Oct 30th, 1:00 PM - 1:30 PM

TOWARDS ASSESSING PASSWORD WORKAROUNDS AND PERCEIVED RISK TO DATA BREACHES FOR ORGANIZATIONAL CYBERSECURITY RISK MANAGEMENT TAXONOMY

Michael J. Rooney
Nova Southeastern University, mr2640@mynsu.nova.edu

Yair Levy
Nova Southeastern University, USA, levyy@nova.edu

Wei Li
Nova Southeastern University, lwei@nova.edu

Ajoy Kumar
Nova Southeastern University, akumar@nova.edu

Abstract

Cybersecurity involves a broad range of techniques, including cyber-physical, managerial, and technical, while authentication provides a layer of protection for Information Systems (IS) against data breaches. The recent COVID-19 pandemic brought a tsunami of data breach incidents worldwide. Authentication serves as a mechanism for IS against unauthorized access utilizing various defense techniques, with the most popular and frequently used technique being passwords. However, the dramatic increase of user accounts over the past few decades has exposed the realization that technological measures alone cannot ensure high level of IS security; this leaves the end-users holding a critical role in protecting their organization and personal information. Despite users being more aware of password entropy, users still often participate in deviant password behaviors also known as 'password workarounds' or 'shadow security'. These deviant password behaviors can put individuals and organizations at risk resulting in data privacy issues, data loss, and ultimately a data breach incident. In this paper, we outline a research-in-progress study to build a risk taxonomy for organizations based on the to identify the risks associated with deviant password behaviors technique based on the constructs of users' perceived cybersecurity risk of data breaches resulting from PassWord WorkArounds (PWWA) techniques. Additionally, this study aims to empirically assess significant mean difference between Subject Matter Experts (SMEs) and employees on their perceived cybersecurity risk of data breaches resulting from the deviant password behaviors and frequency of PWWA techniques usage.

Location

Online Zoom Session

Disciplines

Information Security | Management Information Systems | Technology and Innovation

Comments

Keywords: Cybersecurity risk, cybersecurity management, password workarounds, shadow security, risk to data breach, cyber risk taxonomy.

INTRODUCTION

Data breaches and ransomware incidents are documented daily in the news media, while a tsunami of such incidents have been observed in the United States (US) both for organizations as well as individuals, mainly because of the recent COVID-19 pandemic (Levy & Gafni, 2021). The most recent yearly report by the Federal Bureau of Investigation (FBI)'s Internet Crime Complaint Center (IC3) (2020) indicated that "a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding $4.1 billion. This represents a 69% increase in total complaints from 2019" (p. 3). Such cyber-attacks are not focused on US entities only. The European Union Agency for Cybersecurity (ENISA) (2020) identified that data breaches have increased by 54% from 2018 to mid-2019, with over 3800 breaches being reported exposing 4.1 billion records. About 64% of those data breaches were password data exposure, which increased 25% from previous years (ENISA, 2020). Joseph (2018) defined a data breach as disclosing an organization's protected confidential data through unauthorized access. According to the Ponemon Institute (2020), the global average cost of data breaches was $3.86 million, and malicious attacks were responsible for 52% of those data breaches, with compromised credentials making up 19% of the malicious attacks. Data breaches are crucial to research in cybersecurity, and although critical, empirical work is scarce at an independent level and most deal with data breaches after the fact introducing various biases (Goode et al., 2017). Thus, it appears that the limited number of research studies in individual areas of data breach, such as the use of deviant password behaviors that may create a cybersecurity risk of data breaches, can help contribute to the overall body of knowledge. Therefore, the goal of this work-in-progress research is to develop a taxonomy to identify the risks associated with deviant password behaviors technique based on the constructs of users' perceived cybersecurity risk of data breaches resulting from PassWord WorkArounds (PWWA) techniques and frequency of PWWA techniques usage. Additionally, this study aims to empirically assess if there is a significant mean difference between *perceived cybersecurity risk of data breaches* resulting from the deviant password behaviors and frequency of PWWA techniques usage, using inputs from Subject Matter Experts (SMEs) and employees. This work-in-progress study will use a web-based survey and is aimed to address the following Research Questions (RQs):

RQ1. What are the SMEs' validated PWWA techniques that were identified in literature?

RQ2. What are the SMEs' identified measures for perceived cybersecurity risk of data breaches resulting from each of the validated PWWA techniques?

RQ3. What are the most frequently reported used PWWA techniques indicated by SMEs reported frequency of employees' engagement in PWWA Techniques?

RQ4. What are the employees' aggregated perceived cybersecurity risk of data breaches as a result of each of the validated PWWA techniques?

RQ5. Are there any statistically significant mean differences in employees' aggregated perceived level of cybersecurity risk of data breaches as a result of each of the validated PWWA techniques compared to those indicated by SMEs?

RQ6. What are the most frequently self-reported used PWWA techniques indicated by employees' engagement in PWWA Techniques?

RQ7. What are the most frequently reported used PWWA techniques indicated by employees' reported frequency of co-workers' engagement in PWWA Techniques?

RQ8. How are the PWWA techniques positioned on the Proposed Password Workaround Cybersecurity Risk Taxonomy (PaWoCyRiT) using the aggregated score of perceived cybersecurity risk of data breaches resulting from the PWWA techniques VS. frequency of PWWA techniques usage?

BACKGROUND

In this section, we provide a brief overview of the theoretical background used to formulate this research. We start with a definition and review of Password Workaround, then will briefly discuss the role of password in data breach incidents, followed by defining information security risk and how perceptions of the risk to data breach are relevant to the overall cybersecurity posture of organizations.

Password Workarounds

A workaround is when an employee uses deviated actions from those enforced by their organizational policies and procedures (Patterson, 2018). Unfortunately, some employees perceive their organizational password policies and procedures as barriers while engaged in PWWA to achieve a faster result or make a task easier (Patterson, 2018). These actions of creating PWWA fall into a category of security behavior coined as "shadow security" or "shadow Information Technology (IT)" where employees feel they cannot comply, or unacquainted, with organizational policies and procedures put in place to protect information assets resulting in the use of non-compliant alternative techniques (Kirlappos et al., 2015; Sillic, 2019). Passwords are used as an access control mechanism providing user authentication, which is the first line of defense, to access IS resources and services (Wang et al., 2017). Previous research has suggested the following actions are considered insecure password techniques: reusing passwords, creation of weak passwords,

writing passwords down, and sharing passwords (Chanda, 2016; Chowdhury et al., 2020; Dang-Pham et al., 2017; Kaleta et al., 2019; Kirlappos et al., 2015; Woods & Siponen, 2019). Ives et al. (2004) described the severity of these techniques, such as the reuse of passwords, suggesting they can result in the domino effect. For example, suppose a user has multiple password-protected accounts, including one for the organization they work for, and they reuse the same weak password for all those accounts. In that case, all their accounts will be at risk if just one of those account passwords is compromised (Ives et al., 2004). Levy and Gafni (2021) also outline such domino effect and provided multiple cases on the massive impact it can have not only on a single company but on a whole industry. Although there are several disadvantages of using passwords, and much research has gone into finding new alternatives such as biometrics and multifactor authentications, it has been shown that the "password scored highest in terms of preference, usability, … and lowest in terms of perceived effort and expected problems" (Zimmermann & Gerber, 2020, p. 6). However, the results of these poor PWWA practices have been damaging not only in the past but in recent news with the data breaches compromising user accounts: "Adobe (150 million), Evernote (50 million), Anthem (40 million), Rockyou (32 million), Tianya (30 million), Dodonew (16 million), 000webhost (15 million), Gmail (4.9 million) and Phpbb (255 K)" (Wang & Wang, 2018, p. 708).

The basic types of authentication techniques include token-based 'something you have', biometric-based 'something you are', and knowledge-based 'something you know' (Bhanushali et al., 2015). Another authentication type is behavioral-based 'something you do' which utilize behavioral attributes to authenticate (Mahfouz et al., 2017). The number of passwords an individual needs is set to increase as users are required to have various accounts, not only for work but also for personal matters, resulting in increased cybersecurity risks (Woods & Siponen, 2018). According to AlFayyadh et al. (2012), previous research suggested that individuals mentally classify accounts based on their perceived importance. In this instance, they would practice PWWA, such as reusing passwords for accounts perceived as low importance. As defined by Shay et al. (2010), password entropy is a measure of the difficulty in predicting the value of a variable or, in this case, cracking a password. The higher the difficulty of cracking a password depends on the size of the password's entropy values, which would determine the number of guesses and time it would take to identify the set password (Shen et al., 2016). Many tools and techniques exist for stealing or cracking passwords, such as brute-force attack, dictionary attack, spyware attack, shoulder surfing, phishing, and other social engineering techniques (Bhanushali et al., 2015). To prevent individuals from becoming victims of these attacks, most organizations implement a password policy to enforce a password complexity for strength. Additionally, research has shown that when password entropy is too complicated, employees may forget their

set passwords, which costs time and resources to get the password reset (Mujeye et al., 2016). At the same time, the guidance from industry experts on what constitute a complex password has been confusing over the years. In the past decades, National Institute of Standards and Technology (NIST) provided requirements for the US federal government on proper users' authentication to government IS where the key focus of the requirements was on the use of complex password via combining different types of characters to increase password entropy via combination of letters, symbols, and numbers (NIST, 2004; Grassi et al., 2017). However, in the recent NIST Special Publication (SP) 800-63-3 (2021), which marks the second update within three years, they emphasize the length of the password is more important and advocate for the use of passphrases. The differences ease enforcement of password requirements by recommending the following changes: removal of the password expiration, removal of the requirement for special characters, allowing all characters to be used (including spaces), allowing the copying and pasting of passwords, and increasing the allowed number of characters. According to Topper (2018), NIST initially made these changes in 2017 based on the suggestions that traditional password security encouraged the use of deviant security behavior such as the identified PWWA. The use of PWWA has been heavily researched (Lin et al., 2013; Safa et al., 2015; Siponen et al., 2020; Stanton et al., 2005; Sun et al., 2012; Whitty et al., 2015; Woods & Siponen, 2018; Woods & Siponen, 2019) in different capacities to identify solutions on how to remediate employees from using such techniques. However, even with such guidelines, users still use PWWA to remember these passwords, such as creating weak passwords or passphrases to meet the minimum requirements (Wang et al., 2017).

Data Breaches

Despite this past work on password security, recent research conducted by Brason (2020) highlighted that 42% of IT and Security Managers identified user password compromise as the leading cause of data breaches. Memorization of passwords is a well-researched topic in password security due to most research identifying IS users frequently use weak passwords that are easy to remember and reuse passwords across multiple accounts (Sun et al., 2012). According to the 2020 Verizon Data Breach Investigations Report, 45% of breaches featured hacking, and 80% of those hacking breaches utilized lost/stolen or brute-forced credentials. A brute force attack uses every combination of letters and numbers to crack the original password; the weaker the combination, the faster the password will be cracked (Chanda, 2016). Stolen credentials, generally for sale on the black market, are a cybersecurity risk for organizations whose employees reuse passwords; this warrants some organizations to monitor these black-market sites and send notifications to users who may be victims (Golla et al., 2018). Thomas et al. (2017)

research has identified that there are "1.9 billion usernames and passwords exposed via data breaches and traded on blackmarket forums" (p. 1433). Users were unaware of how frequently these poor password techniques are used by others (Ur et al., 2016). Thus, empirical research is needed to determine employee's perceptions of the likelihood and impact of data breaches (i.e., risk) resulting from the frequency and use of PWWA.

Information Security Risk

Information security risk is defined by Kissel (2013) as:

> The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. (p. 161)

Risk of data breaches has been widely researched in IS since the 1970s with smaller platform physical access ultimately advancing to larger platforms when Internet access became widely available (Goode et al., 2017). Although data breaches are transpiring more frequently and becoming more severe, it seems organizations and individuals are not perceiving the severity of the risk of data breach (D'Arcy et al, 2020). Passwords that are lost or stolen pose problems beyond just password resets such as a risk of data breach due to users practicing PWWA; reusing passwords or creating weak passphrases (Thomas et al., 2017). Risk management, to mitigate the chance of data breaches, has been applied in many aspects of most organization's information security program from instilling it in the development of software to handling security incidents to contain any adversarial attacks (Khan et al., 2021). Unfortunately, when it comes to estimation of information security risk, both individuals and organizations are underestimating the likelihood of a data breach as well as the massive impact it can have. Academic research continues to work on isolating certain factors that play a significant part into the risk, or impact and likelihood, an organization will experience leading to a data breach since this continues to be a prominent problem (D'Arcy et al., 2020). Elmrabit et al. (2020), explored a way to predict an insider threat's risk to data breach before an occurrence claiming that insider threat is a significant risk to an organization due to their familiarity and authorized access. Previous research lacks deeper insight into how to properly and effectively handle data breaches, however, there is a significant need to gain a better understanding on the risks of data breach (Khan et al., 2021).

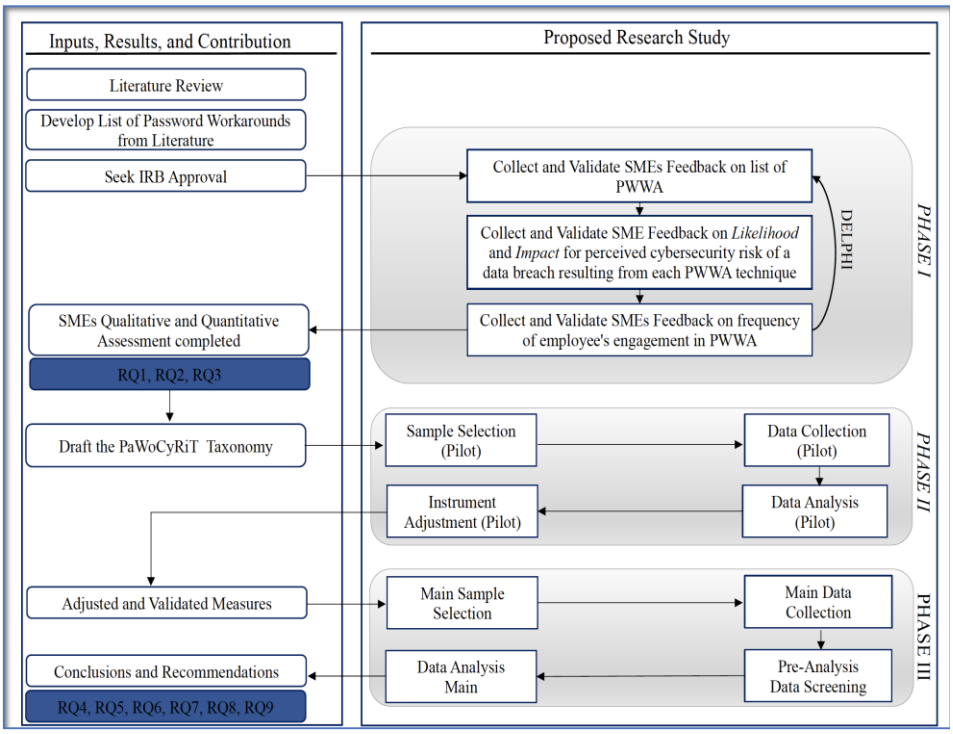
PROPOSED METHODOLOGY

This work-in-progress study is a developmental design conducted in three phases

utilizing qualitative and quantitative methods (Ellis & Levy, 2009). Collecting both data sets, qualitative and quantitative, is considered a sequential mixed methods approach and is a suitable method for the developmental design providing a viable empirical measurement (Creswell & Clark, 2017). Developmental research can be seen as bridging theory and practice and can lead to new methods, models, and tools to solve organizational problems (Ellis & Levy, 2010). The proposed research design is depicted in Figure 1, an overview of the research design process to develop and validate the proposed Password Workaround Cybersecurity Risk Taxonomy (PaWoCyRiT). In the first phase, a literature review will be conducted to compile a list of PWWA provided to the SMEs for validation. The validated list of PWWA will then be used for the SMEs to provide feedback on the likelihood and impact of perceived cybersecurity risk of data breaches for each technique addressing RQ1 and RQ2. The SMEs will also be asked to provide feedback on the frequency of employees' engagement in using each PWWA technique, which will address RQ3. Phase two will consist of a pilot selection, collection, adjustment, and analysis. The pilot will be conducted to ensure reliability and validity, plus identify if any measurement issues will hinder the results (Straub, 1989). The adjusted and validated measurements will then be used in phase three for main data collection,

Figure 1

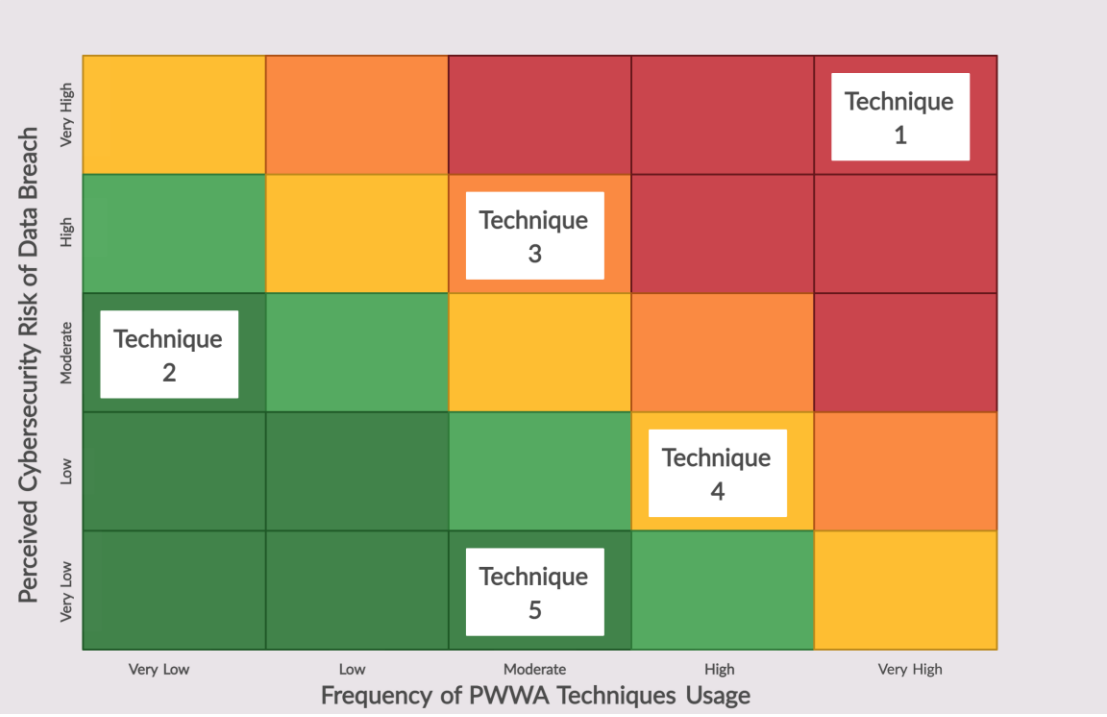
An overview of the research design process to develop and validate the PaWoCyRiT.



surveying employees' perceptions on the likelihood and impact of cybersecurity risk of data breaches for each technique. The employees will then be asked about their co-worker's frequency use of the validated PWWA, collecting demographics data simultaneously, which will allow to address RQ4 to RQ6. Additionally, this work-in-progress study will use the validated measures of perceived cybersecurity risk of data breaches resulting from each PWWA technique and the frequency of PWWA techniques. We will then use these two constructs to construct the PaWoCyRiT as shown in Figure 2, which currently only depict how the proposed taxonomy will look, but once data is collected, each of the PWWA techniques will be positioned based on its averaged level of the two constructs on the taxonomy to further indicate the level of risk such PWWA technique is posing to the organization (See Figure 2). Once the main data is collected, aggregated scores of perceived cybersecurity risk of data breaches resulting from each PWWA technique and the frequency of PWWA techniques usage reported by SMEs and employees about their co-workers will be computed, the PaWoCyRiT will be constructed using these numbers for each PWWA techniques to address RQ7.

Figure 2

The Proposed Password Workaround Cybersecurity Risk Taxonomy (PaWoCyRiT)



Proposed Sample Size

This research-in-progress study will consist of SMEs with backgrounds in cybersecurity and employees who are frequent users of IS for work and personal use. According to Terrell (2016), "sample size should be large enough to allow for equal representation of the characteristics that you have identified as important" (p. 66). A panel of SMEs used in research studies does not have size limitations, but due to this proposed research study soliciting SMEs with high-level credentials, the size is recommended to consist of 20 to 25 SMEs (Skinner et al., 2015). The group of SMEs will be required to have an extensive background in cybersecurity based on the following criteria: a practical level of cybersecurity experience (greater than ten years), advanced industry IT/Cybersecurity certifications, and education relating to cybersecurity; the aim will be to have 25 SMEs participants while soliciting up to 50 SMEs. This work-in-progress research study will aim at a minimum of 100 employee participants; too small a sample size may cause inconclusive results. Research has suggested that the ideal sample size is between 30 and 550 (Sekaran & Bougie, 2016). We plan to solicit 500 participants to alleviate any issues of not receiving enough participants for the sample size to reach the minimum goal of 100 participants.

According to Levy (2006), "pre-analysis data preparation deals with the process of detecting irregularities or problems with the collected data" (p. 153). This work-in-progress research study will utilize a web-based survey platform to collect data from SMEs and employees for the Delphi method, pilot data collection, and main data collection. The pre-analysis collection will be used to validate the quality of the data being collected and try to mitigate any discrepancies prior to the main data collection. The advantages of using a web-based survey platform are the data can be collected from participants at their convenience, and the automatic collection of responses will allow for a more efficient process for data analysis.

CONCLUSIONS AND DISCUSSIONS

This work-in-progress research study will develop a list of PWWA, validated the list by SMEs, and develop a measure to assess the perceived cybersecurity risk of data breaches associated with each PWWA technique, along with the perceived frequency of use by co-workers. The data will be collected using the Delphi method, with a panel of SMSs and employees, using the developed web-based 7-point Likert scale survey and conduct the data analyses. The main data collection and analysis will be used to empirically test and develop the PaWoCyRiT. An expected research outcome would be to recognize if there is a disconnect between what SME's experiences are when dealing with data breaches and the use of PWWA compared to what daily IS users experience. The significance of this proposed research would be to provide a risk taxonomy showing the perceived

cybersecurity risk of data breaches resulting from each of the validated PWWA techniques and the frequency of the use of the validated PWWA techniques. In addition, the taxonomy developed could help organizations identify groups of users who may pose a higher risk to organizations and be used as a powerful tool to map employees, breaking it down into subgroups, determining who will need to be trained or retrained and the PWWAs that the organizations should be focused on.

REFERENCES

AlFayyadh, B., Thorsheim, P., Jøsang, A., & Klevjer, H. (2012). Improving usability of password management with standardized password policies. *Proceedings of the 7th Conference on Network and Information Systems Security (SAR-SSI)*, 38–45.

Bhanushali, A., Mange, B., Vyas, H., Bhanushali, H., & Bhogle, P. (2015). Comparison of graphical password authentication techniques. *International Journal of Computer Applications*, *116*(1), 11-14.

Brason, Steve (2020). Contextual awareness: Advancing identity and access management to the next level of security awareness. *Enterprise Management Associates Summary Research Report,* 1-21.

Chanda, K. (2016). Password security: An analysis of password strengths and vulnerabilities. *Computer Network and Information Security*, *7*, 23–30.

Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, *97*, 1-13.

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Applications of social network analysis in behavioural information security research: Concepts and empirical analysis. *Computers and Security*, *68*, 1–15.

D'Arcy, J., Adjerid, I., Angst, C. M., & Glavas, A. (2020). Too good to be true: Firm social performance and the risk of data breach. *Information Systems Research, 31*(4), 1200–1223.

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, *6*, 323-337.

Ellis, T. J., & Levy, Y. (2010). A guide for novice researchers: Design and development research methods. *Proceedings of the 2010 InSITE Conference*, *10*, 107–118.

Elmrabit, N., Yang, S., Yang, L., Zhou, H. (2020). Insider threat risk predication based on Bayesian network. *Computers & Security*, *96*, 1-19.

ENISA. (2020). Threat landscape 2020 data breach. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach

Federal Bureau of Investigation (FBI) (2020). Internet crime report 2020. *Internet Crime Complaint Center (IC3)*. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Golla, M., Filipe, L., Wei, M., Dürmuth, M., Ur, B., Hainline, J., & Redmiles, E. (2018). What was that site doing with my Facebook password? Designing password-reuse notifications. *Proceedings of the ACM Conference on Computer and Communications Security*, 1549–1566.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action. *MIS Quarterly*, *41*(3), 703-727.

Grassi, P. A., Garcia, M. E., Fenton, J. L. (2017). Digital identity guidelines. National Institute of Standards and Technology, Gaithersburg, MD, Special Publication Series (800), NIST SP 800-63-3, Updated 03-02-2020.

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM*, *47*(4), 75-78.

Joseph, R. C. (2018). Data breaches: Public sector perspectives. *IT Professional*, *20*(4), 57–64.

Kaleta, J. P., Lee, J. S., & Yoo, S. (2019). Nudging with construal level theory to improve online password use and intended password choice: A security-usability tradeoff perspective. *Information Technology and People*, *32*(4), 993–1020.

Khan, F., Kim, J.H., Mathiassen, L., Moore, R. (2021). Data breach management: An integrated risk model. *Information & Management*, *58*, 1-12.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). Shadow security as a tool for the learning organization. *ACM SIGCAS Computers and Society*, *45*(1), 29-37.

Kissel, R. (2013). *Glossary of key information security terms (NIST IR 7298r2).* National Institute of Standards and Technology (NIST). http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2 .pdf

Levy, Y. (2006). Assessing the value of e-learning systems. Hershey, PA: Information Science Publishing.

Levy, Y., & Gafni, R. (2021). Introducing the concept of cybersecurity footprint. *Information and Computer Security*, 1-13. https://doi.org/10.1108/ICS-04-2020-0054

Lin, S. C., Yen, D. C., Chen, P. S., & Lin, W. K. (2013). Coding behavior of authentication code on the internet. *Computers in Human Behavior*, *29*(5), 2090-2099.

Mahfouz, A., Mahmoud, T. M., & Eldin, A. S. (2017). A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications*, *37*, 28–37.

Mujeye, S., Levy, Y., Mattord, H., & Li, W. (2016). Empirical results of an experimental study on the role of password strength and cognitive load on employee productivity. *Online Journal of Applied Knowledge Management*, *4*(1), 99–116.

National Institute of Standards and Technology (NIST) (2004, Jun 30). Electronic Authentication Guideline. *NIST Special Publication 800-63*. https://csrc.nist.gov/CSRC/media/Publications/sp/800-63/ver-10/archive/2004-06-30/documents/sp800-63-v1-0.pdf

National Institute of Standards and Technology (NIST) (2021, Jul 29). Digital identity guidelines: Authentication and lifecycle management. *NIST Special Publication 800-63-3*. https://pages.nist.gov/800-63-3/sp800-63-3.html

Patterson, E. S. (2018). Workarounds to intended use of health information technology: A narrative review of the human factors engineering literature. *Human Factors*, *60*(3), 281–292.

Ponemon Institute (2020). Cost of a data breach report. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf=

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65-78.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th Ed.). West Sussex, United Kingdom: John Wiley & Sons Ltd.

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., & Cranor, L. F. (2010). Encountering stronger password requirements: User attitudes and behaviors. *ACM International Conference Proceedings of the 6th Symposium on Usable Privacy and Security*, 1-20.

Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers and Security*, *61*, 130–141.

Sillic, M. (2019). Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the shadow IT context. *Computers and Security*, *80*, 108–119.

Siponen, M., Puhakainen, P., & Vance, A. (2020). Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Computers and Security*, *88*, 1-12.

Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems, 37*(1), 31-63.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security, 15*(4), 708-722.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.

Sun, H. M., Chen, Y. H., & Lin, Y. H. (2012). oPass: A user authentication protocol resistant to password stealing and password reuse attacks. *IEEE Transactions on Information Forensics and Security*, *7*(2), 651–663.

Terrell, S. R. (2016). *Writing a proposal for your dissertation*. Guilford.

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., Margolis, D., Paxson, V., & Bursztein, E. (2017). Data Breaches, phishing, or malware? Understanding the risks of stolen credentials. *Proceedings of the ACM Conference on Computer and Communications Security*, 1421–1434.

Topper, J. (2018). Compliance is not security. *Computer Fraud and Security, 3*, 5-7.

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). Do users' perceptions of password security match reality? *Conference on Human Factors in Computing Systems Proceedings*, 3748–3760.

Verizon. (2020). 2020 data breach investigations report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Wang, D., & Wang, P. (2018). Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE Transactions on Dependable and Secure Computing*, *15*(4), 708–722.

Wang, D., Cheng, H., Wang, P., Huang, X., & Jian, G. (2017). Zipf's law in passwords. *IEEE Transactions on Information Forensics and Security*, *12*(11), 2776-2791.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7.

Woods, N., & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human Computer Studies*, *111*, 36–48.

Woods, N., & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human Computer Studies*, *128*, 61–71.

Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. *International Journal of Human Computer Studies*, *133*, 26–44.