Evaluating Self-Efficacy Pertaining to Cybersecurity for Small Businesses

Ellen M. Raineri
Penn State University

Jessica Resig
Penn State University

Small businesses are easy victims of cyberattacks due to their limited resources and insufficient training. Furthermore, many small business owners' attitudes diminish their need for safeguards because they think that they are not likely to be attacked. Yet, small businesses experience Denial of Service (DoS) attacks, Distributed Denial of Service (DDos) attacks, phishing, vishing, and tail gating as well as theft of confidential information and hardware. Consequently, numerous small businesses close or experience detrimental results -- loss of consumer trust, lawsuits, credit monitoring fees, tarnished reputations, and lost operational costs. Since past research demonstrated that training positively impacts self-efficacy, this paper explores the effects of cybersecurity training on participants' self-efficacy towards small business cybersecurity practices. Survey participants were face-to-face and virtual attendees at a public university's Cybersecurity for Small Businesses Conference. To evaluate the attendees' perceived self- efficacy, a pre- and post-survey included cybersecurity questions with demographic questions. The results show a significant difference in scores for overall cybersecurity self-efficacy before and after such training.

Keywords: self-efficacy, cybersecurity training, entrepreneurs, entrepreneurship, small business

INTRODUCTION

Cyberattackers are aware of the unpreparedness of small business to have proper security measures in place, and the consequences are high. Based upon analysis of data collection from multiple sources, Verizon reported that 43% of small businesses are victims of cyberattacks (2019). Within 6 months of such attacks, approximately 60% of these small businesses close their businesses ("Arch Angel," 2015).

Furthermore, surviving businesses from cyberattacks often experience negative outcomes from the attacks that can include lost customers, high fees to diagnose/remedy the attack, legal fees, credit monitoring fees, fines, lost business operational time, and damaged reputation (Black, 2013; Paoli, Visschers, & Verstraete, 2018; Paulsen, 2016; Sangani & Vijayakumar, 2012). To illustrate some of the aforementioned consequences, KPMG (2015) conducted a survey of 1,000 businesses and 1,000 consumers and found that 21% of those victims' businesses needed to take their website offline, 32% paid for assistance to remedy the attack, and 20% paid for legal assistance. Recovery costs are significant to small business owners being reported as an average of $20,000 per incident, as well as a high of $38,000 - $44,000 in direct costs such as Legal IT, PR fees) and $8,000 indirect costs such as preventative measures (Berry & Berry, 2018; Raineri & Fudge, 2019).

Small businesses are easy victims of cyberattacks due to factors such as cybersecurity costs, attitudes, and insufficient education and training. Entrepreneurs often cannot afford the proper security equipment and infrastructure for their small businesses. Accordingly, common organizational equipment and activities such as firewalls, Intrusions Detection Systems, Intrusion retention Systems, multi-factor authentication, network hardening, security training, and security policies are not readily available (Bada & Nurse, 2019; "Beazley Identifies Top Misconceptions," 2011; Sangani & Vijayakumar, 2012). Additionally, small businesses may lack the appropriate dedicated technical personnel to implement security measures, monitor the network, and provide internal security audits. Because of the lack of competent security personnel, security tasks are often performed by the owner, family members, or limited workers who lack such expertise (Berry & Berry, 2018; Rai & Chukwuma, 2016).

Because of the significant damages that can be experienced by small businesses from cyberattacks, proper security awareness, security education, and self-efficacy are imperative. Even if a small business owner is aware of security risks/impact and understand mitigation strategies, the business owner must have the belief or self-confidence to initiate preventative measures (through oneself of through others) as well as remediation measures (if an attack has occurred) in order to recover from the security attack (Ng, Kankanhalli, & Xu, 2009; Reddy & Dietrich, 2017). That is, a small business owner's perceived self-efficacy determines if the pursuit of security initiatives is attainable (Bada & Nurse, 2020; Oliver 1991; McGee, Peterson, Mueller, & Sequeira, 2009). Additionally, for small business owners who have been cyber victims and are trying to recover from cyberattacks, self-efficacy determines "how long they will persist in the face of obstacles and aversive experiences" (Bandura, 1977, p. 194).

Although not researched in a cybersecurity context, training and education have enhanced individuals' self-efficacy (Florin, Karri, & Rossiter, 2007; Karl, O'Leary-Kelly, & Martocchio, 1993; Zhao, Seibert, & Hills, 2005). Building upon such previous research, this study poses the following research question: to what degree does training in cybersecurity and related topics influence small business entrepreneurs' sense of self-efficacy related to addressing cybersecurity threats to their businesses? This addresses an important need within the existing body of literature as self-efficacy metrics may serve as a useful metric to understand the ability of training programs to elicit improved confidence and persistence for attendees' behaviors and attitudes.

LITERATURE REVIEW

Types of Cyberattacks a Small Business May Experience

Small businesses can be victims of numerous types of cyberattacks. For example, technical attacks exist. SQL injection occurs when an attacker injects SQL code such that can be added, deleted, or changed for malicious purposes. In Denial of Service (DoS) or in a Distributed Denial of Service (DDos), an attacker floods the network server such that system resources are not accessible to legitimate users. Viruses, worms, and Trojan Horses are types of malicious software used by an attacker. With a Man-in-the-Middle attack, an attacker intercepts to be in the middle to collect or alter information (Bhandari, Sangal, & Kumar, 2016; Hughes & DeLone, 2007; Sangani & Vijayakumar, 2012).

A psychological-based attack is social engineering and can occur through phishing, baiting, vishing, smishing, and tail gating. Phishing attacks often occur through email in in which an attacker sends an email that looks legitimate but has an alternative motive such as capturing confidential information like a user's password, user ID, banking information, or SSN. Another type of phishing attack is baiting in which the attack specifically focuses on an incentive for the user to participate in sharing confidential information (i.e. the chance to win a prize, the option to receive a gift). Vishing is a phone-based attack in which a scammer who request confidential information and may impersonate another person or organization. Smishing is a Smart Phone text-based type of attack in which attackers also try to obtain confidential information. Tailgating occurs when an attacker impersonates someone in order to gain access to a restricted area of the building by following behind someone who has authorized access (i.e. employee who claims to have left an access card in the car or an imposter delivery service (floral, pizza)) (BioCatch, 2020; Bisson, 2019; Yasin, Liu, Li, Wang, & Zowghi, 2018).

Other security attacks can be physical theft of hardware by inside or external employees. Other examples include altering or destroying computer hardware. Last, dumpster diving occurs when an attacker looks though inside trash or external dumpsters for confidential information (i.e. customer lists, Personal Information Identifiers (PHI) as well as information that will assist in gaining access to the organization's network) (Aldawood & Skinner, 2019; Rathore, 2015; Yasin, et al., 2018).

Factors That Determine Users' Motivation for Cybersecurity Preparedness

Bada and Nurse (2019) have identified four key areas that determine the degree to which one will be motivated to participate in proactive measures for cybersecurity risk mitigation. First, perceived self-efficacy is a key factor as users evaluate the degree to which they believe that they will be successful in mitigating a threat if they take action and invest in cybersecurity measures. Additionally, users assess the extent of security, likelihood of the threat, mitigation costs, as well as a cost/benefit analysis. If the threat does not equate to substantial damage or if benefits do not outweigh costs, then a user may reject preventative measures. Although Ganin (et al., 2020) encourage the use of a multicriteria decision analysis (MCDA) model, users often do not have the personnel to find or create their own models and do not usually have the funds to pay for firms to conduct such risk assessments (Bada & Nurse, 2019;"Beazley Identifies Top Misconceptions," 2011;Sangani & Vijayakumar, 2012).

Cybersecurity Deficiencies

Numerous deficiencies exist regarding small business owners' attitudes and actions. For example, in a study completed by Prince and King (2012), 98% of small business owners felt that having high security measures in place was a priority for their businesses. However, when these researchers queried the owners about their actual implementation, only 43% of small business owners implemented security practices.

In another instance, Furman, Theofanos, Choong, and Stanton (2012) conducted a study to gain a better understanding of their level of cybersecurity knowledge, users' awareness, and users' skills. Even though 70% of users rated themselves "moderately knowledgeable" regarding cybersecurity and online risks, data actually indicated a lack of such knowledge.

Additionally, users diminished the significance of preparedness and training. For examples, some of the users could not understand why an attacker would choose them. In other instances, users did not know if anyone in their circle who experienced a cyberattack and rationalized that if such an attack had not occurred to them or individuals in their circle, then an attack probably would not happen. Last, users thought that various online sites they used had sufficient security that would prevent them from experiencing a cyberattack (Furman, et. al, 2012).

In addition to lacking a true rationalization of the need for proper cybersecurity measures, users also lacked appropriate security education and training. In the study from Furman, Theofanos, Choong, and Stanton (2012), the researchers determined that only 8% had received cybersecurity training. Similarly, Raineri and Fudge (2019) studied the sufficiency of undergraduate entrepreneurship major students' cybersecurity knowledge. Limited cybersecurity knowledge existed that was primarily attained through self-study (rather than a university course) and was insufficient for cybersecurity knowledge actually needed by small business owners.

Cybersecurity Awareness Training

Past studies have shown that numerous internal and external benefits exist due to cybersecurity awareness training. For example, after receiving cybersecurity awareness training, recipients displayed increased confidence (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Tschakert & Ngamsuriyaroj, 2019). Additionally, Parsons (et al., 2014) completed a study showing security awareness training had a positive influence on users' attitudes regarding security policies. Similarly, Johnston and Warkentin (2010) concluded that aware users were more likely to comply with security recommendations. As a result of cybersecurity awareness, internal and external changes occur as recipients of cybersecurity training had an increased positive attitude and were more inclined to participate in proactive security measures for password creation and protection (Clarke & Furnell 2012; Rhee, Kim, & Ryun, 2009). Last,

recipients of such training were less likely to be a victim of phishing attack (Dodge, Carter, & Ferguson, 2007; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010).

The Impact of Training on Self-Efficacy

Byrge and Tang (2015) completed a study on the impact of reflective and embodied training on creativity and self-efficacy. In addition to increasing creative expression, creative self-efficacy was also increased. Within healthcare, Ammentorp, Sabroe, Kofoed, and Mainz (2007) recognized the need for quality communications skills between healthcare providers and patients. After training was provided to clinicians, self-efficacy had increased by 37%. Within the technology industry, Delcourt and Kinzie (1993) completed a study showing that training increases internet self-efficacy.

Given the aforementioned benefits of training on self-efficacy and on cybersecurity confidence, attitudes, and practices, the present study sought to explore the effects of cybersecurity training on participant self-efficacy towards small business cybersecurity practices.

METHOD

Penn State University Hazleton campus hosted a full-day Fall Cybersecurity Entrepreneurship Conference in November 2019, during which both in-person and virtual attendees were trained on topics related to general cybersecurity, PCI DSS, social engineering in small businesses, and legal considerations. These topics were chosen to expand attendees' ability to apply cybersecurity concepts to entrepreneurship, articulate reasons for and the impacts of cyberattacks on small businesses, and identify resources to assist small businesses with preventive measures. This program was free and open to the community and was sponsored in part by the Center for Security Research and Education (CSRE) at Penn State University, which promotes research and education to protect people, infrastructure and institutions from the broad range of hazards confronting society today. More information is available at csre.psu.edu. Additional sponsors of the event include Invent Penn State through the Penn State Hazleton LaunchBox and Penn State Hazleton Information Sciences and Technology. To address the need for continued research on the effectiveness of training to address cybersecurity self-efficacy, this exploratory empirical study used a quantitative pre-/post-survey design to collect information from attendees.

Participants completed the survey either in-person or online and were also given the opportunity to enter a raffle for one of five $20 gift cards that was randomly selected after data collection concluded.

Sample

Of the 49 event attendees, 30 participated in-person, 12 joined as a group via videoconference from the Penn State Hazleton LaunchBox, and 7 joined individually via videoconference. Though 25 people completed the pre-survey, 20 (N=20) of the 49 participants completed both the pre-survey and post-survey, resulting in a 40.8% response rate. 19 survey respondents were in person, and 1 participant watched the event via live video stream and completed the surveys online. Of the 20 participants, 13 (65%) were male and 7 (35%) were female. Please see Table 1 for participant demographic information.

TABLE 1
DEMOGRAPHIC CHARACTERISTICS OF PARTICIPANTS

	Frequency	Percent
Participants (*N*)	20	100%
Sex		
Male	13	65%
Female	7	35%
Age		
18-24	4	20%
25-34	3	15%
45-54	8	40%
55-64	5	25%
Ethnicity		
American Indian or Alaska Native	1	5%
Asian	2	10%
Caucasian	15	75%
Other	2	10%
Professional Role		
Undergraduate Student	4	20%
Graduate Student	2[a]	10%
Faculty Member	3	15%
Small Business Employee	6[a]	30%
Small Business Owner/Entrepreneur	2	10%
Other	4	20%

Note. [a] One participant indicated that they were both a graduate student and a small business employee.

Instrument

Because the training was designed to provide a broad overview of cybersecurity practices, the survey instrument was designed with a similar breadth and gradation of difficulty (Bandura, 2006) for each of the four conference sessions. The survey instrument consisted of 14 questions that spanned topics within General Cybersecurity, PCI DSS, Social Engineering, and Legal Aspects, as well as five questions related to participant demographic information. Items were context specific based on the training learning objectives and were developed in consultation with a group of content area experts. Along with evaluating participants' perceived self-efficacy, this design facilitates improved content alignment, highlights areas for future training improvements, and allows for use of the instrument as a pedagogical tool to show participants' growth over time (Nuhfer & Knipp, 2003).

Unless otherwise noted, all items used a 6-point Likert scale ranging from 1 = *strongly disagree* to 6 = *strongly agree*. The survey was administered immediately before and after the conference to determine if there were any changes in self-efficacy due to training. Participants generated a unique five-digit identification code to ensure confidentiality and reduce social evaluative concerns (Bandura, 2006). Given that all survey items were scored as continuous variables, Cronbach's alpha is an appropriate metric to estimate the internal consistency of scores on the instrument (Creswell & Guetterman, 2019). Cronbach's alpha for the pre-survey was .92 and for the post-survey was .94. These scores illustrate a high level of internal consistency and are above the .80 recommended reliability threshold for making decisions about individuals (Thorndike & Thorndike-Christ, 2010). Table 2 outlines the number of items and reliability scores for each construct.

TABLE 2
RELIABILITY OF SCALES

	Number of Items	Pre-survey Cronbach's α	Post-survey Cronbach's α
Overall Survey	14	.92	.94
General Cybersecurity	5	.89	.86
PCI DSS	3	.81	.88
Small Business Social Engineering	3	.78	.71
Legal Aspects	3	.78	.86

RESULTS AND DISCUSSION

A paired samples t-test was conducted to compare participants' perceived cybersecurity self-efficacy before and after receiving training (see Table 3). There was a significant difference in scores for overall cybersecurity self-efficacy before training ($M = 3.55$, $SD = 1.13$) and after training ($M = 5.34$, $SD = 0.57$), $t(19) = 10.89$, $p < .001$, $d = 2.44$. This improvement suggests that the training was effective in improving participants' sense of self-efficacy in their ability to address issues related to cybersecurity for small businesses. These findings are consistent with those from Raineri and Fudge (2019), who suggest that this type of cybersecurity information may be lacking from formal entrepreneurship education programs, and the training in cybersecurity can positively impact the cybersecurity health of small businesses.

TABLE 3
MEANS, STANDARD DEVIATIONS, AND RESULTS OF PAIRED SAMPLES T-TEST

	Pre-Survey		Post-Survey				
I feel confident in my ability to	Mean	SD	Mean	SD	t	df	Cohen's d
Q1. Define cybersecurity	4.40	1.14	5.45	0.55	4.97*	19	1.11
Q2. Identify at least 3 types of cybersecurity attacks	3.95	1.54	5.65	0.49	5.23*	19	1.17
Q3. Identify at least 3 cybersecurity safeguards/security hygiene measures	4.05	1.50	5.40	0.75	4.61*	19	1.03
Q4. Identify categories of employees that pose internal threats	3.50	1.64	5.32	0.75	4.86*	18	1.12
Q5. Explain one or more established security frameworks	3.35	1.76	5.15	0.81	6.09*	19	1.36
Average for General Information on Cybersecurity	3.85	1.28	5.39	0.55	6.94*	19	1.55
Q6. Explain why small businesses are especially vulnerable to cyberattacks	3.90	1.45	5.75	0.44	6.75*	19	1.51
Q7. Explain the impact to small businesses if they are victims of cyberattacks	4.16	1.34	5.70	0.57	5.87*	18	1.35
Q8. Define social engineering	3.68	1.49	5.55	0.61	6.42*	18	1.47
Average for Social Engineering in Small Business	3.88	1.22	5.67	0.43	8.05*	19	1.80
Q9. Define Payment Card Industry Data Security Standard (PCI DSS)	3.10	1.65	5.25	0.72	6.58*	19	1.47
Q10. Explain who needs to be PCI compliant	3.15	1.81	5.45	0.76	7.07*	19	1.58

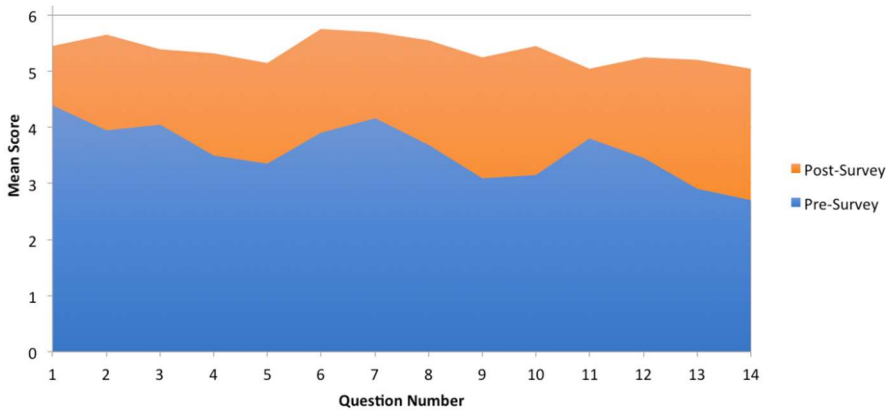
I feel confident in my ability to	Pre-Survey Mean	Pre-Survey SD	Post-Survey Mean	Post-Survey SD	t	df	Cohen's d
Q11. Explain at least 2 types of financial cyberattacks	3.80	1.51	5.05	0.89	5.00*	19	1.12
Average for PCI DSS	3.35	1.42	5.25	0.71	8.52*	19	1.90
Q12. Explain the legal considerations of data security and privacy	3.45	1.64	5.25	0.72	6.28*	19	1.41
Q13. Explain the Children's Online Privacy Protection Act (COPPA)	2.90	1.52	5.21	0.71	7.01*	18	1.61
Q14. Identify the limitations of insurance coverage for breaches	2.70	1.49	5.05	0.83	7.79*	19	1.74
Average for Legal Considerations	3.02	1.30	5.15	0.69	9.49*	19	2.12

* $p < .001$

Participants expressed the largest increases in self-efficacy as they related to legal considerations (ΔM = 2.13, ΔSE = 0.23) and PCI DSS (ΔM = 1.90, ΔSE = 0.22). This may be related to the specialized knowledge and policy-related information covered by these topics. The increased self-efficacy in legal considerations is beneficial as some small business owners who collect data on their website may recognize the importance of complying with COPPA when collecting personal information of individuals under age 13, such as including website operator contact information, listing a COPPA-compliant privacy policy, notifying parents, verifying parental consent, and more. Additionally, as a result of the increased self-efficacy, small business owners may be motivated to pursue proper security and privacy safeguards due to their understanding of the legal consequences of breaches, as well as the limitations with insurance. The increased self-efficacy in PCI DSS is meritorious as some small business owners with e-commerce websites can identify what is needed for compliance and determine security measures for processing, securing, and transmitting credit card data such as firewalls, encryption, need-to-know roles, secure storage, and more.

Though smaller gains, the areas of general cybersecurity (ΔM = 1.54, ΔSE = 0.22) and small business social engineering (ΔM = 1.79, ΔSE = 0.22) also saw significant growth. These were more foundational topics, so it is likely that more participants had some degree of perceived prior knowledge in these areas. These topics were presented early in the day so that the information could be built upon throughout the session. Figure 1 illustrates the changes in self-efficacy by question. The increased self-efficacy in general cybersecurity is important such that small business owners can fill in the gaps of their existing knowledge related to external threats and inside employee threats along with any missing safeguards such as security policies, employee training, network controls, vulnerability assessments, and more. The increased self-efficacy in social engineering is advantageous because small business owners may realize some of the human deceptive techniques like phishing, tailgating and baiting along with the value of security measures such as training and external employee safeguards.

FIGURE 1
SELF-EFFICACY PRE-SURVEY AND POST-SURVEY SCORES BY QUESTION



CONCLUSION

Training in cybersecurity and related topics yielded improved self-efficacy for understanding and addressing basic elements important to instating proper security measures for small businesses. Though small business entrepreneurs and employees are tasked with ensuring that their organizations utilize such measures, resource and education-related barriers often influence the ability to meet these needs. The illustrated improvements in self-efficacy in cybersecurity in general, and specifically within PCI DSS, social engineering, and legal aspects, make targeted training a potentially valuable intervention for affecting behavior, attitudes, goals, and effort (Bandura, 2006).

One limitation of this study is the small sample size, which limits the ability for more in-depth analysis. During data collection, researchers utilized several recommendations for increasing the response rate, including collecting data face-to-face (Hox & De Leeuw, 1994), offering multiple modes to complete the surveys (De Leeuw, 2005), and offering the ability to enter a contest (Bosnjak & Tuten, 2003; Tuten, Galesic, & Bosnjak, 2004). Participants could complete the pre-and post- survey online or in-person, and were given the opportunity to enter a contest to win one of five $20 gift cards. However, the response rate was lower than anticipated. For future events of this nature, researchers may seek increased funding (Dudovskiy, 2019) and improve the immediacy of incentives (Read, Loewenstein, & Kalyanaraman, 1999) to assist with increasing the response rate.

Information Technology changes rapidly, as do laws and regulations pertaining to cybersecurity and privacy (Benamati & Lederer, 2001; Weber & Studer, 2016). For example, some of the evolving legal regulations include the Health Insurance Portability and Accountability Act (1996), Children's Online Privacy Protection Act (1998), Gramm-Leach Bliley Act (1999), and state regulation for data breach notifications (2002-2104) (Gadbow, 228; Shackelford, Proia, Martell, 2015). The increase in emerging technology is also accompanied by an increase of current and new types of cyber threats (Jang-Jaccard, & Nepal, 2014). Consequently, the content for this instrument and training topics are context specific and would need to be updated for future use, rather than generalized. Future research should also focus on exploring the effects of training on self-efficacy for larger, more diverse groups of participants (Allmark, 2004), such as larger, cross-institutional student groups, Small Business Development Centers, and large professional organizations. Alongside a larger, more diverse population, future studies in this area should consider evaluating participants' cybersecurity knowledge (Raineri & Fudge, 2019) and exploring sustained effects of training on future attitudes and behaviors. A final future study could explore if users would be more likely to proactively implement cybersecurity security safeguards if they were aware of the legal consequences of security breaches.

REFERENCES

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. *Future Internet*, *11*(3), 73. doi:10.3390/fi11030073

Allmark, P. (2004). Should research samples reflect the diversity of the population? *Journal of Medical Ethics*, *30*(2), 185–189. https://doi.org/10.1136/jme.2003.004374

Ammentorp, J., Sabroe, S., Kofoed, P., & Mainz, J. (2007). The effect of training in communication skills on medical doctors' and nurses' self-efficacy. A randomized controlled trial. *Patient Education and Counseling*, *66*(3), 270.

Arch Angel Network Security Inc. (2015). Retrieved from http://www.archangelnetsecurity.com

Bada, M., & Nurse, J.R.C. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 1-20. doi:10.1108/ICS-07-2018-0080

Bada, M., & Nurse, J.R.C. (2020). The social and psychological impact of cyber-attacks. In V. Benson & J. Mcalany (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 73-92). Retrieved from https://ebookcentral.proquest.com/lib/pensu/reader.action?docID=5902750

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191-215. doi:http://dx.doi.org.ezaccess.libraries.psu.edu/10.1037/0033-295X.84.2.191

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes*, *50*(2), 248-287.

Bandura, A. (2006). Guide for constructing self-efficacy scales. *Self-Efficacy Beliefs of Adolescents*, *5*(1), 307-337.

Beazley identifies top misconceptions that leave small businesses vulnerable to data breaches. (2011). Retrieved from https://www.beazley.com/documents/2011/019%20Data%20Breach%20Small%20Business%20Misconceptions.pdf

Benamati, J., & Lederer, A.L. (2001, January). How IT organizations handle rapid IT change: Five coping mechanisms. *Information Technology and Management*, *2*(1), 95–112. https://doi.org/10.1023/A:1009986821907

Berry, C.T., & Berry, R.L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1-10. doi:10.1504/IJBCRM.2018.090580

Bhandari, A., Sangal, A.L., & Kumar, K. (2016). Characterizing flash events and distributed denial-of-service attacks: An empirical investigation. *Security and Communication Networks*, *9*(13), 2222-2239. doi:10.1002/sec.1472

BioCatch. (2020). *Types of social engineering attacks: Detecting the latest scams*. Retrieved from https://www.biocatch.com/blog/types-social-engineering-attacks

Bisson, D. (2019, November 5). *5 Social engineering attacks to watch out for*. Tripwire. Retrieved from https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Black, J. (2013). Developments in data security breach liability. *The Business Lawyer*, *69*(1), 199-207.

Bosnjak, M., & Tuten, T.L. (2003). Prepaid and promised incentives in web surveys: An experiment. *Social Science Computer Review*, *21*(2), 208–217. https://doi.org/10.1177/0894439303021002006

Byrge, C., & Tang, C. (2015). Embodied creativity training: Effects on creative self-efficacy and creative production. *Thinking Skills and Creativity*, *16*, 51-61. doi:10.1016/j.tsc.2015.01.002

Clarke, N., & Furnell, S. (2012). Creating a security culture development plan and a case study. In O. Olivos (Ed.), *Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance HAISA 2012* (pp. 13-32). HAISA. Retrieved from http://www.cscan.org/default.asp?page=openaccess&eid=13&id=28

Creswell, J.W., & Guetterman, T.C. (2019*). Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Pearson. New York, US.
De Leeuw, E.D. (2005). To mix or not to mix data collection modes in surveys. *Journal of Official Statistics*, *21*(2), 233. Retrieved from http://ezaccess.libraries.psu.edu/login?url=https://search-proquest-com.ezaccess.libraries.psu.edu/docview/1266791766?accountid=13158
Delcourt, M.A.B., & Kinzie, M.B. (1993). Computer technologies in teacher education: The measurement of attitudes and self-efficacy. *Journal of Research and Development in Education*, *27*(1), 35-41
Dodge, R. C., Carter, C., & Ferguson, A.J. (2007). Phishing for user security awareness. *Computers & Security*, *26*, 73–80. doi: 10.1016/j.cose.2006.10.009
Dudovskiy, J. (2019). *Research limitations*. Retrieved from https://research-methodology.net/research-methods/research-limitations/
Emm, D. (2013). Security for SMBs: Why it's not just big businesses that should be concerned. *Computer Fraud & Security*, (4), 5-8. doi:10.1016/S1361-3723(13)70036-8
Florin, J., Karri, R., & Rossiter, N. (2007). Fostering entrepreneurial drive in business education: An attitudinal approach. *Journal of Management Education*, *31*(1), 17-42. Retrieved from http://ezaccess.libraries.psu.edu/login?url=https://search-proquest-com.ezaccess.libraries.psu.edu/docview/195717403?accountid=13158
Furman, S., Theofanos, M.F., Choong, Y., & Sranton, B. (2012, March-April). Basing cybersecurity training on user perceptions. *IEEE Security and Privacy*, *10*(2), 40-49. DOI: 10.1109/MSP.2011.180
Gadbaw, T. (2016). Legislative update: Children's Online Privacy Protection Act of 1998. *Children's Legal Rights Journal*, *36*(3), 228.
Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*(1), 183-199. doi:10.1111/risa.12891
Hox, J.J., & De Leeuw, E.D. (1994). A comparison of nonresponse in mail, telephone, and face-to-face surveys. *Quality and Quantity*, *28*, 329–344. https://doi.org/10.1007/BF01097014
Hughes, L.A., & DeLone, G.J. (2007). Viruses, worms, and trojan horses: Serious crimes, nuisance, or both? *Social Science Computer Review*, *25*(1), 78–98. https://doi.org/10.1177/0894439306292346
Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993
Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *Management Information Systems*, *34*(3), 549-566.
Karl, K., O'Leary-Kelly, A., & Martocchio, J. (1993). The impact of feedback and self-efficacy on performance in training. *Journal of Organizational Behavior*, *14*(4), 379-394. Retrieved from www.jstor.org/stable/2488290
KPMG. (2015). *Small business reputation and the cyber risk.* Retrieved from https://home.kpmg/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf
McGee, J.E., Peterson, M., Mueller, S.L., & Sequeira, J.M. (2009). *Entrepreneurial self–efficacy: Refining the Measure*.
Ng, B.Y., Kankanhalli, A., & Xu, Y.C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.
Nuhfer, E., & Knipp, D. (2003). The knowledge survey: A tool for all reasons. *To Improve the Academy*, *21*(1), 59-78.
Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change*, *70*(4), 397-420. doi:10.1007/s10611-018-9774-y
Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014, May). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, 165-176. doi:10.1016/j.cose.2013.12.003
Paulsen, C. (2016). Cybersecuring small businesses. *IEE*, *49*(8), 92-97.

Prince, D., & King, N. (2012). *Small business cyber security survey 2012*. Security Lancaster. Retrieved from https://eprints.lancs.ac.uk/id/eprint/60274/1/sbcss2012_report.pdf

Raineri, E., & Fudge, T. (2019). Exploring the sufficiency of undergraduate students' cybersecurity knowledge within top universities' entrepreneurship programs. *Journal of Higher Education Theory and Practice*, *19*(4), 73-92. https://doi.org/10.33423/jhetp.v19i4.2203

Rathore, N. (2015). Ethical hacking and security against cyber crime. *I-Manager's Journal on Information Technology*, *5*(1), 7.

Read, D., Loewenstein, G., & Kalyanaraman, S. (1999). Mixing virtue and vice: Combining the immediacy effect and the diversification heuristic. *Journal of Behavioral Decision Making*, *12*(4), 257-273.

Reddy, D., & Dietrich, G. (2017, October). Cybersecurity training and the end-user: Pathways to compliance. *Journal of The Colloquium for Information System Security Education*, *5*(1), 1-24. Retrieved from https://cisse.info/journal/index.php/cisse/article/view/71

Rhee, H., Kim, C., & Ryu, Y.U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826.

Sangani, N.K., & Vijayakumar, B. (2012). Cyber security scenarios and control for small and medium enterprises. *Informatica Economica*, *16*(2), 58-71.

Shackelford, S.J., Proia, A.A., Martell, B., & Craig, A.N. (2015). Toward a global cybersecurity standard of care?: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Texas International Law Journal*, *50*(2), 305-355.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. Paper presented at the *SIGCHI Conference on Human Factors in Computing Systems*. https://dl.acm.org/doi/10.1145/1753326.1753383

Thorndike, R.M., & Thorndike-Christ, T.M. (2010). *Measurement and evaluation in psychology and education*. Pearson. Upper Saddle River, New Jersey.

Tschakert, K.F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, *5*(6), e02010. https://doi.org/10.1016/j.heliyon.2019.e02010

Tuten, T.L., Galesic, M., & Bosnjak, M. (2004). Effects of immediate versus delayed notification of prize draw results on response Behavior in web surveys: An experiment. *Social Science Computer Review*, *22*(3), 377–384. https://doi.org/10.1177/0894439304265640

Verizon. (2019). *2019 Data breach investigations report*. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Weber, R.H., & Studer, E. (2016, October). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law Review*, *35(5*), 715-728.

Yasin, A., Liu, L., Li, T., Wang, J., & Zowghi, D. (2018). Design and preliminary evaluation of a cyber security requirements education game (SREG). *Information and Software Technology*, *95*, 179-200. doi:10.1016/j.infsof.2017.12.002

Zhao, H., Seibert, S.E., & Hills, G.E. (2005). The mediating role of self-efficacy in the development of entrepreneurial intentions. *Journal of Applied Psychology*, *90*(6), 1265-1272. doi:http://dx.doi.org.ezaccess.libraries.psu.edu/10.1037/0021-9010.90.6.1265