Angela Castronuovo

**Cyber Security Issues of 2020**

As the NSCD is well aware, there have been numerous cyber-attacks in the United States this year. Because so many people have been affected by these malicious acts, this report will be advising you on the most important cyber-attacks in 2020, the most vulnerable industry currently, and recommendations for preventing these attacks from happening again.

After reviewing several attacks committed this year, we have come to the conclusion that the three most important cyber-attacks are the BioStar attack, Hospital Attacks, and the SmarTrack attack. The reason the BioStar attack is so important is if there was a vulnerability in this technology, it would do the most permanent damage since it deals with biometrics. This is because if the database of biometrics was hacked (luckily it was only hacked by white-hat hackers this time), then people’s fingerprints and even their faces can be stolen. It is impossible to change these features on the human body like we would change our passwords on an account that got hacked, so people might not ever be able to recover from this. Additionally, facial recognition technology is used in convicting criminals, so if an adversary were to alter or add biometric data to the database, it could lead to a wrongful conviction.

Hospital attacks are also important mainly because these instances highlight the issues the government has with trying to prevent attacks and punish attackers. From these attacks, it is clear that hackers don’t have any ethics since they’re willing to put so many lives at risk during a pandemic in order to extort hospitals. It shows that if this pandemic will not stop them, then laws certainly won’t scare attackers away. So, we are left with the dilemma of how to create laws that will stop attackers from attempting to hack into hospitals. This emphasizes the amount of work we have to do when it comes to stopping attacks. It is my belief that Hospitals are also the most vulnerable entity when it comes to cyber-attacks. One obvious reason for this is that due to COVID-19, hospitals are swamped with patients. Since so many lives are at risk and the encrypted information is critical to the well-being of many patients, the chances of a hospital paying the ransom is extremely likely. Besides hospitals being huge targets for ransomware in general, they are also vulnerable because most hospital software is outdated which could allow for easier access to files, and most hospital workers are not properly trained to look out for cyber threats.

The SmarTrack attack is also one of the most important attacks of 2020. This is because it is a great example of how companies can be so negligent that they put a product on the market that does not adhere to basic security measures. After the car theft technology, which is supposed to track and immobilize cars, was attacked by researchers, it was found that SmarTrack’s database was not secure against SQL injection because inputs were not being sanitized, SmarTrack technology was using HTTP instead of HTTPS for their GeoFence technology, and there was no authentication required before being able to immobilize cars. This is unacceptable and teaches us the valuable lesson of not releasing a product that isn’t ready and hasn’t thoroughly been checked.

It is in our best interest to take the following preventative measures. As there have been several ransomware attacks this year, backing up our data outside of the network would be a good measure to take. It wouldn’t necessarily prevent a ransomware attack, but it would lead to fewer ransomware attacks. If everyone were to back up their data, there would be no need to recover the encrypted files and pay the ransom, so the motivation for attackers to perform these ransomware attacks would decrease. Another measure we can take is a simple one: don’t be negligent when checking security of a product. Throughout this year numerous attacks could have been prevented if the company’s security team was a little more careful. For example, the Apple IOS attack was because a software developer left an unfinished piece of code in the final product. As discussed before, the SmarTrack company didn’t sanitize their database inputs. And finally, the previously mentioned BioStar Attack was due to lack of password hashing. If these basic security measures were taken, these attacks would not have happened.