The Cybersecurity for All App

Chantel M. White

Academic Paper

20JUN21

CYSE 595 Entrepreneurship in Cybersecurity

Abstract

In this paper we will review peer reviewed articles on cybersecurity that support the need and development for our cybersecurity app. The importance cybersecurity plays with individuals and companies alike. As well as the damage that can and has been inflicted to those that were not prepared for the challenge when confronted by cyber attackers.

The Cybersecurity for All App

As the world continues to progress towards an increasingly digital society, the baked in vulnerabilities to Confidentiality, Integrity, Availability, and Authentication within systems are being constantly challenged. Threats including malware, phishing, adware, zero-day exploit, and ransomware to name a few, continue to grow in scale and magnitude. Anyone able to gain access and operate on any form of network is a player in the cyber arena, whether they would like to believe so or not.

In 2020, it was found that employees working remotely were using devices such as smartphones and tablets that were not properly secured, patched, and managed by IT security, putting their organizations at risk of a cyberattack ("Cyber Security Threats").

People in the military, working in IT related fields, contracting for the military, and most high-level government positions are required to complete annual trainings on cybersecurity to keep them aware of the current threat environment and ways to protect themselves, but that is not enough.

Training has been created for children as young as five years old to teach the basics of Cybersecurity and apps have been created to protect mobile phones the same way that you would a desktop computer. However, there are quite a few options to choose from and some of the free and cheaper apps are worse than having nothing at all, as they run in the background collecting the user's information and selling it to the highest bidder.

In the corporate sector, forty-two percent of companies have designed strategies against mobile threats, and security is cited as the main reason for businesses looking to issue smartphones to their employees. In 2020, it was found that just forty-nine percent of mobile users have an antivirus app and cybercrime is up six hundred percent due to the covid pandemic (Anderson, 2020). Protecting yourself online is hard enough for a person with a basic understanding of the internet and its threats. Now imagine the people that are new to it and/or do not use the services regularly. As society continues to become more interconnected everyone becomes a vulnerability to each other. For the majority, everyone has a cellphone. From the elementary school student to the most senior resident in your community, they are all walking vulnerabilities. As hackers continue to make advancements in their programs and methods of attack, unprotected vulnerabilities can be exploited faster and on wider scales. A post-COVID dinner party with family and friends could be the opening a hacker needs to gain access. As the guests connect their devices to the hosts network, it does not take much for the hacker to find a backdoor and an unprotected device is easy pickings. While none of the people at the dinner party maybe the final target of a hacker's scheme, any of them could be the beginning of a chain reaction. Ignorance should not be an option going forward.

With one app to provide continuous short training at multiple levels of understanding with the option to push alerts and warnings about current and new cyber related issues, we can educate the masses and create safer cyber communities. For convenience, the intention is to work with cellphone providers to get this apps installed on phones and other devices prior to activation, so people do not have to search for it. While the app will not tell people what security service (Norton, McAfee, etc..) to use on their device it will highlight success stories and the benefits that those services provide.

In short, the 'Cybersecurity for Everyone App' will be a starting place and an up-to-date pocket reference for all from the novice to expert user. Using dramatized videos, games, and learning tutorials to educate and engage the user, while providing references and links to current cybersecurity guidelines and resources.

Literature Review

Cybersecurity truly does effect everyone and here we will review articles supporting that fact and why training and understanding from even the simplest minded, is necessary.

Cybersecurity in the Workplace

In this 2019 journal recorded in the International Journal of Information Management, the conceptual domains of employees' security behavior were theoretically defined, and the study found that an organizational information security environment positively influences employees' threat appraisal and coping appraisal abilities, which in turn, positively contribute to their cybersecurity compliance behavior (Li, 2019).

This journal references studies that found some employees do not pay attention to their organization's information security policies, while others tend to underestimate information security risks even though the employees receive written security policy and instructions. These findings support the argument that individuals exposed to adequate levels of information security training from their companies do not necessarily exhibit greater levels of cybersecurity behavior (Li, 2019).

While the studies reviewed and conducted in this journal focused on employees and the impact their awareness to information security policies had/has on their cybersecurity behavior, the common factors included social pressures more than the information that was being presented to them. Which further supports the need for an inclusive cybersecurity training that includes interactive portions to keep the user engaged in the learning process.

The Cybersecurity for all app would help to reinforce the information that businesses are trying to have set in their employees as well as their family members and friends, so that everyone can hold those around them accountable when they see unsafe practices happening or developing adding the social responsibility piece to help push users to stay current and add cybersecurity into everyday conversation.

Cybersecurity in a Pandemic

In this 2020 journal reviewing cybersecurity in health care during pandemics, we are reminded that it is not only bank account information and passwords that hackers are looking to gain access to. It is also the HIPPA protected information that is hard to change or update that can be used with other methods to meet a hacker's overall objectives. We were reminded again about the phishing emails and malware that lay in waiting for someone to slip up and allow it access to the network.

It is important that we remember that some see pandemics and other disasters as opportunities to exploit others. Thriving off the heightened emotional states like fear, making the victims more susceptible to their scams (Williams, 2020). According to the World Health Organization (WHO), the number of cyberattacks launched has increased five-fold during the COVID-19 pandemic and a similar phenomenon was seen after Hurricane Katrina in 2005, where thousands of fraudulent websites appeared soliciting fake donations and offering false government relief (Williams, 2020).

Access to patient records is a gold mine for cybercriminals, as they often contain information like date of birth, insurance and health provider information, as well as genetic and health data—information that cannot be easily altered, unlike the case of a credit card being stolen (Argaw, 2020). While in these situations, the patient is exposed to a high degree of harm. The institutions that are exposed and fall victim to these attacks also receive damage to their reputations and face serious financial losses, as in most cases it is most cost-effective to pay the extortionist. For example, the University of California, San Francisco (UCSF) was hacked by the cybercrime group "Netwalker," who demanded payment in exchange for not releasing confidential information. Out of fear of the consequences of this information's release, UCSF paid the group US $1.14 million (Winder, 2020).

While hospitals and medical practices can update their own security practices, it is also important to add this awareness to our inclusive app, because again, anyone can fall for these phishing attempts, especially during a pandemic when everyone is just trying to find out what the next steps to take would be and an email with the key words, such as 'Vaccine' and 'WHO' show up in your email inbox with a link of some sort offering solutions. This journal builds on the last, with the need to engrain a cybersecurity mindset in both the employees and the patients to protect both from opportunistic hackers during fast paced disasters.

Cost benefits of Cybersecurity Awareness

This journal discusses how the benefit of a Cybersecurity Awareness Training (CSAT) program with different types of cost plays a disparate role in keeping, upgrading or lowering a company's existing security level (Zhang, 2021). Introducing the idea that all CSAT programs offered by companies are not created equal this review of programs emphasizes that employees must receive proper cybersecurity training so that they can recognize the threats to their organizations and take the appropriate actions to reduce cyber risks (Zhang, 2021).

Piccoli and Pigni (2019) show that companies can develop their optimal cybersecurity strategies by balancing the trade-offs between their desired degree of security and their total cost to achieve it. The total cost for the cybersecurity of a company includes both the anticipation cost and the failure cost. The anticipation cost refers to a company's investment in cybersecurity to actively prevent expected cyber threats; maintaining a higher degree of security requires a company to increase its anticipation cost and the failure cost represents a company's financial loss due to unpredictable cybersecurity breaches and threats (Zhang 2021).

The study conducted in this article recommends that companies collect time-series data related to security incidents (such as phishing attacks and malware infections) to see if there is a reduction in trend for those types of security incidents. Also, companies can track whether there is an increase in employees' use of strong passwords (Dimov, 2015) to measure the benefits of their CSAT programs (Zhang, 2021). The study also found that CSAT programs need to identify workers who have access to assets at different protection levels and offer them differentiated training based on their job equirements/functions or their knowledge levels involving representatives from all the related departments, such as the IT department, the human resource (HR) department and the training department. (Zhang, 2021).

In creating our Cybersecurity for All app, the takeaways from this article have been the cost analysis for companies and the understanding that a one size fits all program will not accomplish the overall goal of a safer cyber community. Yet the benefit to apps is the ability to create versions and sections. With the lessons learned from the study conducted, we will involve the different IT departments, human resource, and training departments from organizations that are willing to work with us to make sure we are covering what the requirements are for their organization for the cyber threats their users will be in most frequent contact.

We can do this by creating more sections within the app as more companies and programs adopt our app. As there are basic skills to cybersecurity that everyone should have access to, but once complete with that there will be a drop down for different job positions for more job specific training. While the exact same program will not work for everyone, the same program used for multiple individuals falling it to groups such as administrative professionals, students (elementary, middle, high, and higher education) to name a few. Maybe able to meet the expectation and requirement while keeping those of the same tiers trained to a basic line of knowledge across the board even if they work at two different businesses across town from each other but are completing the same job.

Norms for Global Cybersecurity

Discussing the unclear "rules of the road" for cyberspace this article discusses the serious conflicts that have been presented in the past. Such as the U.S. court ordering Apple to circumvent the security features of an iPhone 5C used by one of the terrorists involved in the San Bernardino shootings. Although Apple refused and made a public appeal, the incident sparked wide-ranging debates over the appropriate standards of behavior for companies like Apple and their customers (Finnemore, 2016). Emphasizing that cybersecurity norms are essential, it also puts forth that Norms are social creatures that grow out of specific contexts via social processes and interactions among groups of actors. Understanding both those contexts and those processes is as important to successful norm construction as agreeing on content (Finnemore, 2016). National regulations, international laws, professional standards, political agreements, and technical protocols are already present and need to be taken into consideration with the cyber realm. All involving substantial normative commitments in various stages of development and diffusion. This existing landscape shows that cybersecurity is not a unified problem set; cyber norms have no single "context." Instead, the Information and Communication Technology (ICT) landscape presents a diverse array of problems rooted in diverse communities of actors and requires diverse normative solutions. Norms for securing the integrity of Internet domain names present an entirely different set of issues from those involved in protecting a firm's networks, let alone those for securing critical infrastructure from a military cyber-operation (Finnemore, 2016).

While this article goes further into these cyber norms and how the C-I-A triad should be concerned more with the indirect attacks, another issue that was highlighted on was the then line between privacy and security that some are willing to step over when disasters happen but may not be so tolerant of everyday.

Going back to the example of Apple versus the U.S. court that wanted them to create a backdoor into one of the cellular phones from the company. Although some may see it as a valid venture, as Apple discussed in their public appeal, is that really where we want to go with cybersecurity. This is important because let us say Apple did go ahead and create the backdoor into the individual's phone. Well now there is a new vulnerability in all phones of that type. Well, who knows about it, maybe those who watch the news, work with Apple or are connected in some way, and possibly a few more. Now who would be affected, those that own the device, which could range across a large span of individuals. While Apple would probably send out a long update to policy notice, most will not read it and will stay in the dark on something that could cause them serious harm in the future.

This is also a scenario where our app could come in handy, by updating the consumer of the changes in a manner simple for them to understand. This leads directly into our next journal.

Public-Private Cybersecurity

This journal highlights the relative roles of the U.S. government and private sector in four important contexts related to international cybersecurity threats: (1) disrupting networks of infected computers used by transnational-criminal groups ("botnet takedowns"), (2) remediating software vulnerabilities that can be used for crime, espionage, and offensive operations ("zero-day vulnerabilities"), (3) attributing cyber intrusions to state-sponsored attackers, and (4) defending privately-owned systems and networks from sophisticated, nation-state-sponsored attackers (Eichensehr, 2017).

The public-private cybersecurity system has accreted over time as a jury-rigged response to perceived security failures and market opportunities, and it has developed without democratic deliberation or even much public awareness. The system evolved without going through the usual processes of public, governmental decision making, and because of its informality, it has also remained largely outside the scope of after-the-fact mechanisms for checking governmental actions, including, for example, congressional hearings (Eichensehr, 2017).

Returning to the issue posed in our last journal we review the issue of individual security within public-private cybersecurity. This article reviews several steps the government could take to shift the balance in favor of individual security, but accountability for decisions with potentially significant consequences are not formally written and some private cybersecurity reports may also have due process and privacy concerns for individual. Overall, this article was around the fact protecting public law values first requires understanding that they may be at risk and as new roles and contexts continue to evolve so must the tools for protecting public values (Eichensehr, 2017).

The takeaway in relation to our app is that things are always changing when it comes to policies and practices around cybersecurity. It is hard enough for those who know where to look to stay current, but these changes and updates effect everyone. Therefore, it is our belief that everyone should be kept abreast of the changes that affect them to the best of our ability. Adding a section to our app that includes current directives and policies regularly, while we update the games and features to include new documents as regularly as possible.

Centralized IT Decision Making and Cybersecurity Breaches

This journal reviews studies on the use of centralized Information Technology (IT) governance. Countering the argument, we reference earlier that there is no one-size-fits-all approach in the cyber domain (Liu, 2020). The studies in this article were preformed using 504 U.S. higher education institutions for generalizability's sake and based around the questions: Does centralized IT decision making lead to better or worse information security? In addition, under what conditions is the relationship most salient (Liu, 2020).

The study conducted, found that the universities using the centralized approach were associated with fewer cybersecurity breaches, and among them public institutions and those with extensive research activities were most pronounced (Liu, 2020).

Information Technology (IT) governance is the specification of decision rights and accountability, which is intended to encourage desired outcomes from an organization's investment in IT. Weill and Ross (2005) identify five major decision domains that fall under the purview of IT governance, including IT principles, IT architecture, IT infrastructure, business application needs, and prioritization and investment, and highlight decision making structure, alignment processes, and formal communications as the three major governance mechanisms (Liu, 2020).

While there were advantages and downsides associated with both centralized and decentralized decision making, it was found that IT governance modes that emphasize efficient operations are more likely to adopt a centralized approach to IT governance, while those that focus on rapid growth and innovation are more likely to espouse a decentralized approach (Liu, 2020).

This study concluded that centralized IT governance facilitates universal compliance with security protocols, results in better security information sharing, raises the level of awareness of security issues, and enhances coordination between business units and that the effect of centralized governance on information security is stronger when a university has a more heterogeneous IT environment with different computer operating systems and hardware from a multitude of vendors (Liu, 2020). The research provided empirical justification for making tradeoffs in flexibility to support standardized security protocols (Liu, 2020).

While earlier we concluded that our app would offer more job specific options as we grew our partnerships, we will still offer a standardized training on basic security protocols. While this study was done through higher learning institutions that offer a variety of people from different backgrounds, since our app is intended to reach most ages and people from all education levels. Starting in public school should provide us with enough baseline information to continue to move forward effectively.

Web of Cybersecurity

This article offers that cybersecurity information obtained from experience and/or derived from analyses ought to be shared across organizations and beyond national boundaries. This sharing of information can avoid situations where, for instance, countermeasures against a certain software vulnerability are available, yet an organization remains vulnerable to cyber-attacks (Takahashi, 2018). Private companies, public organizations, and national entities started to publish vulnerability repositories in the late nineties (Takahashi, 2018).

This paper introduced a mechanism to link and integrate various repositories from all over the world, linking the information and making it discoverable for others to learn and build upon.

The study concluded that their mechanism for connecting the vulnerability repositories was flexible, extensible, and scalable. Linking repositories from all over the world for various purposes (Takahashi, 2018). The mechanism can be used for various purposes, including simple information retrieval, repositories are useful for security operations. The mechanism allows automated security techniques to access assorted cybersecurity-related information and repositories all over the Internet (Takahashi, 2018).

While we continue to learn from and share our discoveries around the world when it comes to cybersecurity it reinforces the need for us to further train our citizens on the need for it since threats are truly everywhere. While threats in the United States may not be the same as those in the United Amirites Emirates, it is still important to have a basic understanding of what is out there and how to help protect yourself from being an easy victim to an opportunistic threat.

Creating a universal way to share knowledge on cybersecurity is helpful but could also be seen as dangerous when the wrong people get their hands on the information, which hackers and bad actors tend to stay in the know about the current cyber environment. When they know vulnerabilities before we can patch or insert other forms of protection, we allow our citizen to become their playthings, as there are ways for them to gain access and turn our devices against us, which makes our app all the more necessary.

We are in the arena with out the rules when we get on a network uninformed.

Risky Cybersecurity Behaviors in U.S. Workers

In this journal we reviewed an exploratory study examining the extent to which risky cybersecurity behavior is predicted by factors of cybersecurity-related avoidance behavior. Self-reported risky cybersecurity behavior was examined considering technology threat avoidance factors in a sample of 184 working adults in the United States (Gillam, 2020). While this journal takes technology-based challenges under consideration, it is the human factor that plays a critical role – a 2014 IBM Global Technology Services cybersecurity report attributed more than 70% of successful system or data breaches to human failure (Carlton, 2015).

Although the study conducted in this article focused on adults using employer-owned IT assets to perform work vice those using personally owned devices, to avoid interference if behaviors between the groups are found to differ at some future date (Carlton, 2015). The article still provided useful information. Besides the devices being used the experiments conducted in this article also controlled for age, gender, years of work experience and formal education levels as all are seen as possible confounding covariates. Overall, this study found that in this older, educated, and professional sample group if taking protective action is difficult or makes one's work more difficult, people are more likely to demonstrate higher levels of risk in the workplace.

We discussed earlier that convenience and simplicity were aims for our app. Making it easily accessible and user friendly, because if a business professional who is informed about the risks associated with cybersecurity is willing to cut corners for convenience it is not unreasonable to argue that someone with learning deficits would do the same.

Cybersecurity for Everyone and the Behavior Analysis perspective.

My current area of study is Cybersecurity, which is where I have focused my current course load. However, my undergraduate degree is in Behavior Analysis and while it has been sometime since my last course, there are areas that tie into addressing the Cybersecurity issue and its solutions. Behavior Analysis is defined by the Association for Behavior Analysis International (ABAI) as a natural science that seeks to understand the behavior of individuals, recognizing that behavior is something that individuals do and placing special emphasis on studying factors that reliably influence the behavior of individuals, and the scientific study of human behavior to help people change behavior in meaningful ways is called applied behavior analysis. Therefore, when we are looking at the problem through the behavior analysis lens, we see the problem that we have defined as the general public not having a strong understanding of cybersecurity and the role it plays in their everyday lives, and the consequence, which we see as harm being introduced to communities and workplaces by including those ignorant to the need for cybersecurity. Using the ideas of the applied behavior analysis practice which is designed and intended for use on individual subjects, my intention by including the antecedent of my Cybersecurity Training App that will hopefully be added to the standard requirements for starting up a new device, the desired behavior would be for everyone to complete the apps trainings, creating the desired outcome of a baseline of safety across the community about how to keep their devices from falling victim to known harm, while the consequence being elicited from the user will be one of positive reinforcement as completing the training will allow them to gain access to their device and hopefully provide them with the feeling of accomplishment and pride of knowing they are a bit smarter.

Other than the effect on the individuals, behavior analyst just like others practicing the realm of psychology and medicine also use computers every day. For logs, treatment plans, and a multitude of other things. Just like everyone else they are included in those that would need to assist with creating the safer cyber environment. It is important to have the perspective from within these areas of expertise on the app construction team when building the app as well, because while we would like to create something for everyone, it is important to take those who see things far different than the majority under consideration.

Is it effective?

While this app will be designed using the agile structure where we will update regularly and request feedback from all customers so that we can continue to improve and provide useful training at all education levels and across all learning styles.

The best outcome would be for every cellphone user to be fully aware and protected from the current threats in the cyber realm. Success for this app will be raising the public level of knowledge as it relates to cybersecurity by meeting the individuals where they are and providing the training and tools for them to protect themselves in a convenient and digestible manner.

While after reviewing the journals referenced throughout this paper there is no ceiling to the education this app can provide to the general public there will be hurdles ahead, when it comes to keeping the information current, accessible, and affordable.

However, it is also clear that the need for everyone to have at least a basic understanding of cybersecurity is widely accepted and understood, just as students of a certain age have access to basic knowledge through public schools, so with the right financial backing, this app could be a success.

Bringing our app to life

In order to get the ball rolling, I would first require a full team. To include app designers, cybersecurity experts, investors, and legal representatives. The initial investors would be required to pay the team, app designers would be necessary to help make an appealing and professional looking product, the cybersecurity experts would be necessary in keeping us current and the information being shared on the app relevant, while the legal counsel will keep us out of hot water as we expand and build on the app.

Once we have our team together, we would need to break our app and all that we want to do with it into smaller attainable goals. Such as first creating an application that includes current learning material and links to the correct websites offering security protection to the users, then once complete with that, pushing out the beta version while constructing the game/ fun interactive learning materials based on the information already shared in the application, and so on. Until we get to what we previously defined as the completed application.

We will also need to build our relationships with the others listed above that offer the actual security options as well as relationships with those that can help promote our application. This will be vital if our application is able to make it off the ground.

Then we will also need to create a budget along with smaller application goals noted above so that we can continue to build up while gaining more investors as our product continues to grow into what we see it can be.

Once we have developed a steady rhythm with the application updates we will go further with our allies, starting the migration into becoming a standard requirement when setting up new devices. Providing logins to users so that they only have to complete the training once over a given time period.

Next Steps.

Now that we have reviewed the impact Cybersecurity has on people from the individual to the organizational perspective the next steps would be to expand our app to include other program specific information such as an area for clear guidance in the event of a pandemic or natural disaster. That will give the apps users a quick reference of what to look for in emails and other communication mediums to verify messages are coming from a trusted source.

Revisiting our business model once we finish including the changes above into our software package, we will review the delivery options for our app, so that we may start delivering the prototype so that we can continue to build based on user feedback. First working with teachers and community service organizers to give benefits of extra credit of some sort to those willing to be our initial beta testers. We will work with our group to gauge the level of difficulty and time consumed as they completed the trainings and adjust where necessary.

Once we have the app functioning as desired and have verified the program as user friendly with our test group, we will begin pitching our idea to more investors. We would like to first start by getting our app space in the app store and promote through social media to gain a bigger and more diverse test group once we collect the data and confirm we are user friendly on a more inclusive scale we will being looking to build partnerships with the larger security companies and network providers. We will also take this time to pitch to businesses and other government programs so they can in turn promote the app to their employees as an alternative to the PowerPoint or direct policy review method of teaching.

References

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D. *et al.* Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Med Inform Decis Mak* **20,** 146 (2020). https://doi.org/10.1186/s12911-020-01161-7

Carlton, M., Levy, Y. (2015) "Expert assessment of the top platform independent cybersecurity skills for non-IT professionals," *SoutheastCon 2015, 2015, pp. 1-6, doi: 10.1109/SECON.2015.7132932.*

Dimov, D., Juzenaite, R. (2015), " Budgeting for security awareness: who-what-when-where-why-how much". https://resources.infosecinstitute.com/budgeting-for-security-awareness-who-what-when-where-why-how-much/#gref

Eichensehr, Kristen E. (2017). Public-Private Cybersecurity. *Texas Law Review, 95*(3), 467-538.

Finnemore, Martha, & Hollis, Duncan B. (2016). Constructing Norms for Global Cybersecurity. *The American Journal of International Law, 110*(3), 425-479.

Gillam, A. R., Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study, *Computers in Human Behavior, Vol. 108, 2020*

Li, Ling, He, Wu, Xu, Li, Ash, Ivan, Anwar, Mohd, & Yuan, Xiaohong. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24.

Liu, Che-Wei, Huang, Peng, & Lucas, Henry C. (2020). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems, 37*(3), 758-787.

Piccoli, G., Pigni, F. (2019), Information Systems for Managers, Prospect Press, Burlington, VT.

Takahashi, Takeshi, Panta, Bhola, Kadobayashi, Youki, & Nakao, Koji. (2018). Web of cybersecurity: Linking, locating, and discovering structured cybersecurity information. *International Journal of Communication Systems, 31*(3), E3470-N/a.

Weill, P.; and Ross, J. A matrixed approach to designing IT governance. MIT Sloan Management Review, 46, 2 (2005), 26.

Williams, Christina Meilee, Chaturvedi, Rahul, & Chakravarthy, Krishnan. (2020). Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research, 22*(9), E23692.

Winder D. (2020). The University Of California pays $1 million ransom following cyber attack. Forbes. https://www.forbes.com/sites/daveywinder/ 2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/#38c2dce18a8f [accessed 2020-07-16]

Zhang, Zuopeng, He, Wu, Li, Wenzhuo, & Abdous, M'Hammed. (2021). Cybersecurity awareness training programs: A cost–benefit analysis framework. *Industrial Management Data Systems, 121*(3), 613-636.

Cyber Security Threats and Attacks: All You Need to Know. (2020, December 4). Stealthlabs. http://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/

Anderson, S. (2020, January 24). *Antivirus and Cybersecurity Statistics, Trends & Facts 2021*. SafetyDetectives. https://www.safetydetectives.com/blog/antivirus-statistics/

WHO reports fivefold increase in cyber attacks, urges vigilance. World Health Organization. 2020 Apr 23. https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance