Osaze Osadolor

IT 659

Dr. Horton

February 7, 2021

**Milestone 1**

Introduction: Application of Cyber Principles

The case of Cybercrime has become very rampant in businesses, e-commerce and communication industries. According to the website cyber.gov.au, it says “The purpose of cyber security principles is to provide strategic guidance on how organizations can protect their systems and information from cyber threats. These cyber security principles are grouped into four key activities: govern, protect, detect and respond” (Australian Cyber Security Center, 2020). In order to apply the cyberlaw and security principles to certain businesses especially the government agency, Washington State Social Security Services didn’t follow certain procedures in order to safeguard people’s social security details. This led to problems with hackers having access to civilian names and using those names to file for benefits. According to Black Point Cyber, it says these are the principles that drive the services at Blackpoint. The article says, “Detection instead of prevention, historically, cyber security solutions have focused on prevention and in a perfect world, this would be the best solution. However, preventing all possible methods of compromise is arguably impossible. Therefore, an effective detection solution must be put into place to catch anything that the firewalls, intrusion prevention systems (IPS) do not catch.

Focus on detecting the common elements of malicious activity, not malware. Examples of common elements include enumeration, lateral spread, and account compromise. Do not focus exclusively on malware detection which is reactionary strategy as malware is constantly evolving and is not the only source of compromise. Asset visibility is crucial to effective cyber security. In order to best protect an organization’s infrastructure, the organization must first know what is connected to it. With the growth in smartphones, IP enabled devices and the Internet of things, organizations need to know what devices are connected to their infrastructure, where they are located, and what they are doing in real time. Detection and response must be faster. Statistics vary on average duration between the initial compromise of an organization and its detection, but it has been known to take several months at least. If organizations are going to win the cyber fight, this detect, and response time must be reduced to hours, minutes and seconds (BlackPoint Cyber, 2019). What this means is that due to the problems that were caused by the hackers, it is best for the organization to run tests to know what the networks are connected too. What will be best is to actually have designated people try to hack the network that way it will help the organization to always be prepared in case of a cyber hack.

Introduction: Summary of Case

The Washington state social security service was breached and the reason why it happened was due to the government organization not checking identities since this breech happened earlier in the year around March, and this was when COVID 19 hit the US making it a very chaotic period. People were asked to not come to work for protection purposes and due to this, some people had to file for unemployment. This was the best time for the man Hushpuppi and his group of cyber criminals to target the Washington State Social Security Services and use stolen social security numbers that were stolen years ago and claim benefits from American citizens. The reason why the Social Security benefit failed to protect its information at this crucial COVID time was because there were so many people filing for unemployment benefits that they did not carefully check who needed it. In the article “The Nigerian Fraudsters ripping off the Unemployment System” written by Lily Hay Newman, she says, “As millions of people around the US scrambled in recent weeks to collect unemployment benefits and disbursements through the Federal Cares Act, officials warned about the looming threat of Covid 19 related scams online.

On Thursday, the secret service issued an alert about a massive operation to file fraudulent unemployment claims in states around the country like Washington and Massachusetts. Officials attributed the activity to Nigerian scammers and said millions of dollars had already been stolen. The email security firm Agari today release findings that an actor within the Nigerian cybercriminal group Scattered Canary is filing fraudulent unemployment claims and receiving benefits from multiple states, while also receiving Cares payouts from the Internal Revenue Service. So far this has netted hundreds of thousands of dollars in scam payments. Scattered Canary is said to be a full- service “business email compromise” operation that uses scams like email impersonation and phishing to manipulate businesses into paying out phony contracts’ other fake invoices. Then they use a network of money mules within the US and around the world to route the money. The scammers can file dozens of individual submissions under as many people’s names using their specific personal information, while managing it all from one centralized email account. One campaign the Agari researchers analyzed used 259 variations of the same address” (Hay, 2020).

In conclusion, this is a detailed explanation on why certain businesses for example government owned businesses like the Social Security Service, should always have their data secured daily so has to not have incidents like the ones listed above.

**Milestone 2**

Ethical issues tend to happen in companies, and this can cause a lot of problems for the firm, the leaders, employees and customers. When an organization has ethical issues, this ranges from accounting, social media, harassment and discrimination, health and safety and finally technology and privacy. According to floridatechonline, “Cooking the books, and otherwise conducting unethical accounting practices is a serious problem, especially in publicly traded companies. The widespread nature of social media has made it a factor in employee conduct and after hours. Is it ethical for companies to fire or otherwise punish employees for what they post about? Are social media posts counted as free speech? The line is drawn when an employee’s online activities are considered disloyal to the employer” (Florida Tech, 2021).

As for the Washington State social security department, the problems that they had was that they did not do due diligence to know who the people were filing for unemployment. If they did a background check to figure out who were the people filing for unemployment, then they would have known that some of these people were not actually employed by the companies. They should have also given calls and mails to the people who filed for unemployment to be sure that the citizens also have records that they filed for unemployment almost like a security check. The second unethical thing that was done was the giving away of government money in a hurry. This although can be supported because it was during the COVID19 pandemic and companies were letting go of their employees. Due to this problem, a number of citizens had to claim unemployment benefits. This was a good time for the hackers to claim any identity that they have stolen over the years because the social security services of Washington state had to make sure that a number of people got their help during this unprecedented time.

According to the social security administration on ssa.gov, there are different laws that should be followed. For example, Subpart B – The Privacy Act, chapter 3 part 401. 45 which writes on the verifying your identity says “When required. Unless you are making a request of or access to a record in person, and you are personally known to the SSA representative, you must verify your identity in accordance. You make a request for notification of a record and we determine that the mere notice of the existence of the record would be a clearly unwarranted invasion of privacy if disclosed to someone other than the subject individual. Request by telephone. If you make a request by telephone, you must verify your identity by providing identifying particulars which parallel the record to which notification or access is being sought. If we determine that the particulars provided by phone are insufficient, you will be required to submit your request in writing or in person” (Social Security Agency, 2021). The government agency according to the writing above shows that they were no mention of unethical issues that might have happened because it the standards look very secure. The main problem that can be seen from this is that by using the telephone, hackers could have easily gotten the information before then and might have pretended to be the stolen identity. According to Rachel la Corte, she says “The breach happened because of vulnerability in an Adobe systems Inc software program, ColdFusion, that has since been patched. Keeling said officials have added a number of additional security measures including isolating anything that could be sensitive into more protected areas implementing code to prevent hackers from getting to other parts of a server and new encryption rules. The administrative office in Washington state will be asking for personal information over the phone and via email related to breach” (Corte, 2013). The problem that can be seen here is that the state is still going to be using telephone and emails as a primary source. This is a legal compliance issue within the organization and until they find better ways, there will still be future incidents (La Corte, 2013).

This problem has brought about a number of societal and cultural impacts due to these issues with the government. In most cases due to identities being stolen and money being stolen, citizens had lack of trust for the government. According to the Washington Post, written by Aaron Blake, Washington state was a 55 percent when it came to trusting the government. Since the average percentage is 50 percent, we can say that the state of Washington is still trusted but it is low compared to states that were above 70 percent that showed a great amount of trust. States like Alaska, Texas, North Dakota and Utah (Blake, 2014).

The next impact that happened was that citizens did not have their checks due to the slow process distributing pandemic benefits. This was because there were so many people requesting at the same time. The criminals already used the names of the people they stole identities to claim benefits so when the person decided to get their benefit, it did not go through because it was recorded as it was already given. This also caused a lot of anxiety to the citizens some people were not able to pay rent, some were not able to feed and this caused a lot of homelessness. According to DW News, the Coronavirus leads to increase in homelessness in the US. “The coronavirus pandemic isn’t just a threat to the health of people around the world. It also puts their livelihoods at risks. The pressure is especially high for people in the US, where the loss of income has left many people evicted and homeless (Wells, 2020.). According to the Washington State Attorney General, the long-term impacts of data breaches, “The ocean of stolen personal data, according to the Washington’s Employment Security Department, helped cause the widespread unemployment fraud that occurred in May. This resulted in the theft of hundreds of millions of dollars from ESD during the COVID 19 pandemic. This added undue stress and made it more difficult for thousands of Washingtonians whose identities were stolen outside ESD’s system to collect unemployment benefits when residents needed them the most in the midst of the pandemic. Washingtonians are increasingly relying on digital and online services that collect user data to conduct business. This increase in online activity may create more opportunities for cybercriminals to steal personal information” (Ferguson, 2020). This shows that even with the stolen information, people are still relying on technology to get them through the day and there are still threats at large. Minorities will suffer the most from this problem because of systematic racism and before help comes to them it might be too late for a lot.

Due to the problem that happened at Washington state, the state government tried to bring different regulations that could help the citizens. The first thing on the list to safeguard the citizen according to Megan Leonhardt “Americans have lost over 68 million dollars in scams and fraud schemes related to the coronavirus pandemic since the beginning of the year. Consumers need to be extra vigilant right now, which includes taking steps to protect yourself. Don’t give credit card or personal information to anyone over the phone, don’t click unknown links in emails and don’t even answer the door for someone claiming to be from the government unless they can show proper identification. Assume it is a scam until someone proves otherwise” (Leonhardt, 2020). The new regulatory changes are mostly for the consumer and it says to set up an account, this will prevent someone else from doing it in your name and getting a benefit that you don’t know. Second is to change your passwords, many identity theft scams happening right now are done by fraudsters who obtained log-in information from data breaches that have occurred within the past few years. Use multiple verification safeguards for accounts and lastly stay alert. By following these regulations, the government says it will help citizens to safeguard their identity and stop cyber theft (Leonhardt, 2020).

When it comes to the impact standards, a comparison with the Washington state social security services compared to a company like Adobe, the difference was very clear. In October of 2013, according to Dan Swinhoe, he says” Adobe originally reported that hackers had stolen nearly 3 million encrypted customer credit cards records, plus login data for an undetermined number of user accounts. Later that month, Adobe raised that estimate to include IDs and encrypted passwords for 38 million active users. Weeks of research showed that the hack had also exposed customer names, IDs passwords and debit = and credit card information. An agreement in August 2015 called for Adobe to pay a 1.1 million in legal fees and an undisclosed amount to users to settle claims violating the customer records act and unfair business practices” (Swinhoe, 2020). This standard is norm but compared to the government who got hacked the same way through using false identity to take COVID 19 claims, they should also have been made to pay a fine for allowing citizens of Washington state have no benefits during a pandemic. Instead, nothing was done about it and as being representatives of the government, they weren’t subjected to any fine. All they did was inform the citizens about the false claims and instruct citizens how to be safe with their information.

The cultural impact of cybercrime has made people to become more diligent at making sure to not go on sites that might have malware. It has also made businesses to hire cyber security specialists that will protect information. In this day and age, once a company gets breeched thanks to social media and the media in general, it usually doesn’t take that much time for the rest of the world to know and that can have a very negative impact on the company. Due to this there are more demands on people with a background in IT to help protect various firms from outside hackers. There are now more colleges advertising online to get students into cybersecurity. Due to the fear of information being stolen, there are now television shows that talk about how the future of computers will be and how information will be stored. For example, a show called Black Mirror on Netflix, specific episode “The Entire History of You” shows that “In the not so remote future, people have implanted a device called the grain behind their ear which allows them to record everything they see and hear. Whenever they need, they can re-watch the recordings of their memories directly into their mind” In shows that data now can be stored directly to the human and shown on a screen. This means that technology has become so much more advanced that we can now use our minds and project what we see into a screen. Keeping our information to ourselves alone for protection is the way the future looks in that world. This makes it very hard to steal information in the future. It also shows that in our modern-day era, security is important to us and we need to be wary on what someone can do if they steal our information. This is specifically important in the 2016 election when Trump ran against Hillary and the Russian hack was a big topic.

In conclusion ethical issues and legal issues can affect any business especially when it comes to keeping the customers identity safe and companies must work harder to find better ways to keep information safe because the hackers are also working twice as hard.

**Milestone 3**

Whenever businesses are compromised by hackers or fraudsters, there is always a big lesson that they learn from such experience. Although, there are many ways a business can learn from these experiences and create big changes to the organization. Washington state social security department is a government institution. Government institutions most times get hacked more than private organizations.

**Recommendations: Organizational Changes**

According to The Washington Post, written by Jeffrey Neal, he says “Many agencies decentralize control of IT and allow program offices to manage the technology that supports their program, rather than having a team of experts who understand technology and a fully engaged leadership team who know what information needs to be protected. They are focused on driving their program rather than what is going on under the hood. The desire to control every aspect of a program is common, and it is based partly on fear that someone else will not do the work as well and partly on purely parochial interests of power and control” (Neal, 2015).

What can be taken from this is that there needs to be a change in the culture of government organizations. Most workers feel like they don’t have the right to talk to their superior even when there is a problem so sometimes it when there is a little problem it is partly ignored until it grows bigger and affects other people. According to the website competition bureau, it gives top 10 fraud fighting tips for businesses. It says “Invest in your people, provide training to employees on scam detection and prevention. Talk about scams and share information in employee meetings. Ensure employees know not to provide personal or business information and banking details to anyone not known and trusted. Let employees know that if a request seems suspicious, they should do an online search and independently verify it. Invest in your networks, consider what business information you post on social media and networking sites, as scammers use publicly available information to target businesses. Invest in security systems to keep your office networks, computers and mobile devices secure. Update your security software, change passwords and backup data regularly. Also, store your backups offsite and offline (Government of Canada, 2019).

**Ethical Guidelines/ External standards**

There are a number of steps that the Washington state social security agency could have done to help prevent future incidents within the organization. According to Investment industry regulatory organization of Canada, it says “Governance Framework – The first step a board or executive team should take is to determine who within the company should be involved in the development of a cybersecurity program. Key initial steps include identifying known risks and established controls. A best practice is to establish a cross organizational committee of senior executives that bring together the full range of enterprise knowledge and capabilities” (IIROC, pg.12, 2020). The author Aidan Knowles says, “Ethics – moral principles that govern a person’s behavior is a critical part of any sound cyber security defense strategy. Without clear ethical standards and rules, cybersecurity professionals are almost undistinguished from the black hat criminals against whom they seek to protect systems and data. In this frenetic climate, we tend to focus on developing individual’s cybersecurity knowledge and talent and putting them on the front line as quickly as possible. In a mad rush, we tend to forget to consider how new recruits could potentially abuse these abilities on the job or in the wild. Individuals must defer to their moral compass. This leads to good decisions as often as it leads to mistakes” (Knowles,2016). Other ethical considerations that should be done to prevent future incidents in the organization are:

1. “Be diligent about enforcing policies – Not everyone is going to uphold every single ethical expectation 100 percent of the time, and rules will inevitably be broken. It’s important that you don’t tolerate unacceptable behavior and show that there are consequences.
2. Praise Positive Behavior – Just as it’s important to stomp out unethical practices, it’s equally important to praise your employees for following best practices. This doesn’t have to be anything over the top, but you should make it a point to acknowledge individuals who live up to expectations.
3. There should be limitations on using company technology for anything other than work in the organization this is very important because hackers could find ways to hack social media sites and that could be the key to finding their way to the organization’s information.” (Resource Management Inc, 2016).

The agency being discussed is the Washington state Social security agency. The external changes would mean the external environment which also means the general environment. Since the organization that is being discussed is a government institution, this means it has to work with the community. According to the webpage External and Internal Organizational environments and Corporate Culture, it says “Types of general macro environments and forces that are interrelated and affect organizations are sociocultural, technological, economic, government and political problems that affect industries and organizations. Hiring and unemployment, employee benefits, politics and governmental policies” (BC campus, 2021). What this means is that Washington state social security agency should give more incentives for the employees so that they will be able to work to their highest capacity. Most people who work for the government don’t work to get high paying jobs but to enjoy the benefits that come with the job. According to the Eric Katz, he says “Biden tells civil servants, you’re the ones running the show. We’re a team. Biden says You’re patriots. You could have done a lot of other things with your careers, but you chose public service. Biden proposed a new minimum wage so federal employees no less than $15 dollars an hour. Before the minimum wage as of 2020 when this incident happened was $10.80 per hour” (Katz, 2021). This is very big because government workers weren’t paid much in the past year and now with this increase in 2021, it will make the workers very diligent and they will make sure to treat the government’s information as their own.

**Global Considerations: International Compliance**

In order to have international compliance standards, the company has to be a trusted company globally. Even though the organization is a government agency the same rules apply. The ISO 27032 explains international compliance standards. Antonio Segovia says “Protect your organization against cyber risks. ISO 27032 provides guidance on addressing common cybersecurity risks, including user endpoint security, network security and critical infrastructure protection. Since this organization is a government owned organization, the ISO 27032 specifies different threats like ISO 27005, but it does give some examples, applied of course to cyberspace. ISO 27032 specifies different types of assets and does not contain a catalogue of threats and vulnerabilities” (Segovia, 2015). ISO 27032 provides guidance for improving the state of cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains in particular to information security, network security, internet security and critical information infrastructural protection. If the company were to be a non-government institution, there will be compliances that will work with it. For example, the webpage for Deloitte says “Establishing an effective cybersecurity program is a major challenge for every company regardless of industry and geography. However, the challenge is much greater for businesses that operate internationally since they must comply with regulations from multiple jurisdictions and multiple regulators. Examples of regulatory similarities:

Around the world, various jurisdictions have established their own unique regulations for cyber integrity in banking.

* MAS TRM and Notice 644: Notice on technology risk management (Singapore). This notice issued pursuant to section 55 of the Banking Act and applies to all banks in Singapore.
* Interagency Guidelines establishing Information Security Standards (12 CFR Part 30) (United States). Regulatory agencies are considering applying enhanced standards to certain entities with total enterprise-wide consolidated assets of $50 billion or more.
* NYDFS Cyber Rule (23 nycrr 500) (New York). This rule stipulates that each covered entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of its information systems” (Deloitte US, 2018).

**Global Considerations: Cultural Impacts**

Due to the hacking that took place in the Washington State Agency, this act could not just cost the information of the citizens social security numbers, but it could test how these cyberattack specialist could manipulate their government elections. The US is seen as one or maybe the leading country in the world in terms of military power, GDP and technological advancement. Most countries are a far second when it comes to the comparison. According to Kartikay and Dina from Bloomberg news, they say, “The cyber-attack on Washington state didn’t impact the state’s election systems. Nonetheless, coming nearly a month ahead of November’s presidential election, it highlights the potential vulnerability of state computer networks, which include election systems… still, the timing of the attack has raised security questions ahead of the presidential election since Russia meddled in the 2016 race by hacking Democratic Party emails and targeting election systems in all 50 states. The election isn’t only a political target for some attackers with nation state allegiance. They are also a potential tool for cybercriminals seeking profit because victims may be desperate to pay to ensure their systems are operational” (Mehrotra, 2020). This is an example of a cultural impact because this incident could show that the country is not strong enough to protect its information from other countries. It could create doubt in other countries and show that the US is not the leader of the free world as it claims it is. Countries could also not want to do business with the US in fear of the information being compromised by hackers.

**Global Considerations: Global Technology Environment**

The case relating to the Washington state social security agency hacking, there are regulations that are already in place but there are around ten methods of occurrence in espionage incidents. Global laws will have to change because the world is becoming a hub and it is giving cyber attackers freedom to create problems from anywhere at any given time According to the website weforum.org, it says “In little over a decade, cybercrime has moved from being a specialist and niche- crime type to one of the most significant strategic risks facing the world today. Nearly every technologically advanced state and emerging economy in the world has made it a priority to mitigate the impact of financially motivated cybercrime. There are three technologies that will very well define the next 10 years of global cyber security.

1. 5G networks and infrastructure convergence – by 2025, 75 billion new devices will be connecting to the internet every year, running critical applications and infrastructure at nearly 1000 times the speed of the current internet. This will provide architecture for connecting new industries geographies and communities, but it will hugely alter the threat landscape as it potentially moves cybercrime from being invisible, financially driven issue to one where real and serious physical damage will occur at a 5G pace. This is because there will be self-driving cars, automated water and waste systems that it will also have the capacity to thrust cybercrime into the real world at a scale and with consequences yet unknown.
2. Biometrics – To combat these emerging threats, biometrics is being widely introduced in different sectors and with various aims around the world, while at the same time raising significant challenges for the global security community. Biometrics and next generation authentication require high volumes of data about an individual, their activity and behavior. Voices, faces and slightest details of movement and behavioral traits will need to be stored globally, and this will drive cybercriminals to target and exploit a new generation of personal data. Exploitation will no longer be limited to theft of people’s credit card number but will target theft of their being” (Dixon, 2019). What this means is that crime will never stop but it will adapt. Even with steps the world will take in order to ensure security of information it creates a whole different problem of cybercrime. It will go from low-risk crime to complete persona theft and could lead from cyber-criminal activities to terrorist threats and attacks on individuals and organizations.

**Summary**

In the start of my paper, the main focus was on cybercrimes. Being able to look at the what the Washington state social security agency went through during a time of uncertainty due to COVID 19. It showed how government agencies will always keep problems in secret before telling the public what is going on with in the organization. The state’s social security agency works based on hierarchy, that means if the superior gets to make all the decisions within the organization even if subordinates have ideas on how to solve some problems. This shows it is very hard to run through ideas to leaders in a government-based organization compared to a private company. When it came to global considerations this was very tough. Due to the US being the center stage and leader of the free world, it just showed that there is still a lot of work that needs to be done in the country. No one country really has the answer when it comes to cybercrime but there is hope now that the world is becoming very global so a country like the US can use different sources to help protect its valuable information. On the flipside, it could become very problematic because hackers aren’t going to stop all of a sudden but will continue to learn different skills to gain information.

Reference:

Australian Cyber Security Center. (n.d.). The cyber security principles. Retrieved December 13, 2020, from https://www.cyber.gov.au/acsc/view-all-content/guidance/cyber-security-principles

Black, S., Gardner, D., Pierce, J., & Steers, R. (2019, February 27). The Organization's External Environment. Retrieved January 24, 2021, from https://opentextbc.ca/organizationalbehavioropenstax/chapter/thMaryville University. (2021, January 05). Ethical Issues Behind Cybersecurity. Retrieved January 24, 2021, from https://online.maryville.edu/blog/cyber-security-ethics/

Blake, A. (2019, May 01). How much does your state trust the government? See this map. Retrieved January 02, 2021, from https://www.washingtonpost.com/news/post-politics/wp/2014/04/04/how-much-does-your-state-trust-the-government-see-this-map/

Canada, C. (2021, January 18). Stop Overpaying. Start Switching. Retrieved January 24, 2021, from https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04569.html

Corte, R. (2013, May 09). Up to 160,000 Social Security numbers exposed in Washington state court hack. Retrieved January 02, 2021, from <https://www.nbcnews.com/tech/tech-news/160-000-social-security-numbers-exposed-washington-state-court-hack-flna1C9864740>

Cyber, B., & BlackPoint Cyber View all posts. (2019, February 11). 12 Cyber Security Principles from The Experts: Blackpoint Blog. Retrieved December 13, 2020, from https://blackpointcyber.com/blog/12-cyber-security-principles/

Deloitte US. (2018, March 28). Global cybersecurity compliance integrity: Deloitte US. Retrieved January 25, 2021, from https://www2.deloitte.com/us/en/pages/risk/articles/global-cybersecurity-compliance-integrity.html

Dixon, W. (2019, June 20). 3 technologies that could define the next decade of cybersecurity. Retrieved January 24, 2021, from https://www.weforum.org/agenda/2019/06/3-technologies-that-could-define-the-next-decade-of-cybersecurity/

Ferguson, B. (2020, October 28). Https://www.atg.wa.gov/news/news-releases/ag-report-washingtonians-affected-data-breaches-nearly-doubled-2020. Retrieved January 03, 2021, from https://www.atg.wa.gov/news/news-releases/ag-report-washingtonians-affected-data-breaches-nearly-doubled-2020

Florida Tech. (n.d.). Https://www.floridatechonline.com/blog/business/the-5-biggest-ethical-issues-facing-businesses/. Retrieved January 02, 2021, from https://www.floridatechonline.com/blog/business/the-5-biggest-ethical-issues-facing-businesses/

ISO/IEC 27032:2012. (2018, December 13). Retrieved January 24, 2021, from https://www.iso.org/standard/44375.html

Knowles, A., & Knowles, A. (2019, March 04). Tough Challenges in Cybersecurity Ethics. Retrieved January 24, 2021, from https://securityintelligence.com/tough-challenges-cybersecurity-ethics/

Leonhardt, M. (2020, June 22). Coronavirus scams have cost Americans $68 million so far-here are the states hit hardest. Retrieved January 03, 2021, from https://www.cnbc.com/2020/06/16/states-hit-hardest-by-coronavirus-scams.html

Maryville University. (2021, January 05). Ethical Issues Behind Cybersecurity. Retrieved January 24, 2021, from https://online.maryville.edu/blog/cyber-security-ethics/

Mehrotra, K. (2020, September 27). Hackers Have Infiltrated Many of Washington State's Agencies - BNN Bloomberg. Retrieved January 24, 2021, from https://www.bnnbloomberg.ca/hackers-have-infiltrated-many-of-washington-state-s-agencies-1.1500211

Newman, L. H. (2020, May 19). The Nigerian Fraudsters Ripping Off the Unemployment System. Retrieved December 13, 2020, from <https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/>

Resource Management Inc. (2020, June 25). Top Five Ethical Practices for Your Business. Retrieved January 24, 2021, from https://rmi-solutions.com/top-five-ethical-practices-for-your-business/

Segovia, A. (2015, August 25). ISO 27001 vs. ISO 27032 cybersecurity standard main differences. Retrieved January 24, 2021, from https://advisera.com/27001academy/blog/2015/08/25/iso-27001-vs-iso-27032-cybersecurity-standard/

Ssa, O. (n.d.). Https://www.ssa.gov/OP\_Home/cfr20/401/401-0045.htm. Retrieved January 02, 2021, from https://www.ssa.gov/OP\_Home/cfr20/401/401-0045.htm

Swinhoe, D. (2020, April 17). The 15 biggest data breaches of the 21st century. Retrieved January 03, 2021, from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html