How To Control Security Morale With Standards And Media

In the world of cybersecurity there is a very big problem when it comes to moral panic around users of technology. Within the recent years and even decades of this topic around technology, the problem has only gotten bigger when it comes to the general opinion of the way cybersecurity should be practiced to keep us safe. More recently there has been a rise of organized cybercrime which has grown the concern for the way we practice cybersecurity in our daily lives. One of the most popular tactics that these criminals use is “ransomware” which has caused quite the fear within people that aren’t confident in their own security knowledge. Ransomware is the act of locking someone's computer in exchange for currency being supplied in order for them to regain control of their system. With the losses many people and corporations have had there has been a widespread fear instilled across our nation without people checking on how they can prevent any of this from happening. The proper use and following framework can easily decrease the frequency of these attacks.

An example of this would be the Kaseya VSA ransomware attack which happened in the summer of 2021. The attack had begun from neglected security features in the system that was built for the program that housed a lot of data and functions for many corporations across the world. Russian state backed hacking group, REvil, was behind the attack which caused many diplomatic disagreements between the United States and Russia. One major setback from this attack was that Major Gas and Supermarket chains across Europe were shut down for a period of time during the summer which caused a widespread panic across those countries. After those systems were back up and running there were many questions to be answered after finding out

who was responsible for the attack on the cloud based company. Many were referring to if there were any other groups that the Russian government backed that could do this again. The newly formed question of whether the infrastructure in your own country is safe against the threat of hacking from a state sponsored cyber terror group became a hot topic in the United States. Some of the questions were answered in a Forbes article that was written by a well respected professional in the field named Ondrej Krehel. One of his quotes stating "In closing, ransomware attacks aren't going away. Hacker groups are getting more powerful with each attack, and without intervention from governments, it is impossible to stop them." Ondrej Krehel Ph.D, *The 2021 Kaseya Attack Highlighted The Seven Deadly Sins Of Future Ransomware Attacks.*

After researching this incident the main cause of it was the neglect of security standards and the implementation of framework. There are multiple frameworks for the space of cybersecurity to keep the industries safe while using their devices and networks. Frameworks are used to lay out some regulations, tips, and advice on how to run an efficient and sturdy security section of your company. There are many for the different industries that require either a certain or even more strict framework than others. For example the Payment Card Industry Data Security Standard has tried to increase and strengthen security of the payment world. This is a very important need for the society that we live in today being that every payment revolves around credit and debit cards now.

Being that most payments made in today's society are digital we need some security protocols for them. Identity theft and fraud have had a huge increase ever since the digital age of payment have come to our world. There had been over nine billion dollars of illegal purchases

made in 2018 alone. Credit card companies like Visa, Mastercard, American Express and others have been required to put out their own security programs to be able to operate in the world of digital payments.

There are six main objectives when it comes to the PCI DSS framework and they're also referred to as the control objectives. The first is Maintain and install a secure network requirement, which is basically stating that you need a safe network that can withstand some people trying to come in and steal your customers personal information and money by using a strong firewall system. You should also be using your own security procedures instead of the retailers. The second control objective would be Protect cardholder data. This one is quite self explanatory. You are protecting the cardholder's information like their name, address, social security number and many more sensitive areas that can be valuable for the wrong reasons. Also protecting a buyer's information while using the card while online by having that secure network that was talked about. The third control objective of this framework would be Maintain a vulnerability management program. This is basically stating that there needs to be some type of anti-virus put into place for these giant card companies in the world. A virus getting into one of these large card companies could be catastrophic for the world. As you go along this route of online and digital you need to make sure that what you have in place for it actually works. You need to engineer certain security aspects in your programs and maintain them along their lifespan. The fourth would be Implement strong access control measures. This restricts your card information from being let out into the wrong hands of the world. Your information is restricted to only what the retailer needs to know. Everyone has an identification tool assigned to them to make sure that it is them when they are using a computer to purchase something. There is also

the authority to freeze someone's card whenever there is suspicious activity suspected. The second to last control objective would be to regularly test and monitor networks. You need to make sure that all of your networks are safe from people trying to get into your cardholders information. By doing this you need to have a system that can record every single transaction made by the people that use your company's cards. You need to be able to see who has accessed your networks at all times to see if they are safe for anyone to use. The last part of this control objective would be to test and see if there are any vulnerabilities in your system that you have made for your customers. The last control objective would be to Maintain a security policy for all of your employers and cardholders to follow to ensure the safe use of your products.

With all of these regulations and procedures there are bound to be some pros and cons that come with this process. One of the first pros of the PCI DSS system would be that it does help prevent the act of credit fraud among the people that use cards for payment. All of the resources and standards given have made online and in store payments much more secure in the present day compared to back in the past. It gives new companies something to build off of when they want to start having people pay with cards. One of the biggest pros is that it makes sure that you are checking up on your infrastructure and know that there are no vulnerabilities in its system.

With most of the pros out of the way let's get to some of the cons about the framework. The systems being used will need to be checked at all times of the day which can be stressful to workers. This may be true but what has to be realized is that you have billions of people's personal information on the line and it is your job to make sure that information is safe. Another

con would be that it is a very complicated process. These large corporations that utilize card payment have troubles implementing these large security programs to all of their programs. With how large some of these corporations are, there are bound to be many vulnerabilities and missed clues that could've been used to help the corporation for its payment security.

The Payment Card Industry Data Security Standard Framework is a lot to take but it is worth trying and placing in your company. The industry for payment cards is a very large market and might one day be the only way we use money in the future.

The National Institute of Standards and Technology (NIST) is one of the main frameworks that we study about in our classes about cybersecurity. It is basically used as a base for learning updated security standards for any type of company that needs help on checking to see their status. There are many good things that can come out of reading and using the examples that are shown in this framework.

In this framework there are 5 main functions. Those functions are identify, protect, detect, respond, recover. Identification is the act of having a strong knowledge on everything that has to do with your job. Whether you're on the frontline acting against the attacks or if your back is trying to see how much damage would cost if an attack were to happen to your systems. Identifying is all about researching so that you can be ready for any event that can happen at any second of the day.

The second function of the framework would be to protect. This is knowing how to keep anything in your system secure. This is the main act of cyber security. We are here to protect these companies and peoples secrets locked up in a network safely. The act of protecting has many examples of doing it like monitoring a database for vulnerabilities, developing some security firmware in a new program that you have made, or installing a new firewall system into your computer's infrastructure. Without this step in the framework there would be no reason to even have cybersecurity in the world of networks.

The third function of the framework would be to detect. The act of detecting is finding any weaknesses of people trying to intrude your network. This is a very important part of the framework being that there are many different ways that people can get into a network. You should have people that are educated in sweeping a system for its vulnerabilities and knowing how to spot different types of attacks on a network. Without having these types of people on your team you can have a catastrophic data breach causing your customers and workers information to be in the hands of the wrong person.

The fourth function of the framework is to respond. The act of responding would be knowing what to do in the midst of a data breach of your company. During these times of data breaches you need to have a plan set within seconds after finding that your infrastructure has been compromised. The plan that has been brought into play needs to work for your problem and resolve the damage or stop them from stealing even more information than they already have

The last function of the framework is to recover. Recovering is very important after the end of a cyber attack. After an incident you may run into a lot of problems. Some of those problems could be having some of your infrastructure destroyed or getting your identity stolen or wiped. People that run the recovery section should be skilled in making back ups for your company and should also specialize in how to get the system back up and running.

The pros of this would be that it's a great start for any company that is new to the scene of online interaction. It is good to get as your first piece of information to keep you and your customers safe during these times of cyber attacks. It is also very easy to work off of when you need to refresh your memory on the subject. Some cons would be that it is too short and does not have enough knowledge to keep a company secure. You also have to branch out and find some other frameworks if you really want to keep your company secure since the information and resources are quite bare.

The second main focus on cybersecurity is keeping a focus on morale around being safe. In the world of cyber we have people that voice their opinions to give the world knowledge on how to be safe and secure. The topic of moral panic can be silenced with properly written articles spread to the community. Many articles and journals have been critiqued by the world of these professionals and that has only made us better when it comes to the way we look at cybersecurity. In the space of moral panic this can really help us when we need to calm down some of the people that feel threatened by these new tactics that people are using to hack into our computers or other devices. Unfortunately though during these times of crisis opposing professionals will issue out articles that can instill fear into the public which can cause this moral

panic to start across a community. Articles like these that gain popularity can be the reason why a country could go into chaos. Here is an example of a proper article that tells the truth without instilling fear. VB Staff , *Report: 60% of U.S. infosec professionals believe ransomware is as serious as terrorism* "According to a recent survey by Venafi, ransomware attacks spiked by 250% in the first half of 2021 alone. According to Cybersecurity Ventures, by the end of 2021, it's estimated that every 11 seconds, an organization will be hit with a ransomware attack. These rising threats led to almost two-thirds of security decision makers (60%) declaring that ransomware should be prioritized at the same level as terrorism, echoing the U.S. Department of Justice's assessment following the Colonial Pipeline attack earlier this year." This figure was an opinion from some of the top cyber professionals in the business which can give this article great credibility when it comes to talking about the problems in the world of technology.

With their being some articles that have made us think about the subject more and more has been great for the community with us becoming curious about the subject that is being argued about. This also does stir up some opinions that could be bad for the public to think about which can cause some moral panic. A great quote from an article can be a very helpful way to think about how cybersecurity should be thought about when it comes to fear. IEDP Editorial "*Cybersecurity: Vigilance or Panic?* "It is important to balance the level of cybersecurity required with the potential threat and not to be overly influenced by scare stories." This gives us hope that many writers are wanting to keep the overall morale towards cybersecurity

In the end we as a community have to be responsible for how we conduct ourselves when it comes to security. We need to ensure that our systems are properly secured with recommended

equipment and practices that have been approved by these frameworks. The spread of informative information rather than fear inducing must be written to give the world a better sense of how to be safe rather than to feel hopeless.

Editorial, IEDP. *Cybersecurity: Vigilance or Panic?*, IEDP , 21 Dec. 2016, https://www.iedp.com/articles/cybersecurity-vigilance-or-panic/.

Staff, VB. “Report: 60% of U.S. Infosec Professionals Believe Ransomware Is as Serious as Terrorism.” *VentureBeat*, VentureBeat, 1 Jan. 2022, https://venturebeat.com/2022/01/01/report-60-of-u-s-infosec-professionals-believe-ransomware-is-as-serious-as-terrorism/.

Krehel, Ondrej. “Council Post: The 2021 Kaseya Attack Highlighted the Seven Deadly Sins of Future Ransomware Attacks.” *Forbes*, Forbes Magazine, 27 Jan. 2022, https://www.forbes.com/sites/forbestechcouncil/2022/01/25/the2021-kaseyaattack-highlighted-the-seven-deadly-sins-of-future-ransomware-attacks/?sh=57dc2bcb5f75.

“Official PCI Security Standards Council Site.” *PCI Security Standards Council*, 1 Dec. 2023, www.pcisecuritystandards.org/.