more than 3,000 recommendations to increase cybersecurity but almost 1,000 of those recommendations remain to be addressed as of late 2020 (U.S. Government Accountability Office, 2021). Among the remaining major challenges within the government include (U.S. Government Accountability Office, 2021):

- Establish cybersecurity strategies and perform effective oversight.
- Securing federal information systems and data.
- Protect critical infrastructure within cyberspace.

- Protect privacy and sensitive information.

According to the Watchdog Report podcast hosted by GAO, Jennifer Franks (2021) identified three major struggles that still exist within the government: lack of full awareness, poorly designed and implemented controls, and lack of personnel. She believes that the government lacks cybersecurity urgency and needs to find solutions to better manage the protection of their assets. Focusing on these issues provides an opportunity for the government to reduce the human threat as a weakness within cybersecurity programs. To combat these issues, the government has already implemented several solutions to address awareness with training and education programs that are required for all government employees (Office of Personnel Management, n.d.). These training requirements must be completed on an annual basis to keep employees up to date and informed on cybersecurity. Additional training requirements exist depending on employees' roles and occupations to address more specific needs (Office of Personnel Management, n.d.). Annual training seems to have only addressed a piece of the problem because human error has not been eliminated nor effectively reduced given the recent reports from GAO as previously mentioned.

The amount of time dedicated to cybersecurity training has shown to have a negative relationship towards cyber incidents (Kweon et al., 2019). As employees spend more time with cybersecurity training, there should be a reduction in cyber incidents that are a result of human error. An issue with annual training is that it is only required once a year or every twelve months (Office of Personnel Management, n.d.). A recent study was conducted by The Advanced Computing Systems Association to investigate the effectiveness of phishing awareness and education to determine how employees respond to threats over time. The study concluded that employees remained aware at four months from the initial training however, after six months, employees were no longer able to identify the threats (Reinheimer et al., 2020). The study shows that annual training may not be effective to address the current challenges the government faces with cybersecurity awareness and human error. It is imperative to implement a solution that addresses employee behavior throughout the entire year and not on an annual basis if the government wants to better protect its assets and reduce human error.

Cybersecurity Culture

Cybersecurity culture has been considered an ill-defined problem due to a difference in the understanding of what delimits a cybersecurity culture (Gcaza & Solms, 2017). A review of academia and industry surveys has led to the development of a clearer definition of what a cybersecurity culture is: cybersecurity culture is the human behavior that protects organizational information through compliance with the organization’s security policies and procedures and an understanding of how to execute them as embedded through initiatives such as training, educations, awareness, and communication (Da Veiga et al., 2020). Cybersecurity culture has also been described as a way that things are done; secure behaviors that have become habitual and require less cognitive effort (Gcaza & Solms, 2017; Haith & Krakauer, 2018). It is also known to be an effective tool that helps manage the human factors within cybersecurity because employee behavior is known to either create or reduce vulnerabilities (European Union Agency for Network and Information Security, 2018; Huang & Pearlson, 2019).

According to the Security Culture Report, industries with strong cultures have higher levels of attitudes, secure behaviors, cognition, compliance, and norms whereas those with weaker cultures have lower levels (Petric et al., n.d.). Individuals within a developed a mature culture operate with a cybersecurity mindset that not only protects the organization against cyber threats but also themselves (Donahue, 2011). Employees need to understand that cybersecurity is everyone’s responsibility and not for a specific group, such as the information technology team, but it has been known to require substantial effort from the organization to instil this mindset (Alshaikh, 2020). There is a lack of information within research that offers a framework for building a cybersecurity culture that focuses on changing human behavior to become more secure with their actions (Alshaikh, 2020). Therefore, there is a need to learn about the influences on human behavior and what methods can be used to ensure employees are complying with security policies and engaging in secure behaviors to reduce organizational risk.

CHAPTER THREE:

METHODOLOGY

Social Cognitive Theory (SCT) developed by Albert Bandura explains how behavior is observationally learned and influenced by environmental and cognitive factors (Bandura, 1997). Bandura proposed the Triadic Reciprocal Determinism theory, which is the basis of SCT, suggesting that behavior, cognitive factors, and environment factors are related and influence one another for a desired outcome (Bandura, 1978). Considering what has been covered in Chapters 1 and 2, a culture of cybersecurity is intended to mitigate the human problem that is commonly found within the government. SCT specifies that individual behaviors can be affected by organizational culture (Wood & Bandura, 1989). The goal is to mitigate the human problem by establishing a culture that influences individuals to behave in a secure manner (European Union Agency for Network and Information Security, 2018). In this context, the SCT will be used as a basis to guide research and collect information on the influencing factors of secure behavior so that it can be utilized to help foster a culture of cybersecurity while focusing on the relationships between 1) environmental factors, 2) cognitive factors (also known as personal factors), and 3) their mediating effect on behaviors.

Having this goal in mind, research was conducted with the utilization of Google Scholar, Pfau Library’s OneSearch, ScienceDirect, and general web searches via Google. Sources were selected and analyzed based on their relevance to the subject. The sources utilized were compiled of research articles, reports, and articles from well-known domains, companies, and authors with a credible background in cybersecurity. Research began by initially discovering how a cybersecurity culture impacts the reduction of cybersecurity risks while narrowing the results down to the general topic of policy compliance. Searches were conducted using key words such as: cybersecurity policy compliance, impact of cybersecurity culture, security awareness "compliant" behavior, social factors that increase policy compliance, cognitive factors that increase policy compliance, and analysis of cybersecurity culture.

The next step was to examine what best practices are being utilized to develop cultures of cybersecurity while also identifying what challenges may be likely to occur. To find the most relevant information for best practices and challenges, Google Scholar was utilized to find recent case studies using following key terms and limiting the publication date from 2017-2021: cybersecurity culture, creating a cybersecurity culture, and best practices to develop cybersecurity culture, challenges with cybersecurity culture, and challenges with changing culture. Two relevant case studies were yielded as a result of the search and were individually analyzed in the following chapter.

Table 2: Overview of Research Methods and Publications

Database	Category	# Of relevant publications	# Selected	Authors

ScienceDirect;
Google Scholar;
Pfau Library's OneSearch
	Cognitive factors	16	11	Roberts, 2021;
				Koohang et al., 2020;
				Li et al., 2019;
				D'Arcy & Lowry, 2019;
				Howard, 2018;
				Muhire & Ayyagari, 2018;
				Balozian & Leidner, 2017;
				Bauer & Bernroider, 2017;
				Pfleeger & Caputo, 2012;
				Benbasat et al., 2010;
				Wood & Bandura, 1989

ScienceDirect;
Google Scholar;
Pfau Library's OneSearch
	Environmental factors	11	7	Bicchieri et al., 2021;
				D'Arcy & Lowry, 2019;
				Li et al., 2019;
				Barlow et al., 2018;
				Balozian & Leidner, 2017;
				Pfleeger & Caputo, 2012;
				Union Agency for Network and Information Security, 2018

Google Scholar; Google Search	Best practices and challenges	7	2	Alshaikh, 2020; Huang & Pearlson, 2019

CHAPTER FOUR:

RESULTS

Results from Social Cognitive Theory

A collection of published articles and documents have discussed what environmental and cognitive factors may have an influence on individuals to exercise compliant behavior (D’Arcy & Lowry, 2019; Koohang et al., 2020; Pfleeger & Caputo, 2012; Roberts, 2021). Research has shown that environmental and cognitive factors both have a significant impact on human behavior and whether they comply with security policies (D’Arcy & Lowry, 2019; Koohang et al., 2020; Pfleeger & Caputo, 2012; Roberts, 2021; Union Agency for Network and Information Security, 2018). While both factors are known to have an influence on human behavior, there is more research available that has studied cognitive factors than there are that studied environmental factors (D’Arcy & Lowry, 2019; Pfleeger & Caputo, 2012). An overview of the environmental and cognitive factors found throughout the research are highlighted below in Figure 4.1.

Cognitive Factors and Behaviors

Cognitive factors are internal influences that have been studied with regard to human behavior and compliance. Self-efficacy is one of several factors identified in research that have a significant impact on compliant behavior. In this context, self-efficacy refers to an individual’s belief that they can perform secure behaviors. Studies have shown that higher levels of self-efficacy positively affect employees' secure behaviors and that they are more committed than those who lack self-efficacy (Koohang et al., 2020; Li et al., 2019; Wood & Bandura, 1989). Earlier research has shown that self-efficacy positively affects an individuals' intention to comply with security policies (Benbasat et al., 2010). Later studies corroborated those findings and determined that self-efficacy does have a positive impact on compliant behavior (D'Arcy & Lowry, 2019; Li et al., 2019). According to Pfleeger and Caputo (2012), employees that have higher levels of self-efficacy will perform secure behaviors and their peers are more likely to learn from them and engage in those same secure behaviors. Questions regarding methods to increase self-efficacy have surfaced throughout research and it has been suggested that self-efficacy can be influenced and strengthened through experiences, social persuasion, knowledge, and awareness (Li et al., 2019; Wood & Bandura, 1989).

The attitude of the individual towards different aspects of cybersecurity has also been linked as an influential factor for compliant behavior. Studies have linked individuals' attitudes towards policy adherence to complaint behavior, concluding that individuals with a positive attitude towards policy compliance are more likely to comply whereas those with a negative attitude are less likely to comply (D'Arcy & Lowry, 2019; Howard, 2018). Muhire and Ayyagari (2018) have argued that attitudes have a positive relationship with an individual's intent to comply with security policies. They found that complaint behavior is a result of an individual's positive perception of the security policy and non-compliance may be the result if individuals perceive the policies as a nuisance (Muhire & Ayyagari, 2018).

Bauer and Bernroider (2017) showed strong support that information security knowledge has a significant relationship with an individual’s attitude towards compliance. The results suggest that an individual with more knowledge is likely to have a greater positive attitude which increases their intention to actually comply with policies (Bauer & Bernroider, 2017). A later study conducted by Roberts (2021) also concluded that there is a relationship between an individual's knowledge and the attitude the individual has towards secure behaviors. Attitudes towards cybersecurity may increase when their knowledge of cybersecurity also increases and may reduce risky behaviors that don’t comply with policy (Roberts, 2021). Balozian and Leidner (2017) broke knowledge into two categories and suggested that increasing these areas can result in secure and compliant behavior from the individual: technical and behavioral knowledge. Behavioral knowledge is described as knowing what behaviors are acceptable as described in policies and technical knowledge is an individual’s knowledge of how to perform secure behaviors (Balozian & Leidner, 2017). Individuals that have knowledge of security policies have been seen perform secure behaviors more often than those who have no knowledge of the security policies (Balozian & Leidner, 2017; Li et al., 2019) and individuals that know how to perform secure behaviors are more likely to comply than those who do not (Balozian & Leidner, 2017). Research has provided strong evidence that an individual's self-efficacy, attitude, and knowledge are contributing factors that influence an individual to perform secure behaviors that are compliant with organizational security policies.

Environmental Factors and Behaviors

Social proximity has been identified as a reason why individuals may or may not behave in a compliant manner (Bicchieri et al., 2021). Social proximity is an environment of people that share a common baseline of traits, characteristics, and identities such that they will behave in a manner that is deemed acceptable by the group and avoid those that are not (Bicchieri et al., 2021). Social environments can play a role in the deterrence or encouragement of exercising compliant behaviors (Balozian & Leidner, 2017). A study using social proximity was conducted to understand its effect on complaint behavior and concluded that observing peer behavior persuades individuals to alter their behaviors based on what they have observed; when compliant behavior was observed within an individual's social proximity, the individual emulated that same behavior (Bicchieri et al., 2021). Other researchers have also concluded that peer behavior is a significant factor that affects how others behave with regard to cybersecurity, suggesting that individuals learn secure behavior by imitating their peers' actions (Balozian & Leidner, 2017, Li et al., 2019; Pfleeger & Caputo, 2012).

An explanation to why individuals imitate peer behavior or comply with policies can be the norms that have been established within the environment such as subjective and descriptive norms. Subjective norms are referred to as the users' belief that significant others, such as managers, approve or disapprove particular behaviors (Balozian & Leidner, 2017). Balozian and Leidner (2017) suggest that if the managers expect compliant behavior, employees are likely to engage in those behaviors. The expectations from significant others creates a social pressure on the individuals to engage in secure behaviors and comply with security policies (Balozian & Leidner, 2017). According to D'Arcy and Lowry (2019), subjective norms have also been considered strong predictors of compliant behavior; if compliant behavior is not a subjective norm, then individuals are unlikely to comply.

Descriptive norms refer to the users' perception that significant others and colleagues are exercising behaviors that are compliant with policies (Balozian & Leidner, 2017; D'Arcy & Lowry, 2019). Peers that exhibit secure behavior are considered role models that provide positive messages and encourage policy compliance (Balozian & Leidner, 2017). On the other hand, those who exhibit poor behaviors and go against policy are known to negatively impact others' behaviors (Balozian & Leidner, 2017). According to a report by the European Union Agency for Network and Information Security (2018), individual compliance levels were positively impacted by when individuals believed their peers were complying with policies and engaging in secure behavior. People often conform to social norm behaviors so that they can fit in or be accepted by others within the environment (Barlow et al., 2018). These findings provide evidence that environmental factors such as social proximity, subjective norms, and descriptive norms can influence an individual's compliance behavior.

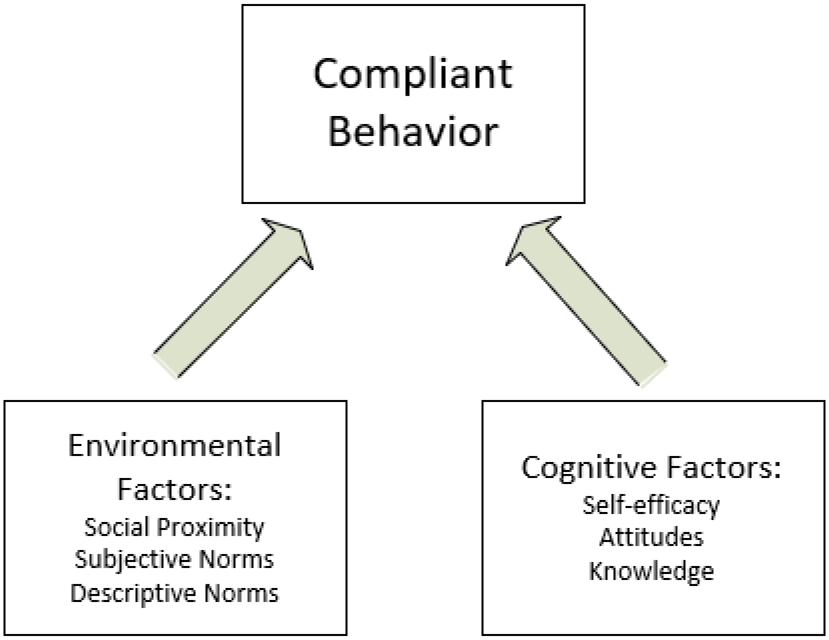

Figure 4.1 Factors of Compliant Behavior

Best Practices and Challenges

Case Study 1

The case study involved three large-scale organizations from Australia and was conducted to identify what methods were utilized to create or improve a culture of cybersecurity that influenced employee behavior (Alshaikh, 2020). The organizations were chosen based on their similarities to one another in terms of their culture and being in the early stages of cultural development rather than those who already have one established (Alshaikh, 2020). Five specific initiatives were identified that helped solve their problem and go from an organization without a cybersecurity culture to an organization with a cybersecurity culture that improved employee behavior. These key initiatives will be reviewed in the following sections.

The first key initiative was to identify the top behavioral themes from each cybersecurity-related policy developed by the organization which resulted in the identification of five key behaviors: be differential and respectful when online, “think before you click”, “think before you send”, ensure files and information systems are secure, report suspicious activity (Alshaikh, 2020). The purpose of identifying these behavioral themes was to communicate them to the employees so that they had knowledge of them. When the employees were performing the desired actions and behaviors, they were in compliance with a majority of the policies which was noticed as a significant improvement (Alshaikh, 2020). Another company took the same approach and identified eight behaviors after reviewing their information security policies. Once they were identified, the organization trained their employees specifically on those desired behaviors.

Secondly, there was a significant need to create a champion network given the large sizes of each company (Alshaikh, 2020). The champion network was meant to help engage all areas of the organization, especially since they happened to have multiple geographical locations, and they were also established in each hierarchical layer of the organization (Alshaikh, 2020). The intent for the champion network was to increase cybersecurity awareness by amplifying the messages, encourage and help employees to adopt the identified security behaviors, identify the knowledge, skills, and abilities required from employees, and report the progress so that the security team could determine the effectiveness of the initiative (Alshaikh, 2020). One important note was that the champion did not need to be a cybersecurity expert but needed to be a good people person and be able to communicate effectively (Alshaikh, 2020). Champions were required to have the most up-to-date information so they could be effective in their responsibilities listed above (Alshaikh, 2020).

The third key initiative was to establish a cybersecurity hub, or internal website, that employees can visit to learn more about cybersecurity and ways to improve their behaviors (Alshaikh, 2020; Ling Li et al., 2019). The design of the website mirrored the key cybersecurity behaviors identified by the organization, consolidated policies and procedures, and allowed employees to ask questions that facilitated learning (Alshaikh, 2020). The cybersecurity hub provided employees a method to effortlessly access specific information regarding behavioral expectations, such as the policy-derived behaviors, and also supported the champion network by supplying them with a platform to spread awareness (Alshaikh, 2020). The organizations found that employees were often bothered by visiting multiple sources to find information and noted that having a single point of contact, or cybersecurity hub, was much more practical (Alshaikh, 2020). Providing information regarding at-home secure behavior for employees and their families was also found very useful (Alshaikh, 2020).

Furthermore, the cybersecurity team branded themselves with a mascot and or a logo to enhance their visibility within the organization (Alshaikh, 2020).

Logos and mascots were placed on all cybersecurity awareness-related material and training to establish relationships between the activities and cybersecurity so employees could relate the material to cybersecurity, acting as a cue to action (Alshaikh, 2020). One organization mentioned that it was important to involve the employees in the decision and design process for the team branding, giving them a personal connection to the brand (Alshaikh, 2020). Consistently using the cybersecurity team's visual identity was essential in the development of their cybersecurity cultures (Alshaikh, 2020).

Finally, the fifth key initiative was to align the organization's cybersecurity awareness program to internal and external campaigns. Using all available resources showed an increase in the effectiveness and overall impact on the employees and influenced positive behavior changes (Alshaikh, 2020). These organizations aligned internal campaigns with external campaigns, such as privacy awareness week and scammer awareness week, to reduce the time and effort required by simply using external campaign information to disseminate to their employees while attaching the organization's visual identity to the material (Alshaikh, 2020). These actions demonstrated effective methods that were used to encourage secure behavior by engaging employees in a fun and exciting way (Alshaikh, 2020). It also enhanced the collaboration between different units and stakeholders and decreased the time and attention demanded from employees (Alshaikh, 2020). These organizations used their communications teams to develop methods for communicating awareness material using non-technical languages allowing their employees to better understand the message while also collaborating with their marketing teams when designing their visual identity (Alshaikh, 2020).

Challenges. It was clear that the organizations did not have an effective method to measure their success and improvement levels during the early stages of secure culture development. The percentage of completed training for was commonly used as a metric to determine if employees were completing their required education, however, it was not able to measure its effectiveness on behavior change outcomes (Alshaikh, 2020). Employees initially resisted the changes because they were neither engaged nor motivated to participate in training, while some even shared answers (Alshaikh, 2020). As a result, the percentage of completed employee training was only satisfying the compliance of mandatory training and could not be used to gage its effect on behaviors (Alshaikh, 2020). Once the key initiatives were put in action and ongoing, the organizations agreed on three methods of measurement: employee feedback regarding cybersecurity activities, analysis of employee engagement using the cybersecurity hub, and reports of increased collaboration (Alshaikh, 2020). As a result, these organizations were able to measure the effectiveness of their initiatives while noticing an increase of incident reporting which indicated an increase in compliance and secure behavior (Alshaikh, 2020). A noteworthy mention is that each organizational leader expressed the importance of leadership buy-in and that it must be a priority for the executive team, otherwise the initiative is likely to fail (Alshaikh, 2020).

Case Study 2

Liberty Mutual’s case study shows an example of how an organization can minimize their employees’ risky behaviors and reduce vulnerabilities by increasing the use of secure behavior. The case study analyses the mechanisms utilized by the company to create a cybersecurity culture for their organization that instills a set of beliefs, attitudes, values, and effective performance measures to influence behavior (Huang & Pearlson, 2019).

Creating a Chief Information Security Officer (CISO) position and assigning someone with that responsibility was Liberty Mutual’s first action to take place (Huang & Pearlson, 2019). Similar to the previous case study, cybersecurity became a top priority for the leadership team given the extreme importance and value they believed it has to the company (Huang & Pearlson, 2019). The CISO’s overarching responsibility was to drive the organization’s culture towards one that had positive cybersecurity beliefs, values, and attitudes while continuously reinforcing its importance (Huang & Pearlson, 2019). Identifying the core behaviors and concepts from the governing policies, called Pillars of Data Protection, helped leadership identify a set of expected employee behaviors and communicated them to each employee (Huang & Pearlson, 2019). Policies and expectations were written using non-technical language to increase the level of understanding by all employees while also further clarifying and explaining exactly how it is related to the employee (Huang & Pearlson, 2019).

A significant amount of effort was directed towards creating an effective communication strategy that ensured cybersecurity messages were being received by all employees. Associating their messages with cybersecurity was done by branding the cybersecurity team and inserting their logo into every message, with the help of the marketing team, so employees could recognize its significance (Huang & Pearlson, 2019). The CISO regularly published blogs that covered relevant topics currently impacting the organization in some way (Huang & Pearlson, 2019). Additionally, as major cybersecurity news stories broke, leaders used the information to raise awareness within the organization and discussed its impacts, how it relates to the organization, and how employees might take steps to prevent or respond to similar events if they happen within the organization (Huang & Pearlson, 2019). Using slogans became an effective tool for communicating messages that helped employees realize they are part of the solution which began shaping positive employee attitudes (Huang & Pearlson, 2019). Employees began to understand the value of cybersecurity, started paying more attention to the messages, and were more encouraged than ever to participate in cybersecurity activities as a result of observing how much the executive team was involved in spreading the messages (Huang & Pearlson, 2019).

Expanding communication, Liberty Mutual took the initiative to provide employees with learning opportunities to increase their knowledge of cybersecurity. Since they recognized that irregular training classes were ineffective, Liberty Mutual decided to incorporate a strategy of continuous learning through regular training classes and communication campaigns to provide employees with an understanding of cybersecurity risks and how to mitigate them (Huang & Pearlson, 2019). Internal campaigns were aligned with external campaigns to provide fresh, current, and relevant information to the employees which help reinforce the value of cybersecurity (Huang & Pearlson, 2019). Videos, digital displays, newsletters, and events were used as a method for consistent delivery of training and awareness to show the importance of data protection (Huang & Pearlson, 2019). Leadership also implemented an incentive program to help motivate employees, highlighting potential rewards and consequences if employees improved their cybersecurity behaviors or failed to perform the expected behaviors (Huang & Pearlson, 2019). The outcome of these actions began creating an environment with strong social norms and beliefs towards cybersecurity because employees began discussing cybersecurity topics and engaging in activities regularly (Huang & Pearlson, 2019).

Lastly, Liberty Mutual implemented a couple of methods to measure the effectiveness of their cybersecurity culture initiative. They conducted employee evaluations to determine how well they have been doing concerning cybersecurity; if employees were performing as expected or beyond, it was annotated in their evaluation with a possibility for the employee to receive a reward, otherwise, poor behavior was reflected in their evaluation with the possibility of consequences (Huang & Pearlson, 2019). Regular interviews were conducted outside of the employee evaluation process to gain employee feedback so leadership could determine if their initiative is showing success (Huang & Pearlson, 2019). Interview results showed an increase in the employees' self-efficacy and awareness levels as a result of the employees understanding what behaviors to perform while feeling more confident and empowered to protect the information systems and data (Huang & Pearlson, 2019).

Challenges. Specific challenges that Liberty Mutual may have encountered were not identified in this case study. However, there appears to be evidence that potential challenges can arise while enforcing consequences for poor employee behavior. Additional training has been used as a consequence for failing cybersecurity exercises, specifically phishing exercises (Huang & Pearlson, 2019). While it was noted that employees are generally not bothered by taking additional courses, not all employees may react the same way which may lead to cybersecurity being perceived as a nuisance (Huang & Pearlson, 2019). To prevent employees from having a negative perception of cybersecurity, the challenge is to determine at what point should consequences be enforced, and to what extent, so that employees remain engaged and continue to participate in the activities and exercises.

CHAPTER FIVE:

DISCUSSION

Results from research provide valuable information in terms of the influential factors of human behavior and what best practices are currently being used by other organizations to create a culture of cybersecurity. As mentioned in Chapter 2, the government is a highly desired target for cybercriminals and negligent behavior by employees has been seen to increase the risk of successful cyber-attacks and security incidents. Identifying the influential factors of human behavior and best practices provides the government with a starting point to build a strategy that targets those factors to create a positive change in their employees' behaviors. Employees that do not meet the expectations of secure behavior and compliance can be poisonous to the government. For example, based on the influence of social proximity, poor behaviors can proliferate throughout the organization just as quickly as good ones when employees engage in non-compliance.

The case studies showed that the environmental and cognitive factors previously identified are associated with a strong cybersecurity culture and secure behavior. There is evidence suggesting that creating a culture focused on cybersecurity appears to have an impact on employees' performances resulting in higher levels of compliance and ultimately stronger security. The case studies share similar implementation methods but also have their own unique methods while each has shown to be successful. Since case studies did not have identical implementations methods, it shows that there is no signal solution to solve the problem of secure behavior. These best practices can be incorporated into other strategies, along with other unique methods, and produce the same result. The collection of best practices is highlighted in figure 5.1. The following section will provide recommendations for the government based on the research results.

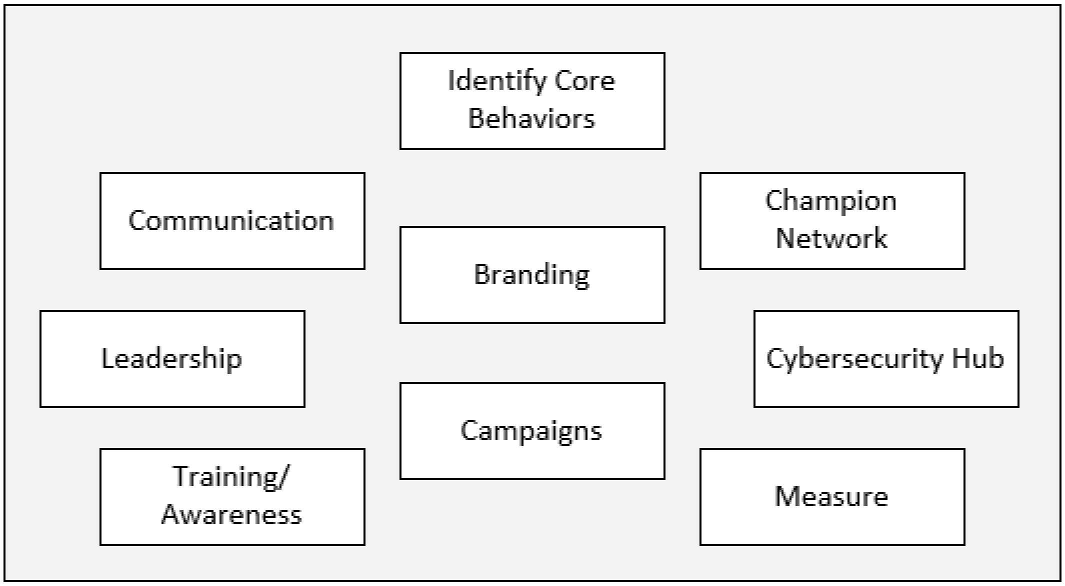

Figure 5.1 Best practices for developing a cybersecurity culture

Recommendations

Leadership Support

Gaining leadership support is the first step the government must take in order to have the best chances of success. It is likely that additional resources will need to be acquired which may require new budgets and approval from leadership. To no surprise, leadership tends to prioritize efforts that support their overall mission and if they do not see the value of developing a cybersecurity culture from a mission perspective, the initiative is likely to lose leadership support and the necessary resources to be successful. Thus, the requirement for a cybersecurity culture should be communicated in a way that adds value to the mission. For example, the DoD has a mission to protect the United States and deter war by providing military forces. With that comes a significant amount of sensitive data, that if compromised, could also compromise the mission and the integrity of our military. A cybersecurity culture can provide an environment where employees are constantly thinking about data protection and exercising secure behaviors. Doing so will ensure the integrity, availability, and confidentiality of DoD assets and so that they can continue supporting their mission with reduced risk.

Once leadership support is obtained, a top-down approach is likely to be best given the hierarchical structure and culture of the government. Leadership will need to be consistently involved and will need to communicate and express the importance of creating a cybersecurity culture down the chain of command. Subordinates are likely to engage when they observe the importance it has with leadership. Each department will need to determine what their role is and how they will engage in the creation of a cybersecurity culture. Doing so will make sure the culture spreads throughout the entire organization and stays consistent with supporting the mission. Since technology is not the only defense, leadership should communicate to every employee that they play a critical role in cybersecurity and are part of the solution. Doing so may help reinforce the importance of the requirement and encourage employees to behave accordingly.

Set Expectations

Following the top-down approach, behavioral expectations should be set for each department and hierarchical level of the organization. Expectations should be derived from policies and include specific behaviors that are expected from each department employee. Oftentimes, departments have unique policies pertaining to their function, so a single set of expectations may not be applicable for the entire organization. However, expectations similar to phishing email behaviors can be an expectation set for the entire organization since everyone typically uses email. Deriving expectations using the top-down approach can simplify the process and make it easier to determine which expectations are applicable for each function of the organization. Behavioral expectations should be communicated regularly by leadership and be made easily available to employees. This approach can help establish descriptive and subjective norms by setting expectations of approved behavior and which helps create a pattern of secure behavior and compliance.

Communicate

Communication is arguably one of the most critical pieces to this solution. As mentioned earlier, communicating the requirement to leadership is critical. It is also critical that the same message of importance is communicated through the organization so employees understand its significance and what their role is. A good communication strategy should involve several steps. First, information should be communicated using a language that everyone understands. The government is employed with both military and civilian personnel and they may have different languages of communication. It will be important to find a common ground when communicating the information. The information should describe how it relates to the employee and how their actions impact the organization in a positive way. The second step would be to establish an internal website that consolidates policies, expected behaviors, and additional information so employees have easy access to all the information rather than having to gather information across multiple sources. This can reduce the efforts required by employees and create an efficient way to seek information regarding cybersecurity and expectations. The website should have the capability that allows employees to ask questions when they need additional information. The content on the website should remain aligned with the mission and be consistently updated to reflect the most relevant information.

Moreover, employees need to be able to recognize cybersecurity-related messages as important information from cybersecurity. One way to accomplish this is to insert a unique reference that is symbolic of cybersecurity, such as a cybersecurity logo which will be discussed further in the following section. Furthermore, leadership should encourage employees to discuss cybersecurity-related topics with their colleagues and start building a social environment of cybersecurity. As employees engage in cybersecurity discussion more often, cybersecurity may start to become a common cognitive process while also sharing valuable information with one another. Lastly, leadership should provide feedback to their employees to inform them of their positive contributions to the mission. This can result in an increase in employee engagement, self-efficacy, and lead to positive attitudes towards cybersecurity.

Cybersecurity Team

A cybersecurity team is necessary for the government and should consist of trained personnel that understand cybersecurity and the organization's information systems. Not only should the team be responsible for ensuring the systems are secure, but also help develop awareness activities, maintain the information on the cybersecurity hub, and develop content for cybersecurity messages. Furthermore, the team should increase their visibility and by creating a logo or mascot that can be inserted into important messages related to cybersecurity. The brand should be designed in a way it is unique to the cybersecurity team and allows for easy identification. The brand will allow employees to relate the message to cybersecurity and understand that it has significant value and is important to the organization. Examples of messages that should include the team's branding are newsletters, flyers, training documents, and posters. Lastly, a champion network should be established across the government. Their responsibility should be to help spread messages, encourage employee engagement, and ensure the organization as a whole is consistent with its efforts.

Educate

Training and education plans should be developed to increase the knowledge gap employees have with cybersecurity and expected behaviors. Training should be offered at least once and year and more frequently if negligent behavior is not decreasing. We have seen data that shows employees may forget what behaviors are expected, or how to perform them, when not engaged for some time. As the top-down approach is being used, specific training may be required for each department or group depending on their functions. Policy awareness should be included in the training to inform employees of expected behaviors and to provide a reference to the documents so employees know which behavior is derived from what policy. Policy awareness has been seen to help increase secure behavior since employees are aware of expected behaviors. To gain a consistent presence in cybersecurity, the government should align internal campaigns with external campaigns regularly. For example, each month can consist of a unique campaign that spreads awareness of current and relevant information and encourages employees to participate in cybersecurity activities. Since the government requires employees to maintain the secrecy of specific information, a campaign can be developed that targets how employees can communicate effectively without unintentionally leaking information. Other campaigns can provide awareness that informs employees of current threats, how to identify them, and how to appropriately respond to them.

Measure Success

Establishing methods to measure the effectiveness of the cybersecurity culture is necessary to determine if there have been positive impacts on the organization. Possible methods of measurement may include employee engagement in related activities, compliance, number of incidents, and employee feedback. Surveys can be used for employee feedback which can help leadership determine if there has been a shift in employee attitudes, changes in employees' self-efficacy, and changes in social norms. Identifying these levels can be used to help target specific hindering factors that are causing poor secure behaviors and non-compliance. A reduction in security incidents, increased employee engagement, and positive feedback results may suggest that the cybersecurity culture is making a significant impact on the organization in a positive way. The data can be used to seek additional funding that supports the ongoing efforts for sustaining the cybersecurity culture within the government.

Limitations

There exists limitations to the study and proposed solutions. Research barriers such as key terms and repositories used throughout the study may have reduced the possible number of available resources. Access to limited amounts of research data may have restricted the discovery of additional SCT factors that are known to influence human behavior. Additionally, recommendations were based on recent best practices and it is possible that the best practices may change over time.

It’s important to note that SCT is not the only theory that can be applied to developing a cybersecurity culture. Attribution theory is another psychology based theory that has been used to study why specific behaviors are motivated (Graham, 2020). Attributions have been found to motivate behaviors based on an individual's perceived cause of the outcome; a rationale of the observed behavior after it occured (Schunk & DiBenedetto, 2020). Effort and ability have been argued as attributions of higher performance; individuals that exert more effort or have greater abilities will perform better than those who lack effort and ability (Schunk & DiBenedetto, 2020). However, SCT was chosen as a research guide because it helps discover influential factors that exist or can exist within organizational cultures by looking at environmental and cognitive factors so that employees behave more securely.

Conclusion

The purpose of this research project was to discover best practices for developing a culture of cybersecurity, identify potential challenges, and use this information to provide recommendations for the government. Creating a culture of cybersecurity to influence secure behaviors has been undoubtedly challenging for many organizations but it has been recognized as adding significant value to the organization. The results of this research share valuable insight to the factors and methods that the government can adopt to develop a cybersecurity focused culture of their own. There is no single solution that works for every organization, so it is important that the government considers its environment and considers the recommendations provided as guidance to support their efforts. The government's success will depend on the strategy of their execution, identifying the most effective ways to measure its effectiveness, and gaining support from senior leadership. A successful cybersecurity culture implementation can have a strong influence on employees engaging in secure behaviors and may help mitigate future incidents.

REFERENCES

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

America is Under Cyber Attack: Why Urgent Action is Needed, 112–85, 112th Congress, Second (2012). https://www.govinfo.gov/content/pkg/CHRG-112hhrg77380/html/CHRG-112hhrg77380.htm

Andres, R. (2017, December 21). Cyber gray space deterrence. *PRISM* | *National Defense University*. http://cco.ndu.edu/News/Article/1401927/cyber-gray-space-deterrence/

Aon. (2020). *2020 Cyber Security Risk Report*. https://www.aon.com/getmedia/8496a44a-7006-40ad-81a2-111aa15cc237/Aon-2020-Cyber-Security-Risk-Report-vDigital-SECURE.pdf

Armerding, T. (2019, January 10). *GAO cybersecurity report confirms major government gaps* | *Synopsys*. Software Integrity Blog. https://www.synopsys.com/blogs/software-security/gao-cybersecurity-report/

Ashford, W. (2017, August 25). Security professionals name top causes of breaches. *ComputerWeekly.Com*. https://www.computerweekly.com/news/450425184/Security-professionals-name-top-causes-of-breaches

Balozian, P., & Leidner, D. (2017). Review of IS security policy compliance: toward the building blocks of an IS Security Theory. *ACM SIGMIS Database:*

The DATABASE for Advances in Information Systems, *48*(3), 11–43. https://doi.org/10.1145/3130515.3130518

Bandura, A. (1978). The self system in reciprocal determinism. *American Psychologist*, *33*(4), 344–358. https://doi.org/10.1037/0003-066X.33.4.344

Bandura, A. (1997). *Self-efficacy: The exercise of control* (pp. ix, 604). W H Freeman/Times Books/ Henry Holt & Co.

Barlow, J., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*(8). https://aisel.aisnet.org/jais/vol19/iss8/3

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *48*(3), 44–68. https://doi.org/10.1145/3130515.3130519

Benbasat, I., Cavusoglu, H., & Bulgurcu, B. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523. https://doi.org/10.2307/25750690

Bicchieri, C., Dimant, E., Gaechter, S., & Nosenzo, D. (2021). Social proximity and the erosion of norm compliance (SSRN Scholarly Paper ID 3355028). *Social Science Research Network*. https://doi.org/10.2139/ssrn.3355028

Bowen, A. S. (2021). *Russian Cyber Units*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11718

Cancian, M. F. (2019, October 15). *U.S. Military Forces in FY 2020: Army*. U.S. Military Forces in FY 2020: Army. https://www.csis.org/analysis/us-military-forces-fy-2020-army

Center for Internet Security. (n.d.). *Cybersecurity Spotlight—Cyber Threat Actors*. CIS. Retrieved February 25, 2021, from https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/

Cluley, G. (2021, February 18). North Korean hackers charged by US in relation to attacks. *The State of Security*. https://www.tripwire.com/state-of-security/featured/us-charges-north-korean-hackers-wannacry-sony-pictures-attack/

Connell, M., & Vogler, S. (2017). *Russia's Approach to Cyber Warfare*. Center for Naval Analyses. https://apps.dtic.mil/sti/pdfs/AD1032208.pdf

Cyberedge Group. (2021). *2021 Cyberthreat Defense Report*. https://www.isc2.org//-/media/ISC2/Research/Cyberthreat-Defense-Report/2021/CyberEdge-2021-CDR-Report-v10--ISC2-Edition.ashx

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

D'Arcy, J., & Lowry, P. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*, 43–69. https://doi.org/10.1111/isj.12173

Datta, P. (2021). Hannibal at the gates: Cyberwarfare & the Solarwinds sunburst hack. *Journal of Information Technology Teaching Cases*, 204388692199312. https://doi.org/10.1177/2043886921993126

Donahue, S. E. (2011). Assessing the impact that organizational culture has on enterprise information security incidents. https://www.semanticscholar.org/paper/Assessing-the-impact-that-organizational-culture-on-Donahue/d9cac5132a3b0b518f56d94d96f7aada660745eb

Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, *51*, 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

Eggers, S. (2021). A novel approach for analyzing the nuclear supply chain cyber-attack surface. *Nuclear Engineering and Technology*, *53*(3), 879–887. https://doi.org/10.1016/j.net.2020.08.021

European Union Agency for Network and Information Security. (2018). Cyber Security Culture in organisations. https://doi.org/10.2824/10543

Executive Office of the President. (2018). *Classification Guidance*. https://ustr.gov/sites/default/files/foia/Classification%20Guidance.pdf

Executive Office of the President of the United States. (n.d.). *Federal information Security Modernization Act of 2014: Annual Report to Congress*. https://www.whitehouse.gov/wp-content/uploads/2020/05/2019-FISMARMAs.pdf

Federal Bureau of Investigation. (2021). *IC3 Releases 2020 Internet Crime Report* [Press Release]. Federal Bureau of Investigation. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

Fessler, P., & Martin, M. (2017, June 18). *Russians believed to have used spear-phishing in election hacking.* NPR.Org. https://www.npr.org/2017/06/18/533438850/russians-believed-to-have-used-spear-phishing-in-election-hacking

Franks, J. (n.d.). *Urgent Actions Needed to Address Federal Cybersecurity Challenges*. https://www.gao.gov/podcast/urgent-actions-needed-address-federal-cybersecurity-challenges

Fruhlinger, J. (2020, February 12). *The OPM hack explained: Bad security practices meet China's Captain America*. CSO Online.

https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Gcaza, N., & Solms, R. von. (2017). Cybersecurity Culture: An ill-defined problem. *Information Security Education for a Global Digital Society*, 98–109. https://doi.org/10.1007/978-3-319-58553-6_9

Gootman, S. (2016). OPM hack: The most dangerous threat to the Federal Government today. *Journal of Applied Security Research*, *11*(4), 517–525. https://doi.org/10.1080/19361610.2016.1211876

Graham, S. (2020). An attributional theory of motivation. *Contemporary Educational Psychology*, *61*, 101861. https://doi.org/10.1016/j.cedpsych.2020.101861

Haith, A. M., & Krakauer, J. W. (2018). The multiple effects of practice: Skill, habit and reduced cognitive load. *Current Opinion in Behavioral Sciences*, *20*, 196–201. https://doi.org/10.1016/j.cobeha.2018.01.015

Howard, D. (2018). Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents. *Graduate Theses and Dissertations*. https://scholarcommons.usf.edu/etd/7306

Huang, K., & Pearlson, K. (2019, January 8). For what technology can’t fix: Building a model of organizational cybersecurity culture. https://doi.org/10.24251/HICSS.2019.769

Huseyin, M. (2019, July 17). Why humans are the weakest link in cybersecurity | *The Association of Corporate Treasurers*.

https://www.treasurers.org/hub/treasurer-magazine/why-humans-are-the%E2%80%93weakest-link-in-cybersecurity

Jennings, J., & Nagel, J. C. (2020). *Federal Workforce Statistics Sources: OPM and OMB*. 1–11. Congressional Research Service.

Kiener-manu, katharina. (2019). Cybercrime. //www.unodc.org

Kierkegaard, S. M. (2005). Cracking down on cybercrime global response: The cybercrime convention. *Communications of the IIMA*, *5*(1), 9.

Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, *120*(1), 231–247. https://doi.org/10.1108/IMDS-07-2019-0412

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2019). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-019-09977-z

Latto, N. (2020, December 19). What is Cybercrime and How Can You Prevent It? https://www.avast.com/c-cybercrime

Lederer, E. M. (2021, February 9). UN experts: North Korea using cyber attacks to update nukes. *AP NEWS*. https://apnews.com/article/technology-global-trade-nuclear-weapons-north-korea-coronavirus-pandemic-19f536cac4a84780f54a3279ef707b33

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Macak, M., Kruzikova, A., Daubner, L., & Bühnová, B. (2020). Simulation games platform for unintentional perpetrator attack vector identification. In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops* (pp. 222–229). Association for Computing Machinery. https://dl.acm.org/doi/abs/10.1145/3387940.3391475

Michael, C., & Sammons, J. (2017). Chapter 5. Cybercrime. In *The Basics of Cyber Safety* (pp. 87–116). Joe Hayton. https://learning.oreilly.com/library/view/the-basics-of/9780124166394/xhtml/chp005.xhtml

Milkovich, D. (2020, December 23). 15 Alarming Cyber Security Facts and Stats. Cybint. http://www.cybintsolutions.com/cyber-security-facts-stats/

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: concerns for psychiatry. *Current Psychiatry Reports*, *23*(4), 18. https://doi.org/10.1007/s11920-021-01228-w

Muhire, B., & Ayyagari, R. (2019). Employee Compliance to Information Security in Retail Stores. *Communications of the IIMA*, *16*(4). https://scholarworks.lib.csusb.edu/ciima/vol16/iss4/2

Musto, J. (2020, October 21). NSA warns Pentagon about Chinese government hackers. FOXBusiness; Fox Business.

https://www.foxbusiness.com/technology/nsa-advisory-warns-defense-department-about-chinese-government-hackers

Office of Information Security. (2021, March 25). *North Korea Cyber Activity*. https://www.hhs.gov/sites/default/files/dprk-cyber-espionage.pdf

Office of Personnel Management. (n.d.). *Federally Mandated Training—Training and Development Policy Wiki*. U.S. Office of Personnel Management. Retrieved May 4, 2021, https://www.opm.gov/wiki/training/Federally-Mandated-Training.ashx

Office of the Director of National Intelligence. (2021). *Annual Threat Assessment of the US Intelligence Community*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

Office of the Secretary of Defense. (2015). *Department of Defense Cybersecurity Culture and Compliance Initiative*. https://dod.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf

Olejarz, J. M. (2015, July 27). Why Cybersecurity Is So Difficult to Get Right. *Harvard Business Review*. https://hbr.org/2015/07/why-cybersecurity-is-so-difficult-to-get-right

Petric, Dr. G., Eriksen, A.-C., Huisman, J., Smothers, R. L., & Carpenter, P. (n.d.). *Measure to Improve*. KnowBe4, Inc. https://www.knowbe4.com/hubfs/Security-Culture-Report.pdf

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Pollock, T. (2017, October 20). Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS). 2017 KSU Conference on Cybersecurity Education, Research and Practice. https://www.researchgate.net/publication/321278165_Reducing_human_error_in_cyber_security_using_the_Human_Factors_Analysis_Classification_System_HFACS

ProofPoint. (2019). *Protecting People 2019*. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-protecting-people-2019.pdf

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Bettina Lofthouse, Tatiana von Landesberger, & Melanie Volkamer. (2020). *An investigation of phishing awareness and education over time: When and how to best remind users*. 27.

Roberts, S. A. (2021). Exploring the relationships between user cybersecurity knowledge, cybersecurity and cybercrime attitudes, and online risky behaviors. *Northcentral University, ProQuest Dissertations Publishing*. https://www.proquest.com/docview/2506630550/BFE64010521C479BPQ/1

Sanger, D. E., & Perlroth, N. (2020, April 15). U.S. accuses North Korea of cyberattacks, a sign that deterrence is failing. *The New York Times*. https://www.nytimes.com/2020/04/15/world/asia/north-korea-cyber.html

Scarfone, K., & Souppaya, M. (2009). *Guide to Enterprise Password Management* (NIST Special Publication (SP) 800-118 (Retired Draft)). National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-118/archive/2009-04-21

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World, 15th Anniversary Edition* (15th Anniversary Edition). John Wiley & Sons, Inc. https://learning.oreilly.com/library/view/secrets-and-lies/9781119092438/

Schunk, D. H., & DiBenedetto, M. K. (2020). Motivation and social cognitive theory. *Contemporary Educational Psychology*, *60*, 101832. https://doi.org/10.1016/j.cedpsych.2019.101832

Sen, R. (2018). Challenges to cybersecurity: current state of affairs. *Communications of the Association for Information Systems*, *43*, 22–44. https://doi.org/10.17705/1CAIS.04302

Sobers, R. (2020, September 8). *Government Hacking Exploits, Examples and Prevention Tips*. Inside Out Security. https://www.varonis.com/blog/government-hacking-exploits/

SolarWinds. (2020). *SolarWinds Public Sector Cybersecurity Survey Report 2020: IT Complexity, Insider Threats, and an Abundance of Privileged Users Plague Public Sector Cyber Readiness* (p. 43).

https://www.solarwinds.com/resources/survey/solarwinds-public-sector-cybersecurity-survey-report-2020

Steves, M. P., Greene, K. K., & Theofanos, M. F. (2019). A Phish Scale: Rating Human Phishing Message Detection Difficulty. *Proceedings 2019 Workshop on Usable Security*. Workshop on Usable Security, San Diego, CA. https://doi.org/10.14722/usec.2019.23028

Temple-Raston, D. (2021, April 16). *A "Worst Nightmare" Cyberattack: The Untold Story Of The SolarWinds Hack*. NPR.Org. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

United States Department of Agriculture. (2019). *Improper Usage of USDA's Information Technology Resources*. https://www.usda.gov/sites/default/files/50501-0020-12.pdf

United States Department of Justice. (2021, February 17). *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe*. https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

United States Department of State. (2019). *DS Report on Security Incidents Related to Potentially Classified Emails sent to Former Secretary of State Clinton's Private Email Server*.

United States Government Accountability Office. (2021, March 24). *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*. https://www.gao.gov/products/gao-21-288

Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information and Computer Security*, *24*, 139–151. https://doi.org/10.1108/ICS-12-2015-0048

Whitaker, B. (2021, February 14). *Unprecedented Russian SolarWinds hack that infiltrated federal government likely still happening*. CBS. https://www.paramountplus.com/shows/60_minutes/video/BJMDBl_P14QPGckrQzu9n3yMRUEzNZMc/unprecedented-russian-solarwinds-hack-that-infiltrated-federal-government-likely-still-happening/

Wood, R., & Bandura, A. (1989). Social Cognitive Theory of organizational management. *Academy of Management Review*, *14*, 361–384. https://doi.org/10.5465/AMR.1989.4279067