TKR Solutions

Rafael Figueroa Medina

Old Dominion University

CYSE 494

Akeya Porcher, MS Ed

12/2/2022

Nowadays, our society is increasingly becoming economically and socially dependent on the cyberspace (Armenia et al., 2019). Our endeavor TKR Solutions looks to become a bridge between technology and local businesses in achieving their goal while reducing the risks associated with Internet of Things (IoT) devices and the rest of the internet. We plan on achieving this by offering a consultation service with detailed reports upon conclusion highlighting various forms of risk associated within our customer's network.

Cybersecurity issues have expanded in the contemporary information and communication technology environment due to device and system diversity, ubiquitous connectivity, and varied networks. The information and communications technology (ICT) environment in modernity permits multiple sharing connectivity through the internet culminating in a soaring combination and interconnected space. The multiple networking and accessibility to the ICT components have contributed to modern-day globalization characterized by global interactions in social, economic, cultural, and political spheres. Consequently, the ICT environment harbors numerous vulnerabilities and flaws that attract exploitation by potential cyber crooks. The high interconnectivity and increased accessibility to the ICT increase the creativity of cyber crooks to access and orchestrate malicious activities which jeopardize international cyber and physical security. Current cybersecurity issues target hardware and software in ICT while aiming to disrupt services in critical sectors of the economy, such as communication and power connection. Increased cyber security issues have coincided with increased ICT compatibility and the clamor for integrating ICT components leading to interconnectivity. Current issues in cybersecurity involve threats and vulnerabilities and possible exploitation by cyber crooks necessitating risk assessment for safeguarding ICT systems and enabling business continuity.

Cyber security companies (Kaspersky lab and Symantec) have classified current trends in cyber threats by including phishing, malware web application attacks, and botnets.

The current ICT environment has other cyber security trends and consistent threats, such as distributed denial of service cyber espionage and data breaches (Kavanagh, 2019). These cyber-threats have affected SMEs worldwide due to their vulnerability and lack of capacity to address emerging threats. Research findings show that about 60% of small businesses in the UK suffered data breaches (Koeze, 2017). Similarly, over 20% of small business enterprises in the Netherlands encountered issues with data breaches and other cybercrime cases. Cybercrime and data breaches tarnish the reputation and require extra spending to address the damages and losses (Koeze, 2017). Extra expenditure by small businesses due to cybercrime stretches their limited budgets, negatively impacting their operations. Some small businesses fail to survive cybercrime and data breach experiences due to inadequate funds rendering them insolvent. More recently, global events like the COVID epidemic forced a lot of educational institution to implement a robust distance learning program in order for them to keep providing their service. This led to an increased chance of vulnerabilities due to the different programs that would be needed to utilize this program, like video chat programs like Zoom and Microsoft Teams and curriculum technology, and service providers (Ganesen et al., 2022). According to Malwarebytes, the education sector is the top target for Trojan malware.

Malware continues to perpetuate modern-day cybercrime by targeting existing and emerging vulnerabilities in ICT systems. Cyberspace criminals and attackers rely on malware to orchestrate system disruptions and damages (Kavanagh, 2019). Its mode of operation involves intrusion into systems using similar vital credentials. Malware varies depending on its mode of operation and classification. For instance, ransomware is a malware type utilizing advanced cryptography to deny bona fide users access to their devices and data until making a ransom payment (Kavanagh, 2019). Conversely, wiper attacks do not seek financial gain but disguise as ordinary malware before deleting data in the user's device. In 2016, a United

States hospital paid $17,000 in ransom compensation after a ransomware attack (Locky attack) (Kavanagh, 2019). Ransomware attacks escalated after the 2016's Locky attack growing in impact scale and scope in 2017 (Kavanagh, 2019). This situation culminated in the Petya and Wannacry attacks that significantly affected users and organizations.

Wannacry and Petya attacks attracted massive headlines in the cybersecurity sector owing to their adverse impact scope and scale of the devastation. The Wannacry attacks, for instance, inflicted systems and software relying on Microsoft Windows as an operating system. It targeted vulnerabilities in Microsoft Windows associated with the failure to institute encryption of data (Kavanagh, 2019). Consequently, Wannacry encrypted the data for users and organizations using Microsoft Windows and demanded a substantial ransom payment. Attackers sort payments made through bitcoin cryptocurrency to avoid chances of tracing and identification. Moreover, attackers capitalized on the US National Security Agency's (NSA) failure to address vulnerability upon discovery to run a remote code on the agency's unpatched device (Kavanagh, 2019). At the time of the Wannacry attacks, Microsoft was against the targeted vulnerabilities of the concerned users and organizations. However, several users and organizations ignored Microsoft's patching of the vulnerabilities, while others relied on the pirated or legacy versions of Microsoft Windows (Kavanagh, 2019). As a result, several users and organizations had their devices susceptible to vulnerabilities targeted by the Wannacry attackers.

The 2017's NotPetya attack followed the Wannacry attack but used a different mode (wiper attack) to delete data on user systems. This attack capitalized on vulnerabilities and flaws in the Microsoft Windows operating system. Microsoft Windows exhibited flaws related to passwords that became subject to exploitation by attackers (Kavanagh, 2019). The EternalBlue exploit targeted the password flaw to lift passwords retained in the RAM and launch hacking attempts on devices. This action was a larger attack affecting several

machines and multi-user networks that accessed and operated with similar login credentials. Attackers in the NotPetya attack extracted massive volumes of data from multi-user network devices (Kavanagh, 2019). Subsequently, attackers encrypt data on multi-user devices preventing access by bona fide users. The attack involved infiltrating targeted devices before exfiltrating massive amounts of data. As a result, the NotPetya attack represented a massive modern attack on the ICT environment that necessitated a risk assessment approach in cybersecurity.

The necessity of risk assessment in cyber security is apparent owing to the escalating supply chain attacks. Supply chain attacks are escalating due to increased complexity and interconnectedness in the IT market (Kavanagh, 2019) Organizations and markets have capitalized on technological advancements and the ICT environment to merge supply chain processes of forecasting, design, manufacturing, distribution shipment installations servicing, and maintenance. The merging of these supply chain processes aims at increasing efficiency and reducing process bottlenecks. However, process interconnectedness and complexity generate opportunities to insert malicious tools. According to Symantec reporting, software supply chain attacks increased by 78% in 2018 (Kavanagh, 2019). Attacks on supply chains affect end-users by compromising software codes and accessing user operations. Cybercriminals in the supply chain focus on software products and insert malware codes before entering the supply chain (Kavanaugh, 2019). Others insert malware codes at the vendor patch site before compiling unique codes. This strategy enables attackers to escape antivirus and anti-malware programs instituted in the software codes before entering the supply chain to the intended consumer.

Software developers and critical ICT physical infrastructure are primary targets of supply chain attacks. Cyber attackers target crucial credentials to compromise or divert control tools when the software reaches third parties and consumers. Moreover, cyber

attackers are targeting crucial credentials at the software development point to acquire capabilities of invading large software projects and extorting, exfiltration, manipulating, and destroying sensitive and confidential information (Kavanagh,2020). These cyberattacks are strategic and purposeful when targeting an organization's sensitive data. Moreover, modern-day cyber-attacks target vital ICT physical infrastructure third parties, and consumers use. Physical infrastructure such as routers and microchips are sources of cyber-attacks at the manufacturing, installation, shipment (supply chain), and application points. Detecting cyber-attacks in microchips and routers points of development and supply chain and installation is challenging since hardware bears the electronic signatures of manufacturers (Kavanagh, 2020). These cases and emerging cyber security issues trigger global concern about threats inherent in the supply chain.

Recent technologies for instance the Internet of Things (IoT) and Smart cities have exacerbated cyberattacks in critical industries such as healthcare and finance. In the US, financial healthcare and industrial sectors are susceptible to cyber security attacks due to IoT incorporation in their systems and operations (Kandasamy et al., 2020). The IoT-backed systems and operations in healthcare and finance firms cause concerns of insider threats involving leaking confidential information to potential cyber crooks. Insider threats manifest when organizational staff uses components of the internet of things to extract sensitive organization information (such as IP addresses) using video and photo technologies (Kandasamy et al., 2020). The extracted IP addresses and other sensitive details leaks to third parties leading to vulnerabilities and flaws in organization systems. Moreover, IoT has other insider threats to its systems and components manifesting through network connections involving Wi-Fi, Bluetooth, and flash drives Kandasamy et al., 2020). Cyber security attackers capitalize on these connections using malware-infected smart devices and compromising database and physical ICT systems.

IoT systems have several interconnected and heterogeneous devices that increase vulnerabilities to hackings and data breaches. The IoT environment contains the latest technologies, such as wearable and smart devices and sensor nodes, that require high-level security, particularly networked services, to guarantee safety against cyber-attacks. Devices using IoT technologies require cybersecurity at the cloud storage (database), web, and API (Kandasamy et al., 2020). Moreover, IoT devices and systems achieve security using secure operating systems and acquire hardware, software, and routers through reliable supply chain networks. The increasing scope of IoT systems vulnerabilities requires securing the system's surface vulnerabilities through device hardening (Kandasamy et al., 2020). Today, IoT devices in homes (security cameras and smart doorbells) are potential points of cyber-attacks. Vulnerabilities in these systems arise due to potential cross-site scripting, using devices without server certification and updates, and file directory reversals. These vulnerabilities have resulted in distributed denial-of-service attacks targeting IoT devices and systems and necessitating risk assessment processes.

The relevancy of risk assessment in the ICT environment and IoT systems is providing guaranteed security through safe practices. Risk assessment equips organizations and individuals with systems protection to prevent unforeseen intrusion and compromise of data and servers. In risk management, individuals and firms have options provided by Supervisory Control Received and Data Acquisition (SCADA) and industrial control systems ICS (Kandasamy et al., 2020). These organizations provide risk management models and methods to conduct a risk assessment. Risk assessment under the risk management models explores risk probability and domain and provides decision support for risk analysis and quantification. Subsequently, organizations and individuals modify and encrypt their software and devices in systems to enhance protection against threats (Kandasamy et al., 2020). The decision support system identifies critical infrastructure requiring elevated security against

cyber-attacks. As a result, risk assessment and risk management are relevant in ICT and IoT environments to protect against system infiltration and exfiltration and prevent degradation of performance which denies service delivery.

Risk assessment is necessary to curb increasing data breaches, ransomware, and malware attacks in the healthcare industry. Healthcare facilities have critical infrastructures that deal with sensitive and confidential client and human resource information. As a result, the healthcare industry is susceptible to phishing and malware attacks orchestrated by insider threats, where employees deliberately or accidentally share sensitive and private organization details with third-party vendors. These developments have necessitated the identification of risks before appropriately eliminating or preventing potential impacts on the healthcare industry processes and systems (Kandasamy et al., 2020). Moreover, the healthcare industry has sensitive operations utilizing sensitive devices such as insulin pumps, cardiac pacemakers, and other biomedical devices that utilize advanced technologies in the IoT environment. The deployment of advanced ICT systems in the healthcare sector has contributed to the static monitoring and real-time delivery of medical services in a ubiquitous environment (Kandasamy et al,. 2020). Despite this positive contribution of advanced ICT and IoT systems, a proportional rise in threats and potential cyber security risks have emerged. This environment requires healthcare organizations to implement risk management frameworks with risk assessment processes that discover risks and thirds before occurrence to mitigate their potential impact on devices and electronic health records.

Appropriate procedures for cybersecurity risk assessment are necessary for the healthcare industry to explore and understand inherent risks. These procedures should deploy advanced technologies such as machine learning algorithms that capture how risks emerge when exchanging sensitive client employee and organization data in healthcare organizations (Jofre et al., 2021). Implementing systems that enhance learning and understanding of risks

during operations and integrating automated solutions in the healthcare sector prevents frequent data breaches (Jofre et al., 2021). The risk assessment process enables learning and understanding of risks and potential and facilitates decision-making toward successful risk mitigation. Consequently, stakeholders in the healthcare industry can evaluate and calculate the potential impact on critical assets and operations of the organization upon a cyber-attack (Jofre et al., 2021). Moreover, advanced risk assessment models have vulnerability scoring systems that assign severity scores on flaws and vulnerabilities identified in the system and operations. These scores act as metrics guiding the categorization and prioritization of risks and deploying resources and actions to thwart the threats.

Risk management models have risk assessment procedures targeting insider threats and internet of things devices within the healthcare and financial sectors of the economy. These risk assessment procedures target employee behavior and operations while assessing the supply chain (Jofre et al., 2021). Risk assessment procedures focus on the sensitive areas of big data and the interoperability of systems in the clinical health environment. Healthcare environments prepare for potential ransomware and wiper attacks which target vulnerabilities associated with insider threats (Kandasamy et al., 2020). A risk assessment identifies flaws in operations and vulnerabilities caused by operating systems in ICT gadgets and personal missteps that contribute to data breaches. Consequently, organizations use risk assessment outcomes to institute corrective measures against personnel behavior and systems' acquisition from the supply chain to installation and maintenance.

Risk assessment is necessary for the current ICT and IoT environments where security threats exist without capabilities and understanding. The complex ICT environment and interconnectedness of systems introduction environments, particularly IT, automotive, pharmaceutical, and telecommunication Industries, have generated unforeseen vulnerabilities for cyber-attacks (Kandasamy et al., 2020). Moreover, security threats continue to emerge

and escalate in wireless Mobile communications and newly developed systems in telecommunication healthcare finance and other modern-day systems. As a result, risk assessment enables organizations to undertake appropriate risk management by analyzing, interpreting, and developing knowledge of these emerging security threats (Jofre et al., 2021). It enables the development of protective methods and policies to address multiple sources of vulnerabilities and points of failure in complex and interconnected systems. Risk assessment in interconnected systems is also necessary to prevent enormous damage and disruption orchestrated by cyber-attacks on the ecosystem.

Ultimately risk management that uses relevant risk assessment procedures is necessary for the modern-day interconnected and complex ICT and IoT ecosystems. The new paradigm involves the interconnectivity of devices ranging from personal laptops, smartphones, Smart cars, city wearables, and other IoT devices. Moreover, supply chain processes of Several production processes in the software, automotive, pharmaceutical, and healthcare Industries exhibit similar complexities and interconnectivity. The primary intention of highly complex and interconnected systems is to increase efficiency and reliability in production and supply chain networks. However, the increased interconnectivity among systems using networks and nodes creates several points of failure and vulnerabilities, becoming attack vectors for cyber criminals and malicious intruders. The dynamism and intricacy of the supply chain network and networked IoT environment cause unknown flaws serving as fodder for cyber-criminals to capitalize and intrude into the ecosystem. The interconnected IoT environment has several actors operating without due diligence and outside regulatory frameworks. The interconnectedness of services, stakeholders and systems operating outside regulatory requirements opens doors for intrusion and cyber-attacks on the entire ecosystem.

The procedures is not the only necessary items that go into play. Implementing a fostering a culture of good cyber behavior is as crucial as practicing good ethics within an organization. According to the Federal Financial Institutions Examination Council (FFIEC), It is not simply the obligation of those employees in the server room, but rather an enterprise-wide initiative involving all employees. It is crucial the board institutes a corporate culture prioritizing cybersecurity (Wright, 2021).

Our innovation relates to many other different disciplines. As long as our customers has any device that can potentially connect to the internet or some other forms of technology like Bluetooth, there can be risk involved that if left unattended can cause substantial harm within an organization. For example, I have taken classes within my time in school that varied from Oceanography, all the way to Accounting. Our service can benefit both areas and offer beneficial insight that can assist them in their endeavors. Oceanographers often utilize different means of technology within their areas. A lot of scientists record their data on paper while they are out on the field but is later transcribed within a laptop for storage and later use. They also sometimes rely on various communications systems that are spread around different bodies of water in order to get necessary data for their research or current experiment. Our service can help them ensure that they are taking the necessary steps and precautions to safeguard their information mitigate potential risks associated. Not only can we offer that service, but we can also educate them on recovery procedures based on their structures, so that if some sort of mishap were to occur, like a damaged or stolen laptop, they have some sort of means of recovering their data. If an entrepreneur is working on some sort of project that will benefit their community, and they are only working off a single laptop with all of their work from their project, what steps are they doing to back their information up? Do they have a process in place to access their information from another medium? Often times local entrepreneurs have very limited time and resources to look at the entire

picture and really think about some of the things that they will need if things were to take a bad turn. My other example is accounting, which is an entirely different monster on its own. There is so much data and money associated within this field that if left unchecked, people can actually go to jail. Every entrepreneur will deal with this field regardless of their work. There are actual regulations associated with this field like the Payment Card Industry Data Security Standard (PCI DSS) which is a compliance that any business that transmit, stores, handles, or accepts credit card data must follow. It is designed to keep user data safe and prevent attacks that would steal sensitive data. There are many other compliances, but it is something that entrepreneurs may not be aware of, and they have to ensure that whatever set up that have in place are in accordance with the different regulations that are out there.

Perhaps the customer owns a salon business, and they decide to purchase a website from a third-party vendor in order to take appointments and accept payments, but the actual website is not in an acceptable format where it is safeguarding information. The owner most likely is not going to have the knowledge in order to catch this potential issue, nor the company who supplied the website is not going to regularly check and monitor the site if the owner is not complaining about it. Our service can potentially catch the issue and bring it to the owner's attention and possibly offer a solution that will help them conduct their business in a more secure fashion, or give a recommendation that perhaps will cost less, which will leave more monetary resources to allocate in a different area of their business.

Our innovation does not have to impact an area directly or physically like our previous examples, sometimes the other disciplines directly apply and relate to the material. Cybersecurity is an interdisciplinary field which means that it is composed of various of disciplines. Specialties like Psychology has a direct impact in our innovation because cybersecurity deals with a lot of psychological aspects because its studying people's mindset in manipulating machines. Some of the foundational skills you learn in cybersecurity is

learning about the different types of attackers and the desired agendas that they want to achieve. You also learn about different attacks that deal with manipulating the mindset of people which are called social engineering attacks. It can be something as simple as playing a video of an infant crying while calling a company and trying to acquire someone else's sensitive material, by wearing down the patience of the employee who received the call.

Regardless of the kind of impact cybersecurity and risk analysis have in different areas, the fact remains that it transcends to different areas, and can have a beneficial impact.

Our organization can determine the effectiveness of our innovation in several different ways. One of the clear indicators of measuring success is looking at the amount of revenue that was earned and comparing it to previous cycles. If there is a steady increase in revenue, that can be one indication that can say that the organization is progressing in a positive direction. Surveys can also be an effective tool. Depending on how an organization values effectiveness and success, satisfied and pleased customers can be a big attribute. Happy and satisfied customers can lead to more customers which can have a positive effect in the direction of your organization, and in turn negative reviews can give the organization an area to focus on and improve. Another way can be by comparing the results from the assessment. We plan on offering a free re-assessment either at the 6 month or 1 year mark from the initial assessment, to see what processes changed and how effective they are based upon the various risk factors that we encounter. This process will give our company a very good baseline in evaluating not just the effectiveness of our company, but also how the other companies are receptive and implementing of our recommendations. I ran across an article about innovation online by Stefan Mitzkus and the different ways that companies can measure their success which was very interesting. They displayed different metrics like product innovation, innovation ratio, and degree of innovation. Each has its own measurement with guidelines, and each has its own meaning. Product innovation is the rate

that represents your innovation activity in relation to your sales. It shows whether your new developments are successful on the market or not, and it is measured by revenue share of innovation / total revenue * 100. Innovation Ratio shows how important innovations are to your company because it relates their number to your total product range. When it is paired with the innovation rate, it can give a clear indication on the success of your innovations.

At the end of the day, depending on how the organization wants to measure and view their effectiveness, they are a myriad of different tactics and methods that they can employ or utilize to measure the effectiveness of that attribute.

In order to make our organization a reality, there are different things that would have to be put in place in order to start our endeavor. First and foremost, my partners and I would have to know where the funds in order to purchase the materials we need will come from. We would have to sit down and decide together on how many stations we need and the different software licenses we will require in order to conduct our job. All of those things cost money, and nothing in the IT world is cheap. There may be an option where we supply some of our own money, but most likely it will end up being that the company would borrow the capital in order to get the assets that we need.

We would also need to make sure they we have the required credentials in order to be able to conduct our jobs. Although there is not any specific cybersecurity or IT certification that are federally regulated for consulting services, there is a lot of different certifications and standards that are aligned with many of the popular frameworks that are utilized by several of companies across the globe. Certifications like COMPTIA Security+, COMPTIA Pen Tester, Certified in Risk Information Systems Control (CRISC), Certified in the Governance of Enterprise IT (CGEIT), Chartered Enterprise Risk Analyst (CERA), and Control Objectives for Information and Related Technologies (COBIT). These certifications are not all inclusive

and are also constantly changing and evolving. They will allow us to have those credentials to further show our customers that we are indeed aligned with community and standard practices within our area. Now every employee will not need to have every single certification in order to be able to work with our organization, but we will have a certified technician doing the work in their respective field when conducting our assessments.

Finding the right type of business to start up as that will offer us the most protection while increasing our tax options a credibility. A Limited Liability Company (LLC) is our best bet in starting off our organization. Once we have our paperwork set up, we have to continue to get our affairs in order within our business. Along with registering the business, we would also have to ensure that we get our Employer Identification Number and open up a business account if needed. Additional Professional Liability is another option that will gives our company an additional layer of protection, against various claims such as negligence.

Another component that would be nice to have but isn't necessarily a must need at the time of launch would be a centralized location to serve as our hub for our services. There we can safeguard and protect our physical assets like computers in one area, and we can also have a central place where people can communicate and work together on different projects. Funding may require us to work remotely and utilize different services like cloud technologies to avoid building and maintenance costs.

Once all of that is settled, another thing we would have to do to make our innovation a reality is to create a website of our company along with the services that we provide. Within our website, we can have an educational area, where we can provide information regarding common mistakes made by new business owners, or links to other reputable resources that can assist people with securing their organizational networks.

Finally, before everything is implemented and the organization goes live, we would have to ensure that our methods and processes are in place and aligned with the company goals. We would need to find some entrepreneurs who can volunteer their company for complimentary assessments, and we can work out any unforeseen details with our hardware or software, before we take our company live and start charging fees for assessing people.

The next step that would be needed to take with our organization is to compile a list of the various different software that we need to do our job. Applications that serve as penetration testers like Nessus are crucial because it can scan inputted IP Address and come up with various vulnerabilities based on their current firewall configurations. The vulnerabilities are based on score of severity and color based on how effective or catastrophic the damages could be if that vulnerability were to be exploited. It also gives a code that aligns with other applications like Metasploit which can serve as a tool to attack various networks and gain control to exploit users and their systems.

Once we are able to acquire the necessary software in order to conduct our job, another step would be to generate contracts for both internal and external use. The internal use contracts would be more of a non-disclosure agreement, so that our intellectual property or processes aren't spread by our employees for the period of time that they are employed with us and a certain period of time for after. The external contracts would be for our clients, and would be a service agreement that clearly define expectation for both the company and our clients. We would work with an experienced attorneys in LLCs to ensure that documentation is aligned with current practices, and that verbiage in place protects both the company and the customer. We understand and tell our customers that our findings and never all-inclusive. It's important to understand that in this field, there are always emerging

technologies and processes, and we offer a service that puts organizations in the best place to mitigate those risks.

Once all of that is in order, we would start looking for a hiring quality employees. Until we are able to get some type of human resource team in place, we have to make sure that are processes are aligned with any state and federal laws, as well as obtain workers compensation insurance to protect our employees who become injured or ill at work.

Dear Director,

TKR Solutions is a cybersecurity risk assessment consultation company, that is designed to assist up and coming entrepreneurs mitigate the various risks associated with the use of technology. We understand that entrepreneurs are often time stretched thin due to the scarcity of resources and personal limitations of time in order to conduct their day-to-day jobs, and we are looking for ways to add solutions and reducing the number of businesses that fail because they can not recover from a cyberattack. The way our project would work is that we would talk with the business and find out as much information as we can related to their organization and the processes in place from start to finish. We would observe, and work with the company in understanding their most important assets, and we will look at the different ways they protect, monitor, respond, and recover actions associated with those assets. Based on our findings, we can offer various solutions to help mitigate the potential risks that were found. Our process can be beneficial to these new business owners because there may be certain processes in place that we might think are being over or underutilized, which can help these owners reallocate their resources in different areas to make their endeavor more impactful. Throughout this journey, I learned a lot about the various details regarding starting up a business, and a lot of the different compliances associated with it. I

also learned the economic principal of scarcity, and that regardless of what I may think, that I do not have unlimited resources, and I have to learn to make tough decisions in where to allocate those limited resources and time that I have. Students might find value to my project because technology is a thing that we as a society are relying on a lot. We bank, shop, monitor, and communicate through the internet, and it is sad to say with so many people devoted to their devices, they don't understand or want to educate themselves on the various risk associated with it. Too often are people clicking on random emails from unknown centers with links that may lead to malicious malware that will compromise their device along with any sensitive information on there. I want to offer a service or solution to assist with those means and help people understand that it isn't really that hard or complicated to take some steps in protecting yourself. If I were to be sought out from advanced technology center for work as a consultant, some of the things I would do different is monitor more consulting companies to ensure that we are someone aligned with the methods that are out there. I would ask more questions about why certain things are and aren't in place, so I can better educate myself and my peers.

References

Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E., & Medaglia, C. (2019). Towards the Definition of a Dynamic and Systemic Assessment for Cybersecurity Risks. Systems Research and Behavioral Science, 36(4), 404-423.

Kavanagh, C. (2019). *Stemming the exploitation of ICT threats and vulnerabilities: An overview of current trends, enabling dynamics and private sector responses*. United Nations Institute for Disarmament Research. Medium https://unidir.org/sites/default/files/publication/pdfs//stemming-the-exploitation-of-ict-threats-and-vulnerabilities-en-805.pdf

Ganesen, R., Asmidar Abu Bakar, Ramli, R., Fiza Abdul Rahim, & Md Nabil Ahmad Zawawi. (2022). Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions. *International Journal of Advanced Computer Science & Applications, 13*(8), International journal of advanced computer science & applications, 2022, Vol.13 (8).

Zamora, W., & ABOUT THE AUTHOR Wendy Zamora . (n.d.). *Trojans, ransomware dominate 2018–2019 education threat landscape: Malwarebytes labs*. Malwarebytes. Retrieved November 21, 2022, from https://www.malwarebytes.com/blog/news/2019/08/trojans-ransomware-dominate-2018-2019-education-threat-landscape

Koeze, R. (2017). Designing a cyber-risk assessment tool for small to medium enterprises. Medium https://repository.tudelft.nl/islandora/object/uuid:8ffae35d-0695-4eb9-b488-471bd1c9e10d/datastream/OBJ/download

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*(1), 1-18. Medium https://jis-eurasipjournals.springeropen.com/counter/pdf/10.1186/s13635-020-00111-0.pdf

Jofre, M., Navarro-Llobet, D., Agulló, R., Puig, J., Gonzalez-Granadillo, G., Mora Zamorano, J., & Romeu, R. (2021). Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach. *Applied Sciences*, *11*(15), 6699. Medium https://upcommons.upc.edu/bitstream/handle/2117/356888/applsci-11-06699-v2.pdf?sequence=1

Wright, M. (2021). What's in a cybersecurity risk assessment? *Independent Banker, 71*(10), 36-37.