Human Factor on Computer Cyber Innovation

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Mai Luu

May 8, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____

Approved: _____ Date_____

Rider Foley, Department of Engineering and Society

Background

For the past several years, the total malware infections have been on the rise from 12.4 million in 2009 to 308.96 million malware attacks in 2018 (Firch, 2021). Malware is a piece of software that was written to wreck the security of computer to get access to sensitive information. Over the year 2018, malware has increased by 165%. The number of new malware variants have increased significantly along with the development of mobile application (Firch, 2021). Phishing emails and ransomware are one the leading causes of cybercrime along with malware attacks. Phishing emails are designed to trick recipients to click on a malicious link. On the other hands, ransomware is designed to block access to the device until an amount of money is paid (Kraemer and Carayon, 2014). The combination of malware, ransomware and phishing emails are a severe threat to any enterprise. Malicious software will enter the system and try to run background and collect personal data. A noteworthy point is that data theft is a concern because most users do numerous business transaction by mobile application and online website. Although more resources are being developed to prevent cyberattack including a change in software platform, cybersecurity industry still has to face the risk of cyber threats (Fruhlinger, 2019). There are several causes for cyber-attacks but human factors are major contributing factors for cybercrime. The most common types of human error in cybersecurity are decision errors, skill-based errors, and perceptual errors (Daughery, 2016). Human error in cybersecurity represents an action when the human error results in vulnerabilities and security breaches. Decision errors occur when the behaviors or decision of the individuals are inadequate to achieve the desired results (Pollock, 2017). Skill-based errors which occur when the negative habit results in unsafe situation. And perceptual errors are caused by when a decision is made by a faulty information (Pollock, 2017). According to the data security incident report, human error

accounted for 37%, which is the leading cause among the process. The data incident report showed human error by phishing or malware was 25% in 2015, external theft of a device (22 %) and employee theft (16 %). Most contemporary studies focus on individual's privacy concerns and social media privacy issues but pay little attention to major threats to cybersecurity that arise from humans. In other words, no matter how the systems are secure, humans are the major factor that causes data breach. Human error can be either deliberate or unintentional. An intentional error has or involves motivation behind it and becomes an insider threat while an unintentional one is either reckless or negligent but involves no pre-planning (Daughery, 2016).

Many researchers have studied the major threats to cybersecurity that arise from humans with the research of Human Factors Analysis and Classification System (HFACS) framework. HFACS is a methodology to evaluate whether there are any latent organizations that led to the errors (Pollock, 2017). The HFACS is a broad framework but its goal is not to attribute blame. The HFACS framework is designed to understand the underlying causes of the incidents (Pollock, 2017). In fact, human error is a complicated security problem that may never be eliminated from the tasks. However, many performance problems can be prevented if we understand the cause and the threat thoroughly. In cyber security, understanding the cause of the incident can mitigate the risk of cyberattack as hackers are simply looking for a weak link that exists by human mistake. The purpose of this paper is to research the major threat to computer and information security that arise from humans.

Negligent and Reckless in The Technology

Responsibility has become an extensive theme and the first key role in the technology area. Responsible innovation builds on the understanding that science and technology are not only technically but socially where humans take an important role in using technology to shape

the desirable future. Jack Stilgoe, Richard Owen and Phil Macnaghten found what the responsibility of science means to take care of the future of the community through the innovation and development in science and technology in the present (Stilgoe et al., 2013). The role of human factors in computer security attacks is divided into two groups: unintentional and intentional. In other words, it can be either negligent or reckless. Negligence or recklessness is a major threat to the technology that causes data breaches. Furthermore, insider threats are more complicated to prevent and resolve than outsider threats because the latter requires more worldwide effort such as from criminal groups (Daughery, 2016). To measure the human factor of cyber security, researchers aim to question the risks or causes they can anticipate and then conduct the experiments to prove the sustainability of humans to cyber-attack. However, the study showed that the causes of data breaches are from employee's routine engagement. It includes using universal serial bus (USB) that are not converted into a code, using a weak wireless network, or clicking on business email compromise (BEC) scams to trigger the curiosity of employees, and others (Ponemon Institute LLC, 2012). Even though the risks are anticipated and minimized as much as possible by the companies' policy and by engineers themselves, human factors in cyber threats are somehow not eliminated entirely.

In contrast to the negligence of human factors, recklessness means being careless of the possible consequences. Recklessness in cyber security is quite similar to the negligence concept except from the fact that the users already know the potential outcomes but explicitly choose to ignore them due to their personal needs. The causes of data breaches due to recklessness are not only from employment's routine engagement but also on a larger scale. Josephine Wolff indicated that the cyber security strategy in 2018 of the national cyber strategy was considered reckless (Wolff, 2018). Instead of continuing to strengthen the defensive technology, the new

strategy plan at that time proposed to ramp up offensive cyber activities. The new strategy belittled the goal of increasing the defenses but focused on showing off the power. There are no doubts that this strategy expanded the number of ransomwares, spyware and trojans. Spyware is defined as malicious software which enters your computer to gather data and sell it illegal to the third-party company. And trojan malware is a different type of malicious ware but it is disguised as legitimate software (Kraemer and Carayon, 2014). The idea of ramping up offensive cyber operations was not a new idea, but for the U.S government was a sharp change since the prior American Government valued the defense-oriented system more than attacking strategy. (Wolff, 2018). Computer Security Innovation was developed to protect data and security of consumers and businesses. However, attackers make use of human factor's vulnerability to gain access to computer networks. The responsibility of protecting data is not only the responsibility of engineers and inventors, but also of the consumers, businesses or any individuals since human errors can be made by any of us. However as mentioned above, insider threats are more complicated to prevent and resolve than outsider threats (Daughery, 2016). Therefore, the second aspect of the study is to do further research towards an issue, which is followed by planning and actions necessary towards negligence behaviors to achieve the desired changes. Bowen Brian, Ramaswamy Devarajan, and Salvatore Stolfo at Columbia University studied that "users can be trained using decoy technology to be cognizant of potential threats" (Brian et al., 2014). However, the conclusion is not enough to determine whether training is efficient on a large scale instead of a small scale. Many people have the belief that cyber-attack is the sole responsibility of Information Technology (IT) department. Even though other human factors played a significant role on cyber vulnerability, most damage is the result of negligence. Human negligence, whether by ignorance or carelessness, is responsible for cyber damage.

According to Tommy Pollock, system design and human factors both play a key role in how human error occurs, especially when there is a slight disconnect between system design and the person who manages the system (Pollock, 2017). Brian and colleagues (2014) at Columbia University conducted an experiment with 4,000 selected participants including students, staff, and faculty to show how vulnerable behaviors can lead to malicious activities accomplished by human interaction. The experiments began with 500 emails sent to obtain user's credentials. The attachment, forms and embedded URL are designed to trick people with the subject containing words like "urgent". Only users that engaged with the phishing emails were selected to the second round in which they were sent several phishing emails several weeks later. It took four rounds until users could identify which emails were dangerous. The experiment was then conducted a second time with 2,000 participants to test its reliability (Brian, et al., 2014). The experiment studied how negligent users respond to phishing emails and if the results improve until the fourth round of the experiment. There were four categories of decoy emails which included emails with internal URLs (hyperlink that directs the reader to your own specific website), email with external URLs (hyperlink that directs the reader from one's website to another website to provide addition information), forms to obtain credentials and beacon documents (is a technique that is embedded in the document allow checking that a user has accessed the document). Brian and colleagues (2014) found that users are users are less likely to respond to emails that had internal URLs than emails that had external URLs. However, there is not enough evidence to conclude that external URLs are more suspicious than internal ones. This is because internal URLs resemble emails from Columbia University which were not attractive enough. The results showed that the number of times that users entered their credentials information into the bogus forms were higher than expected. However, the times that students

responded to phishing emails gradually decreased in the fourth round of the experiment. This means that results generally improved compared to the first-round experiment (Brian et al., 2014). This study showed that the potential of human behaviors and knowledge affect the result of the experiment. Those who answered phishing emails in earlier rounds of experiments were less likely to do so in later rounds.

Human factors analysis and classification systems

In addition to conducting experiments, several researchers also studied the application of human factors analysis and classification systems to evaluate if it is helpful for the development of cybersecurity due to human error. The HFACS tool was considered a bridge that connects the gap between theory and practice. The HFACS is divided into four levels: unsafe acts, preconditions for unsafe acts, unsafe supervision, and organizational influences. HFACS is an analytic tool that was originally created from the U.S Navy (Pollock, 2017). However, the scientists aim to develop the framework to evaluate human factors in general. For example, if the failure was due to human factors falls into the preconditions level of HFACS, it means the failure might have been influenced by another factor such as personal factor or environmental factors and were not fully prepared for the complex or unexpected situation.

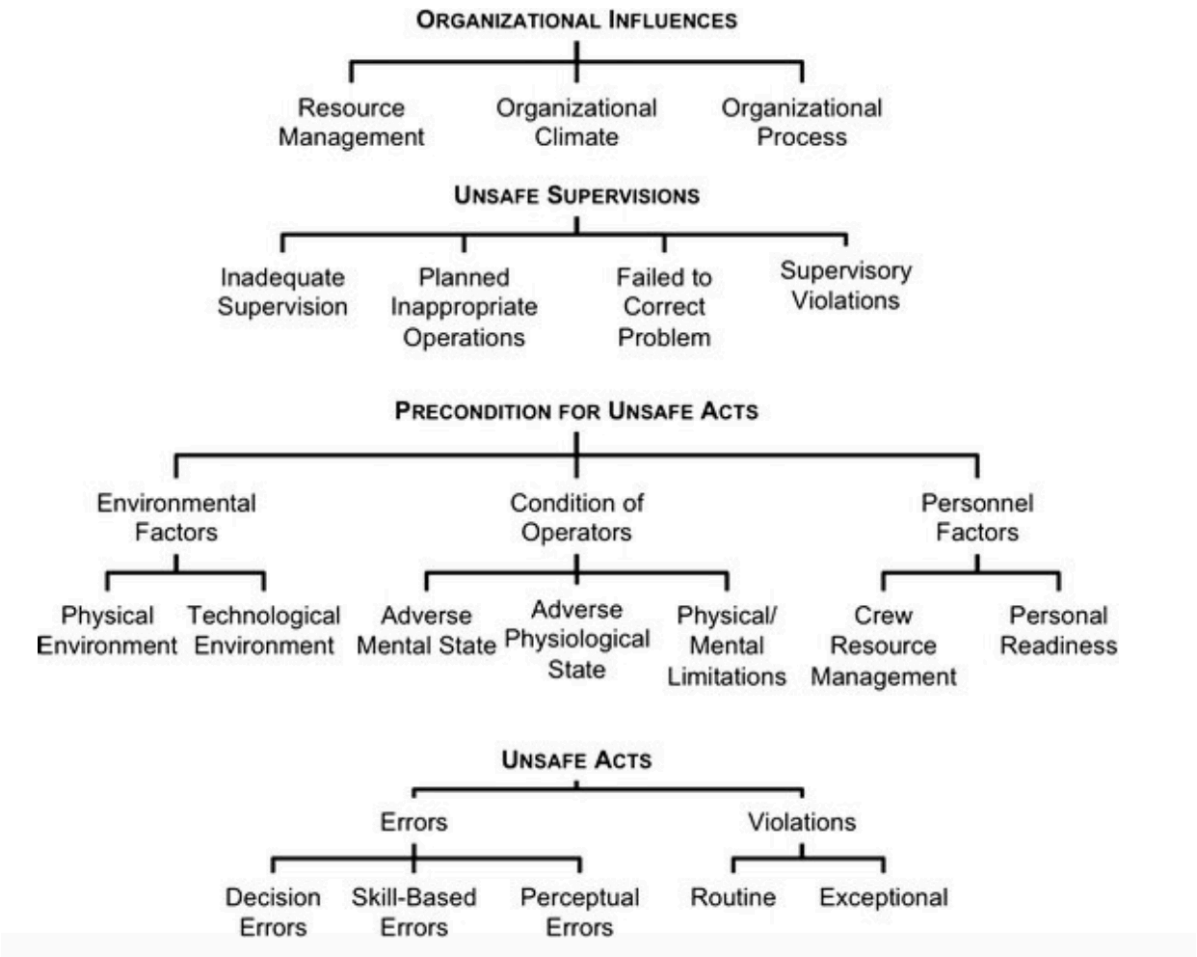

Figure 1: HFACS framework (Pollock, 2017)

Research Question and Methods

The research question studies the impact of human error on the entire cybersecurity industry. More specifically, how does cybersecurity breach caused by human error affect the cybersecurity industry? This paper will collect data from case studies and prior literature on cybersecurity due to human factors to answer the research question. The historical data breaches are collected by CNBC, CPO Magazine, Time Magazine, Wall Street Journal and also by widely-used application companies, such as Twitter or Internet-based social media platforms in general. The data of human impacts on cybersecurity industry will be divided into two categories: The damage cost of 10 selected incidents and HFACS application on each scenario.

The approach of gathering evidence to answer the research question will be a combination of established resources and publications. Cybersecurity data statistics will be collected by several different sources and then categorized into each column of the Excel sheet. Each column will show the average cost of cyberattack by different industries, such as in healthcare, finance, and enterprise. Besides collecting data on cost and spending of cyberattack, the paper will also research on the application of human factors analysis and classification systems to evaluate which HFACS category has the highest frequency. In each of the datasets collected, there would be a brief explanation of how cybersecurity is vulnerable. The failure of each case will be categorized to evaluate which failure falls into which level of the HFACS framework. The purpose of the HFACS framework is to identify the contributing factors and the development of safety design to decrease the potential risks by humans. The HFACS provides a better understanding of whether the failure is due to frontline employees (or users) or prompted by the operators. The rankings were decided on through the research of literature. After the data is collected and organized on the worksheet, data analysis and interpretation will be provided to indicate the responsibility of human factors in cyber vulnerabilities and if negligence and recklessness play important roles in human factors. This method serves as a way to group the conditions and scenarios together, making it easier to see what prior literature has the same human factors.

After randomly selecting the top 10 popular company or institution that suffered from cyber-attack, result shows that human factors caused significant cyber damage on industry. Business email scams are the most effective and common type of cybercrime, accounting for $334 million in losses. Phishing email methodology takes 4 of the 10 case studies, and is the leading cause of cyber-attacks. The second common type of cybercrime is Malware, which is

accounting for $700 million in losses. However, according to the datasets, denial of service attacks was responsible for $2.28 billion including compensation fees for the victims, compliance requirements fees, and legal fees, which is the highest damage cost among the selected sample. The data collected varies by industry to ensure the accuracy of the analysis. From the abovementioned research, it can be concluded that all types of cyber-attack result in loss to the U.S economy, as major as billions of dollars in damages. Most companies declare their initial damage immediately after the attack. However, after a year or longer, the damage cost tripled from their starting cost due to the impact of stock prices, equipment loss and, business disruption. In addition to the establishment of the damage cost, the datasets show that most cybersecurity breaches are caused by human error. Specifically, frontline employees seem to take more responsibility for the attacks than organizational influences. Human errors are primarily due to their skill-based error, perceptual error, and precondition unsafe acts. The description of the results will be discussed in the paragraph below.

BY INDUSTRY	ORGANIZATION/ COMPANY'S NAME	INITIAL DAMAGE ($)	TOTAL DAMAGE ($)	MANUFACTURING METHODS
HEALTHCARE	National Health Service	25 million	100 million	Phishing email
EDUCATION	UCSF's medical school		1.14 million	Denial of Service

FINANCE	Financial Institutions	100 million	350 million	Malware
FINANCE	Equifax	700 million	1.14 billion	Denial of Service
SOCIAL NETWORK		117 million	134 million	Phishing email
SOCIAL NETWORK	Twitter	NA	121,000	Phishing message
SOCIAL NETWORK	LinkedIn		4 million	Password Attack
TECHNOLOGY	Google	NA	~100 million	Phishing email
TECHNOLOGY	Uber	NA	148 million	Malware
ENTERPRISE	Target	18.5 million	202 million	Malware

Table 1: Damage Cost by Cyber-Attack

Unsafe acts and preconditional acts play a major role in data breaches. The assignment of the weight is supplemented by literature research. For example, if the recipient falls for the phishing scam, it means they are inexperienced in dealing with emergent condition, or be manipulated by the emotions and unconscious biases. A dashed line indicates HFACS level has no effect on the researched literature. An empty circle indicates low effect, a half filled indicates

a medium effect and a filled in circle indicates a strong effect of the human factors on the scenarios.

By Industry	Manufacturing methods	Description of methods.	Unsafe Acts		
			Skill-Based Error	Decision Error	Perceptual Errors
Healthcare	Phising email	The goal to trick recipient into believing that this is an urgent email.	○	—	●
Education	Denial of Service	Leaving some data and servers inaccessible	●	○	—
Finance	Malware	Because most of financial instituition use legacy digital systems-defenseless against sophisticated attack	○	○	—
Finance	Denial of Service	Application vulnerability lead to data breach	●	○	—
Social Network	Phishing email	These phising messages usually come from friends that have been hacked and send out the scammed email to their friends.	○	—	●
Social Network	Phishing message	Use the account of the most people in the country to ask followers send bitcoin to the anonymous address	—	—	●
Social Network	Password Attack	" Million accounts password were leaked.LinkeIn required users and affected cardholfer to change their passwords	○	—	●
Technology	Phishing email	Fraudulent Phishing emails were sent to employees, tricking them to wire money to an anonymous account	○	—	●
Technology	Malware	Two individuals outside the company had inappropriately accessed user data stored	○	○	—
Enterprise	Malware	Installed malware to capture other customer's data.	○	○	—

Figure 2: Scenario Analysis-Human Factor Assessment

By Industry	Description of methods.	Preconditional for Unsafe Acts			Unsafe Supervision	Organizational Influences
		Environmental Factor	Conditional of Operators	Personnel Factors		
Healthcare	The goal to trick recipient into believing that this is an urgent email.	–	◐	◐	–	–
Education	Leaving some data and servers inaccessible	–	–	–	●	–
Finance	Because most of financial instituition use legacy digital systems-defenseless against sophisticated attack	–	–	–	◐	●
Finance	Application vulnerability lead to data breach	–	–	–	◐	–
Social Network	These phising messages usually come from friends that have been hacked and send out the scammed email to their friends.	–	●	●	○	–
Social Network	Use the account of the most people in the country to ask followers send bitcoin to the anonymous address	–	●	●	–	–
Social Network	" Million accounts password were leaked.LinkeIn required users and affected cardholfer to change their passwords	–	◐	–	–	–
Technology	Fraudulent Phishing emails were sent to employees, tricking them to wire money to an anonymous account	–	●	●	–	–
Technology	Two individuals outside the company had inappropriately accessed user data stored	–	–	–	◐	–
Enterprise	Installed malware to capture other customer's data.	–	–	–	◐	–

Figure 4: Scenario Analysis-Human Factor Assessment (Continued)

According to the data breach report by internal business machine (IBM) security, the goal of phishing emails is to trick the receiver into believing that the message is urgent or important to open (IBM, 2020). Therefore, perceptual error, which is the inability to judge a situation accurately due to unconscious biases, is the reason for people responding to phishing emails. In another scenario, threat actors may use a phishing scam to target users that have high stress levels or lack cybercrime awareness (IBM, 2020). Through literature review, unsafe acts and preconditional unsafe acts are predominant factors of phishing attacks and scams. Therefore, perceptual error, condition of operators, and personal factor are assigned the weight of filled

circle in figure 3 and figure 4. Other human factors for phishing attacks have a low effect on the scenario. In different situations, Naveen Goud from Cybersecurity Insiders reported that financial institutions suffered malware attacks because most Financial Institutions use legacy digital systems, which are defenseless to sophisticated attacks (Goud, 2020). In this case, organizational influences and unsafe supervision are responsible for the attack since the organization and supervisor fail to update the software and change the format of the system. In other words, organizational influences and unsafe supervision have a strong effect on the scenario, rather than frontline employees. Other weight assessment is evaluated by the same criterion and logic. The act of using obsolete digital systems is considered recklessness because it will preferably invite someone malicious to exploit and harm the system. This malware can steal the data and, even worse, take control of the system. In the consideration of table 1 and figure 2 and 3, it is concluded that many types of cyber-attacks pose a risk to small and large corporations when it comes to data theft. Regardless of corporation size, these cyber-attacks give rise to equal consequences. The human factors in cyber-attacks are perhaps the toughest challenge to the cybersecurity system. According to figure 2 and figure 3, most of the attack strategies target the recklessness and negligence of humans. The negligence includes not paying attention to the details of phishing emails or not having enough experience and training in detecting scams. And this recklessness represents the scenario when the institutions use the outdated legacy digital system, which is incompatible with security features surrounding access.

HFACS method is not only an application to evaluate human factors in cybersecurity but also is used in a variety of industries such as in mining, construction, and healthcare. Different industries will approach human factors from different perspectives. Rouse and his colleagues (1997) found that in medicine and aviation, safety is the primary reason for incorporating human

factors, while the military focus on how to train a large number of people to operate complex equipment (Rouse et al.,1997). Therefore, the application of HFACS and the responsible innovation are helpful in analyzing human performance in similar cases. The major threat to computer and information security that arise from humans indicates both the responsibility of human performance on technology and social construction of technology. This means the technology does not shape human action, but human action shapes technology (Rouse et al., 1997). However, HFACS is not the only framework used to evaluate human performance.

Limitations and Future Work

The first limitation to the study is not including the full dataset from the cybersecurity data statistics but only the sample of each cyber-attack case. The sample was selected to indicate the most significant to generalize the monetary lost in industry. However, at the same time, there exist chances of biasness when selecting samples. Since HFACS is not an ultimate method, there are drawbacks of using this particular method. Gui Fu (2017) found that "HFACS does not provide enough corresponding measures to predict and eliminate exterior causes" (Fu et al., 2017). Some researchers combined HFACS with another method to ensure the accuracy of the accident analysis. Researchers usually combine the HFACS framework grey system theory, a system where information of accident causes is both known and unknown, to cope with the uncertainty of the system. (Fu et al, 2017). Additionally, the scenario analysis reflects upon the description of the cyberattack method. However, the accuracy of the assessment may also depend on the information that is not publicized. The HFACS methodology in this study compares which human error might outweigh another. The information provided is not enough to elaborate if the accident causes are unintended or intended in some situations. With the combination of the historical data breach and human factor analysis, the paper would study how

the current situation may affect the economy in the next couple years. The paper would concentrate on the application of HFACS framework and grey theory to analyze accidents from a new perspective. Instead of choosing the top 10 of significant cases to evaluate, research in the future aims to select random cases from business, ranging from small to large, to prevent biases. This research paper on human factors in the cybersecurity industry is really helpful for the future of engineering practice. The paper indicates the significant role of the human factor and responsibilities along with it. In engineering practice, a mistake, whether by skill-based error or perceptual error, can lead to significant damage, loss, or mental and physical injury. Therefore, the scenario analysis in this paper along with another method (emergent condition analysis and criteria assessment) in the future will be a good combination to advance the risk management of technological systems.

Conclusion

Human factor in cyber threat is not a new topic to discuss but most of us tend to take the issue lightly since we think human error is natural. However, raising awareness such as providing training for employees may be the first step to mitigate mistakes. Besides the casual cases that cyber-attacks are caused by our habitual errors and negligence, there are some external factors that lead to the sudden increase in cyber-attack cases. Jenna Walter found that there were a 300% increase in cybercrimes reported by the FBI due to COVID-19 (Walter 2020). The difficult situation makes individuals become more unknowingly reckless because they are easy to fall into the trap of phishing emails with titles of “Covid-19 emergency” or “Emergency funding for people in need.” Overall, the number of human factors impacts the situation fluctuates due to the given emergent condition. The data breach report estimated that the worldwide information security market would reach $170.4 billion by 2022. This means that the number of cyber-attacks

will not decrease if each individual including the government, private sector and the community do not take an action such as restricting more spam emails or being more cautious of phishing traps. With the evidence that the major threat to computers and information security arises from humans, it is important to design a system-of-work to reduce the opportunity of making a mistake. In addition to providing employees with training, the improvement of workplace ergonomics, safety management, and standard operating procedure are examples of methods to enhance human performance. It is actually impossible to build a system that completely immune of human error. However, designing the system that can minimize human error is a collective effort and shared responsibility between everyday individuals and system designers.

References

Abrams, R. (2017). *Target to Pay $18.5 Million to 47 States in Security Breach Settlement.* The New York Times. https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html

Bissell, K., & Ponemon L. (2019). *Ninth annual cost of Cybercrime Study: Unlocking the Value Of Improved Cybersecurity Protection.* The cost of Cybercrime, 3-44, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Bowen, Brian, et al. *Measuring the Human Factor of Cyber Security*, Nov. 2011, www.researchgate.net/publication/232747655_Measuring_the_Human_Factor_of_Cyber_Security

Daugherty, W. (2016, June 06). *Human Error Is to Blame for Most Breaches*, February 18, 2021, http://www.cybersecuritytrend.com/topics/cyber-security/articles/421821-human-error-to-blame-most-breaches.htm

Firch, J. (2021). 10 Cyber Security Trends You Can't Ignore In 2021. April 27, 2021. https://purplesec.us/cyber-security-trends-2021/

Fruhlinger, J. (2019, May 17). Malware Explained: How to Prevent, Detect, and Recover from It. *CSO United States*. April 27, 2021, https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html

Fu, G., et al. (2017). *Comparative Study of HFACS and the 24Model Accident Causation Model,* 570-578. https://link.springer.com/content/pdf/10.1007/s12182-017-0171-4.pdf

Goud, N. (2020). *Cyber Attacks Incur $100 billion Losses to Financial Institutions.* Cybersecurity Insider. https://www.cybersecurity-insiders.com/cyber-attacks-incur-100-billion-losses-to-financial-institutions/

Gutzmer, I. (2017, September 07). *Equifax Announces Cybersecurity Incident Involving Consumer Information.* Equifax. https://investor.equifax.com/news-and-events/press-releases/2017/09-07-2017-213000628

Kraemer, S., & Carayon, P. (2014). Human Factors and Ergonomics Society Annual Meeting IBM Proceedings. *A Human Factor Vulnerability Evaluation Method for Computer and Information Security,* 1-7, https://www.researchgate.net/publication/232747655_Measuring_the_Human_Factor_of_Cyber_Security

Security. *Cost of Data Breach Report.* (2020). IBM-13-81. https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

Josh, F. (2020, March 9). *Top Cybersecurity Facts, Figures and Statistics.* CSO United States. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Khosrowshahi, D. (2017, November 21). *2016 Data Security Incident.* Uber Newsroom. https://www.uber.com/newsroom/2016-data-incident/

Leswing, K. (2020). *Twitter Hackers Who Targeted Elon Musk and Others Received $121,000 in*

Bitcoin, Analysis Shows. CNBC.

Pollock, T. (2017). Reducing Human Error in Cyber Security Using the Human Factors Analysis Classification System (HFACS). *Kennesaw State University*,1-15, https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1051&context=ccerp

Ponemon Institute LLC. (2012, January). *The Human Factor in Data Protection*. Ponemon Institute LLC, https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf

Rouse, W., et al (1997). *The Case for Human Factors in Industry and Government.* National Research Council, 1-36.

Stilgoe, J., Owen, R., Macnaghten, P. (2013). Developing A Framework for Responsible Innovation. *Research Policy*, 42, 1568-1580.

Wolff, J. (2018, Oct 04). Trump's Cyber Security Strategy is Reckless. February 18, 2021, https://www.businesstimes.com.sg/opinion/trumps-cyber-security-strategy-is-reckless