CYBERSECURITY: A REVIEW OF HUMAN-BASED BEHAVIOR AND BEST PRACTICES TO MITIGATE RISK

by

JIMMY W. HARPER

B.S., Middle Georgia State University, 2010

M.S., Kennesaw State University, 2012

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment of the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA
2023

Cybersecurity: A review of human-based behavior and best practices to mitigate risk

Jimmy W. Harper, *Middle Georgia State University, jimmy.harper@mga.edu*

Abstract

Cybersecurity-related threats and compromises are a constant concern for organizations. An incident can cause an organization to face financial and reputational loss. This article attempts to review the human element related to cybersecurity and the basic practices an organization can deploy to mitigate the amount of risk in the cyber environment. The research reviews articles with a focus on cybersecurity, human behavior, organizational culture, and overall awareness. From this research, a set of themes emerge that indicate the importance of the human element involved in mitigating cyber-related risk. While it is difficult to discuss all of the techniques that can aid an organization create a well-rounded, cyber-aware employee, this research indicates a few focus areas that organizations can use to establish their cybersecurity culture. This research also indicates that future research is needed to fully understand the impact that deploying these techniques can have on an organization's ability to mitigate cyber-related threats and compromises.

Keywords: cybersecurity, awareness, human, behavior, culture

Introduction

It is critical in the current electronic work environment to create a culture of cybersecurity awareness for all employees. The threat of cyberattacks is very prevalent, and some organizations are still not well-equipped to mitigate their risk. All organizations are at risk of a cyberattack regardless of their shape, size, or market sector (Phair & Alavizadeh, 2022). While organizations often rush to ensure that they are scanning their networks for vulnerabilities and patching their endpoints, there is one area of cybersecurity that is often overlooked, the employee. Employees need a certain level of access and trust to perform their day-to-day functions at an organization. Unfortunately, the human element is often involved when a cyberattack is successful.

Even though systems are configured with security measures, those measures may be compromised by humans (Scala et al., 2019). For this reason, organizations need to focus on putting the proper measures in place to minimize the chance that one of their employees will fall victim to a cyberattack that leads to a data breach. Therefore, procedures that encourage sharing information play an important role in enhancing cybersecurity, as well as standardized leadership methods and security policies (Pavlova, 2020).

This research examined the different methods used in cybersecurity to identify and mitigate human vulnerabilities in an organization. In addition, this research explains that implementing these practices can help reduce the risk of the human element. This review describes human-based behavior and the impact it can have on an organization’s cybersecurity awareness culture. The findings in this review reveal best practices that organizational leaders can use to mitigate the risk of human-enabled cyberattacks. These best practices were used to develop a conceptual model to help organizations understand how to enhance cybersecurity awareness.

The research provides answers to the following question:

RQ1: What are some best practices organizations can implement to minimize cybersecurity threats that can be enabled by employees?

Review of the Literature

Organizations in today's world must establish a culture of cybersecurity awareness with all of their employees. Humans need to feel secure, and it is truly a part of our human nature and instinct (Seungmug, 2020). Enhancements in technology have greatly increased our ability to communicate with others but it has also exposed us to hackers, competitors, disgruntled co-workers, and other bad actors. Communication online ranges from personal to business while security measures range from hard (restrictive firewalls) to soft (authentication and passwords). The University of California Berkeley had some political scientists, engineers, and management theorists study businesses they deemed as high-reliability organizations such as nuclear power plants, naval aircraft carriers, and air traffic control centers (Batteau, 2011). Some organizations are highly specialized and must follow their established protocol to accomplish any task. As a result of studying these organizations, the group noticed some themes emerge such as constant training mode, accountability pushed to the lowest level, reliance on open and robust communications, and shared perceptions of hazards (Batteau, 2011). Developing an organizational culture is not a new concept and is something that many businesses need to establish if they want to be successful in their share of the market. The thought of creating an organizational culture through management and research gained traction back in the 1970s and then garnered scientific attention in the early part of the 1980s. Organizational culture is defined as a system of shared assumptions, values, and beliefs that govern how people in an organization behave. Essentially an organization is setting up a set of ground rules on how they want to function and react to certain situations. As with most things, some organizations likely do this better than others. Having a shared perception of hazards is key to developing a cybersecurity awareness culture. Cybersecurity is defined as a set of policies, tools, concepts, guides, actions, training, good practices, and technologies that can be used to protect cyberspace, organizations, and consumers. While a cybersecurity culture is defined as people's knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values concerning cybersecurity and how they manifest themselves in people's behavior with the help of information technology (Pavlova, 2020).

To establish an effective cybersecurity culture an organization must know the major problems they are facing. While cyber threats do change on a daily and even minute basis, there are some core aspects an organization can focus on to build its culture. There are five hard problems, scalability and composability, policy, security metrics, resilience, and human behavior. Studying these problems can help an organization determine a direction for its cybersecurity culture. Also, addressing the risk that is associated with each one of these problems will advance both the cybersecurity community and the risk community at an organization. The main purpose of this research is the human behavior problem. While computer systems are built with security measures, those measures are often compromised by human behavior. Establishing clear policies related to technology will help employees understand the correct way to proceed in a given situation. Policy and human behavior can be addressed and evolved by examining the integrity and vulnerabilities of particular systems (Scala et al., 2019). An important thing to keep in mind is that most employees want to do the right and they just need proper guidance. Organizations are responsible for providing this guidance through policies and effective training. Three board policy categories that are generally recognized are enterprise cybersecurity policies, technical cybersecurity policies, and issue-specific cybersecurity policies. Enterprise cybersecurity policies help establish the strategic direction for security initiatives, technical cybersecurity policies are focused on the specific standards and procedures that IT staff use to configure and maintain the infrastructure, and finally issue-specific cybersecurity policies are the guidelines, rules, and procedures that all employees must adhere to when uses certain IT resources or performing processes. Organizations should establish periodic reviews to ensure they are conducting these examinations, so they stay up with the latest best practices. Conducting these types of reviews will also help the organization develop effective training for their employees and keep it relevant. If an organization simply tells an employee the consequences of clicking on a phishing email it might raise their awareness, but if they show an employee how to also distinguish a legitimate email from a phishing email it will likely lift the employee's confidence (Cram et al., 2020). If an employee is confident, it will

increase their desire to take ownership of their cybersecurity awareness and thus lead to them becoming more vigilant. This vigilant employee will likely communicate with other employees to help them understand best practices and show them where they can receive guidance for given situations.

As an organization is going through the process of establishing its cybersecurity culture and arming its employees with cybersecurity awareness, they will most certainly ask themselves, how do we test our employees? One of the most common answers in the realm of cybersecurity currently is internal phishing. Phishing is defined as a fraudulent form of an email that solicits personal or financial information from the recipient, such as a password, username, or social security or bank account number (Resnik & Finn, 2018). Given this definition, it is easy to see this is an easy way to test an organization's level of cybersecurity awareness. Based on the results of this information it can tell an organization if they have employees that are cyber-aware or if they have a lot of work to do. There is, however, an ethical question that comes into the equation. One of the most significant ethical problems with internal phishing is that under real-world conditions they can violate informed consent, which is required by numerous laws, guidelines, and professional codes (Resnik & Finn, 2018). This creates a balancing act that organizations must manage to educate, test, and advance their employees. The cybersecurity problem is not like any other security problem countries have ever faced before (Harknett & James, 2011). With that being said, organizations must be willing to find new and creative ways to ensure their employees are prepared for the cyber dangers they will certainly face in the workplace every day.

Hiring the right person for a position in an organization is even more important today because there are so many other external factors that need to be managed in the workplace. Hiring an employee that can "buy in" to the value of cybersecurity policies and has an ethical orientation has become a necessity (Cram et al., 2020). An employee's appetite for cybersecurity awareness can make the difference in some organizations between a good or bad employee. Personality can be considered a better predictor of cybersecurity behavior than some other factors. Employees will tend to bring in a certain sense of morality and ethics with them based on their previous life experiences. To fully understand and analyze an employee's personality an organization can reflect on the "Big Five" which are conscientiousness, openness, agreeableness, neuroticism, and extraversion (Shappie et al., 2020).

Conscientiousness is related to the impulse to control behavior, openness is tied to the extent to which an individual's mind and experiences are complex and original, agreeableness is connected to their attitudes towards others, neuroticism is the contrast on emotional stability, and extraversion is an employee's Sociability and an energetic approach to the world (Shappie et al., 2020). When an employee's personality can match up with an organization's cybersecurity culture, then the right components are present to develop an employee who can be an asset to the organization. Having a vigilant employee is key to the success of any business.

On the complete opposite side of having a vigilant employee is coming in contact with someone interested in committing a cybercrime. There is still not a lot of knowledge about what characteristics are significant when identifying a cybercriminal (Leukfeldt, 2020). This can make it hard for an organization to identify someone that is potentially a bad actor in their company. Making this even harder for organizations is hiring someone that is a good employee initially but then is corrupted over time.

The knowledge needed to commit acts of cybercrime can come from technically skilled friends, forums, and chat channels (Leukfeldt, 2020). Given that the information to commit these acts is readily available and diverse, someone that has been a model employee can be tempted. That is why it is so important for organizations to emphasize physical security. Physical security focuses on protecting organizations from natural and man-made disasters. While physical security is not a new concept by any means, it is something that can help an organization minimize its risk. It can range from fences, secure doors, traffic controls, and

identification cards/badges, to internal safes and vaults (Seungmug, 2020). Most cybercriminals will take the electronic approach, but an organization should never neglect to secure its technology infrastructure.

As organizations develop a cybersecurity awareness culture and aim to hire the right employees, they will need some tools to aid them along the way. One of the main things for organizations to consider is how they want to manage their employees' credentials. Single-factor authentication is one of the foundational pieces of cybersecurity because it sets up the user with a standard username and password that they can use to access the information and tools they need to perform their jobs. The organization must entrust the employee with their credentials and expect that the employee will protect them based on the policies and training they have reviewed. One tactic that organizations can do to assist their employees in this effort is to force the employee, through technical policy, to update their password routinely. If an employee was to give out their password accidentally to a cybercriminal, the password would become invalid on the next required routine change. In today's world, this most likely will not occur soon enough to prevent a data breach so organizations need to do more. Another technical policy that organizations can enforce is password complexity which can consist of a mixture of allowed characters and lengths. Through this policy and training, organizations can educate their employees on how to create unique easily rememberable passwords and how to safeguard them. One of the most popular trends in cybersecurity over the past few years has been the use of two-factor authentication. It is a two-step verification process in which an employee must grant their consent twice to access a particular data set or tool. This particular safeguard can help employees that fall partially victim to a cybercriminal through a phishing scam or other means because without both consents the cybercriminal will not be able to access the employee's account. Just because the safeguards above are in place at an organization does not the business should forget about the training employees need to prevent an incident. Phishing emails continue to increase and gain a look of authenticity as the cybercriminal's skills and sophistication increase. The risk of a data breach as the result of a cyberattack has grown more serious in recent years and will likely continue to expand for the foreseeable future (Allen, 2018).

Organizations must always look for ways to mitigate risk and help their employees prevent cyberattacks. Incidents can consist of breaches in information related to confidentiality, integrity, availability, and damage to information systems resources; it is a wide spectrum to cover. The human equation is something that will likely always exist at some level because, for every vigilant employee, there is a cybercriminal enhancing their skills. Human threats can come from potential intrusions or lapses in handling, training, or monitoring personnel dealing with information resources (Zadeh, 2020). While there are many cybersecurity threats an organization must manage, the human equation is always involved at some level whether it is intentional or not. Organizations must also define their appetite for risk and work with employees to keep their level of risk in an acceptable range.

Methodology

Organizations need to measure and understand the cybersecurity culture amongst their employees continuously. As threats evolve and become more sophisticated the likelihood of an employee falling for an attempt increases. To help ensure that employees are aware of these threats and properly trained many organizations have hired cybersecurity professionals. The role of these professionals within the organization is to review and create policies and procedures, ensure those policies and procedures are being employed, generate cybersecurity awareness, provide adequate training, and provide safeguard techniques to minimize human behavior risks. A well-documented cybersecurity program should include everything across all categories and serve as a guide for recommendations (Perry, 2021).

A narrative review served as the methodology for this research. This type of methodology can be used to describe the management of a particular problem (Macapagal & Tablarin, 2021). The articles were selected through forward and backward citation searches based on the key articles found during the research. The

articles were restricted based on a date range of fewer than 15 years. This approach ensured the articles used to conduct the research were relevant to modern technology and cybersecurity methods. The articles were selected by limiting them to academic journals in GALILEO and scanning the titles and abstracts for the following terms cybersecurity, awareness, human, behavior, and culture. Inclusion criteria were based on a review of the article's abstract to determine if the article included relevant information as judged by this researcher.

The researcher used the information found in the selected articles to develop a set of emerging themes based on an iterative analysis. The contributions from the selected articles were identified and grouped into a set of theoretical foundations. From these themes, the researcher developed a thematic map that shows the relationships between cybersecurity, awareness, humans, behavior, and culture. The researcher used the information learned from this process to share results, further the discussion, and examine opportunities for additional research.

Results

A thorough review of academic journals reveals several themes and sub-themes related to cybersecurity and mitigating risks. Human behavior was one of the early themes to emerge in the documentation. Based on the reviews that were conducted there was a noticeable relationship between human behavior and personality along with their overall understanding of cybersecurity. Additionally, culture emerged as a key theme for the management of cybersecurity in organizations and how they communicate with employees and stakeholders. Training and awareness were also themes that were discovered during the review process. Policies and accountability have key roles in helping mitigate human behavior that can lead to loss of data. Security metrics applied to devices and system access at an organization can also limit human behavior that leads to data breaches. All of these findings have a significant role in mitigating human behavior that can open up organizations and individuals to cyberattacks. Regarding RQ1, the research results show that organizations need to focus on cybersecurity training, employee awareness of cyber-related threats, robust security metrics, policy development, a holistic culture of cybersecurity awareness, and the role of human behavior in mitigating cyber-related threats. Table 1 is a list of themes that emerged from the articles reviewed in this research. Figure 1 serves as a thematic map that shows how culture, training, awareness, and security metrics are all connected to human-based behavior related to cybersecurity.

Table 1: List of Themes by Articles

Year	Authors	Themes
2018	Allen and Hallene (2018)	Security Metrics
2011	Batteau	Culture
2020	Cram, Proudfoot, and D'Arcy (2020)	Accountability, Awareness, Human Behavior, and Training
2011	Harknett and James	Policies
2020	Leukfeldt (2020)	Human and Behavior
2018	Resnik and Finn (2018)	Training and Phishing
2020	Pavlova (2020)	Culture, Communication, and Organization
2019	Scala, Reilly, Goethals, and Cukier (2019)	Deployment, Human Behavior, Policies, and Security Metrics
2020	Seungmug (2020)	Human and Security Metrics
2020	Shappie, Dawson, and Debb (2020)	Human Behavior, Personality, and Understanding
2020	Zadeh, Jeyaraj, and Biros (2020)	Human, Understanding, and Training

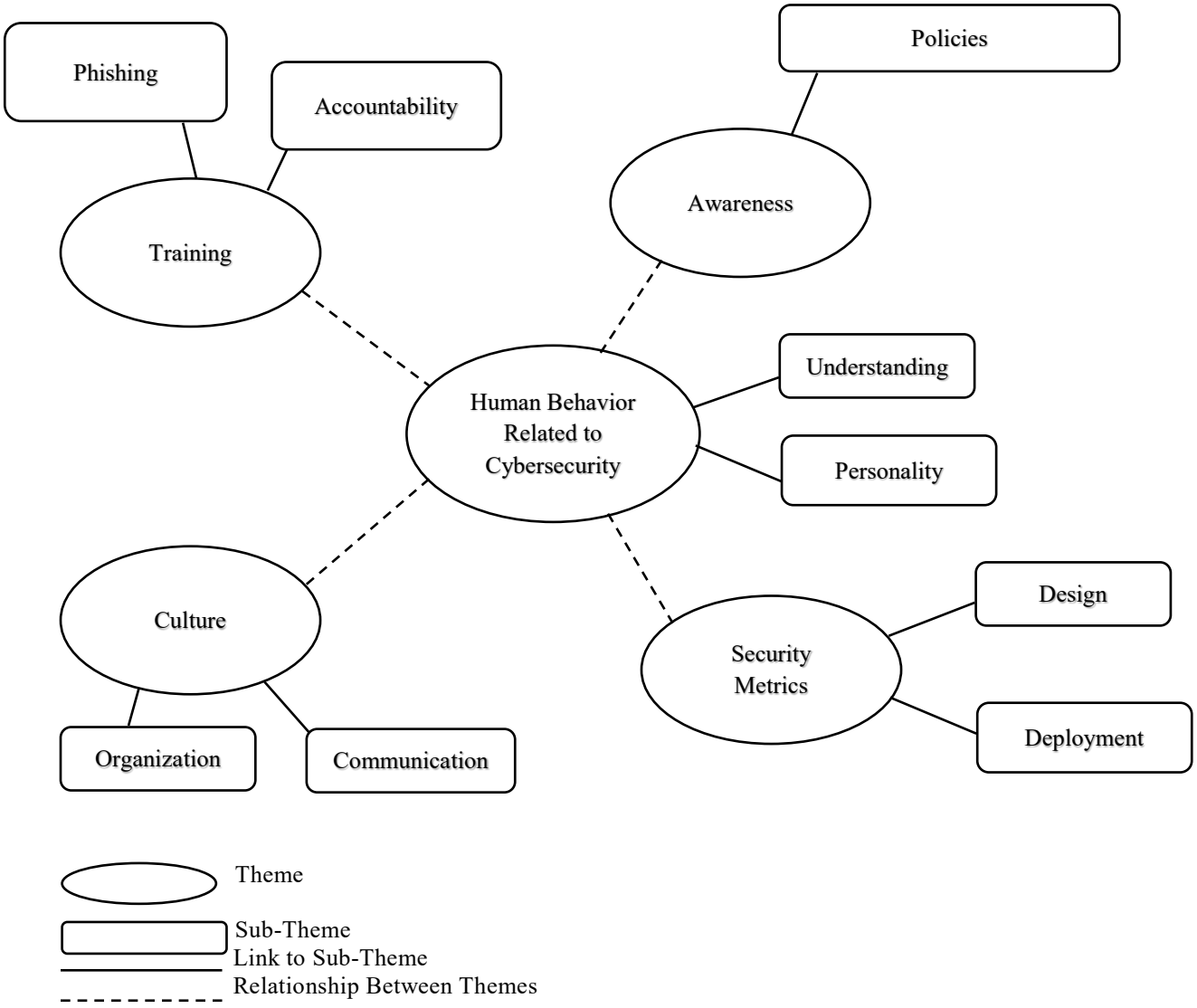

Figure 1: Thematic Map of Human-Based Behavior

Conclusion

The results presented here suggest that organizations can mitigate their cyberattack risks by ensuring that employees have appropriate training, understand establish security metrics, have general cybersecurity awareness, and become a part of a culture that embraces the benefits of cybersecurity. It is up to organizational leadership to set the tone when it comes to the culture of cybersecurity awareness. Investing in cybersecurity awareness and knowledge development is the best way to create sustainable behavioral change (Pavlova, 2020). By placing employees into real-world situations with training and awareness programs organizations can gain valuable knowledge that helps them set up effective countermeasures to mitigate risk (Resnik & Finn, 2018). Most individuals want to do the right thing and perform their job duties well, but organizational leadership must place a focus on developing their employees the right way. Human behavior is a problem in cybersecurity that must be addressed and no matter how many safeguards are put into place those measures can always be compromised by human behavior (Scala et al., 2019).

Overall, many opportunities exist for analyzing techniques that mitigate the risk of cyber-related threats and compromises. Through employee education, organizations can limit their risks and can create a culture of understanding and learning. By investing and improving the organization's cybersecurity practices with a focus on improving an individual's sense of self-efficacy; an organization can decrease an employee's perceived barriers to cybersecurity practices (Shappie et al., 2020). This tactic will strengthen their workforce peer support and a desire to protect the organization's information and reputation. Employees must understand the true impact a compromise can have on their organization. While organizations can address their liability in a data security breach through cybersecurity risk policies, it can come with a major loss of financial status and present trust issues for others (Allen & Hallene, 2018). Following the recommendations in this article will help organizations trend in the right direction to limit their exposure to cybersecurity-related threats and compromises.

With continuous changes in technology, it is impossible to cover every avenue that can help an organization mitigate the risk of a cyber-related threat. Additional research is needed to fully investigate the impact of the techniques suggested in this article. There is an ongoing struggle to organizations face when trying to achieve a high level of compliance with cybersecurity-related policies and procedures (Cram et al., 2020). Studying an organization that implements these techniques over several years will indicate the success of these measures. Also, research needs to be conducted in different industries such as education, finance, manufacturing, medicine, and technology to name a few. This type of research will help indicate what techniques are more beneficial in certain industries to help an organization prioritize its focus and funds.

References

Allen, J., & Hallene, A. (2018). Privacy and Security Tips for Avoiding Financial Chaos. American *Journal of Family Law*, *32*(3), 101–107.

Batteau, A. W. (2011). Creating a Culture of Enterprise Cybersecurity. *International Journal of Business Anthropology*, *2*(2), 36–47.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). Maximizing Employee Compliance with Cybersecurity Policies. *MIS Quarterly Executive*, *19*(3), 183–198. https://doi.org/10.17705/2msqe.00032

Harknett, Richard J., James A. Stever, Richard J. Harknett, & James A. Stever. (2011). The New Policy World of Cybersecurity. *Public Administration Review*, *71*(3), 455–460. https://doi.org/10.1111/j.1540-6210.2011.02366.x

Leukfeldt, R. (2020). The Human Factor Examined: Directions for Future Research. *International Journal of Cyber Criminology*, *14*(1), 67–75.

Macapagal, J., & Tablarin, S. G. A. (2021). Implicated Guidelines of Cost-efficient Teledentistry during the COVID-19 Pandemic for a Developing Country: A Narrative Review. *Applied Medical Informatics*, 43(4), 112–123.

Pavlova, E. (2020). Enhancing the Organisational Culture related to Cyber Security during the University Digital Transformation. *Information & Security*, *46*(3), 239–249. https://doi.org/10.11610/isij.4617

Perry, P. M. (2021). Establishing a Cybersecurity Program for My Size Entity. *Journal of Pension Benefits: Issues in Administration*, 29(1), 4–9.

Phair, N., & Alavizadeh, H. (2022). Cybersecurity skills of company directors — ASX 100. *Journal of Risk Management in Financial Institutions*, 15(4), 429–436.

Resnik, D. B., & Finn, P. R. (2018). Ethics and Phishing Experiments. *Science & Engineering Ethics*, *24*(4), 1241–1252. https://doi.org/10.1007/s11948-017-9952-9

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the Five Hard Problems of Cybersecurity. *Risk Analysis: An International Journal*, *39*(10), 2119–2126. https://doi.org/10.1111/risa.13309

Seungmug (Zech) Lee. (2020). A Basic Principle of Physical Security and Its Link to Cybersecurity. *International Journal of Cyber Criminology*, *14*(1), 203–219. https://doi.org/10.5281/zenodo.3749780

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, *9*(4), 475–480. https://doi.org/10.1037/ppm0000247

Zadeh, A. H., Jeyaraj, A., & Biros, D. (2020). Characterizing Cybersecurity Threats to Organizations in Support of Risk Mitigation Decisions. *E-Service Journal*, *12*(2), 1–34. https://doi.org/10.2979/eservicej.12.2.01