Cyber Attacks

ANALYTICAL PAPER

Nathaly Flores | CYSE 200T | 06/13/2021

Cyber threats

Any nation's Critical Infrastructure provides services that support society and comfort everybody's way of life. It is the central part of the nation's security, economy, and health, especially the Electric grid. We must keep the electric grid update constantly with Cybersecurity. Electric Grid has evolved in so many ways that there's a constant threat.

The security and resilience of this critical infrastructure are vital for everyone and the nation's safety, wealth, and well-being. So, this Critical Infrastructure Security and Resilience defines the security which decreases the risk to critical infrastructure by security measures to virus attacks, the effects of the natural disasters, etc.

Phishing - this cyber threat is dangerous for the user who doesn't know about the cyberattacks or any form of hacking. This threat is probably hazardous for the parents because they are the ones who most click malicious links on social media. For example, in Facebook, the attacker will create a creative website that will inform you that you won in this kind of company. You need to sign up to claim your prize. The moment you enter your credentials, the attacker will save it and log on to it and change your password, they will they want in your account and some worse scenario they will sell your account in the black market that will cost 5 dollars it depends how much popular you are.

Insider Damage - This is probably the most dangerous one in terms of the company; this the cause of data breaching that most big companies are experiencing. Data breaching is the most complex Disaster attack in the company because many big companies don't resolve these attacks. Still, they pay for the media that don't broadcast it because it is a bit ashamed in the company.

FRAMEWORK

The framework provides a systematic methodology and common language for managing cybersecurity risk. The framework serves as a system of guidelines, standards, and best practices to manage risks in a digital world. A framework is a plan to complement, not replace, an organization's cybersecurity program and risk management process.

A cybersecurity framework repeatable, prioritize as a flexible and cost-effective approach to acquire the protection and resilience of the business. Creating Framework Profiles provides a firm with an opportunity to identify areas where an existing process may be build-up or where different methods can be employed.

The National Institute of Standards and Technology evolve the Framework for Protecting Critical Infrastructure Cybersecurity concerning an executive order from President Obama. The first report of what would be later called the NIST Cybersecurity Framework (CSF) was published in 2014. It becomes much easier to define the course and procedures that your firm must take to assess, monitor, and mitigate cybersecurity risk

with a structure in place. Examples of cybersecurity frameworks are NIST Cybersecurity Framework, SOC2, GDPR, HIPAA. It's important to realize that Cybersecurity helps with the growth of your business. Using a framework to align controls like local, offline, and cloud backups will improve resilience from any attack or reliance on hardware.

The five Framework Core activities of the NIST Cybersecurity Framework are:

1. Identify and manage cybersecurity risk to systems, assets, data, and capabilities. The company should identify and have complete visibility into your digital and physical support and their interconnections and their current risks, policies, and procedures to manage the risks.

2. Protect - Organizations should protect themselves by applying and implementing the appropriate safeguards to limit and control the impact of a potential cybersecurity issue. The company should control the access to digital and physical assets and educate the employees about these.

3. Detect - Organizations should apply and implement processes and procedures to identify cybersecurity issues and events and detect anomalous activity and other threats to business continuity and other issues.

4. Respond - In case of a cybersecurity incident, the organizations must have the ability to contain the impact, have a response plan, and be ready to collect and analyze information about the event, solving and getting on top of the even to control and eradicate the incident.

5. Recover - The organizations should have recovering capabilities when the capabilities or services were impaired due to a cybersecurity event. Thus, restoring the normalcy of the systems and the business, it is necessary to have a recovery plan, coordinate restoration activities, and update the strategy.

THE COLLISION OF SMALL BUSINESSES

Cybersecurity is something that could be used for small businesses and larger companies. As the internet industry grows more and more, there has been an increased demand for Cybersecurity. It is certainly something that has caught the attention of smaller-sized businesses. Their funds are more limited, so they have a limited amount of spending. There are easy ways for people to access credit card records due to less attention to Cybersecurity. Small businesses are more vulnerable to cybercrimes causing an increased risk of going out of business, so it is necessary to look at their priorities and their spending on Cybersecurity. They should hire employees and go over the basis for the security of an organization. Teach them basic practices and measures taken and ensure that they can be entrusted with the data given to them. Small businesses need to be more

informed about the consequences of cybercrime that has been performed against them. They should also spend some money on the latest software best suited to defend themselves from any cyber threats. Small businesses also need to make backup data if a cyberattack has been made to at least try to make up for the crime that has been made against them. They also need to use VPNs and Firewalls, which tend to be effective from any cyber-attacks. The Wi-Fi for a network should be heavily defended. They need to set up a wireless access point to make the grid visible or make it less visible.

Importance of cybersecurity

Cybersecurity is critical since it ensures all categories of information from burglary and harm. This includes touchy information, by and by identifiable data (PII), secured wellbeing data (PHI), individual data, mental property, knowledge, and administrative and industry data frameworks. Without a cybersecurity program, your organization cannot protect itself against data breach campaigns, making it a robust target for cybercriminals. Both characteristic and remaining hazards are expanding, driven by worldwide network and cloud administrations, like Amazon Web Administrations, to store delicate data and individual data. The broad destitute setup of cloud administrations matched with progressively modern cybercriminals implies the chance that your organization endures from a practical cyber assault or information breach is on the rise.

Cybersecurity's significance is on the rise. On a fundamental level, our society is more innovatively dependent than ever sometime recently, and there's no sign that this slant will moderate. Information spills that seem to result in being robbery are presently freely posted on social media accounts. Touchy data like social security numbers, credit card data, and bank account subtle details are currently being put away in cloud capacity administrations like Dropbox or Google Drive. The fact of the matter is whether you're a person, little commerce, or expansive multinational, you depend on computer frameworks each day. Match this with the rise in cloud administrations, destitute cloud benefit security, smartphones, and the Web of Things (IoT). We have a collection of cybersecurity threats that didn't exist a couple of decades prior. We have to contrast Cybersecurity and data security, even though the skillsets are getting to be more comparable.

Conclusion

The risk scene of the mechanical world has been quickly changing. It has grown challenging to keep up with the potential effect of dangers since of a few components. We will see the social meaning and impacts of cyber-related specialized frameworks because it relates to infrastructure, threats inside the work environment, and the advancement of cybersecurity programs. The problems, results, impediments, and improvements are tended to inside each subject. This article concludes by reflecting on the effects of specialized cyber frameworks and how to progress from the current environment.

The Social Meaning and Effect of Cyber security-related Specialized Systems As a society, we have ended up exceptionally subordinate to innovation as a portion of our lives. Organizations have turned to numerous digitalizing parts of their operations. As this happens, the social meaning and effect of specialized cybersecurity frameworks will alter alongside it, and not always in a positive way. There are numerous components of the framework which work in a way to protect us and our data. Looking at multiple issues and viewpoints has made a difference in the development of resolutions to assist in directing us in neutralizing cybercrime. Cyber-attacks have gotten to be as commonplace as the Web itself. Each year, industry reports, media outlets, and educational articles highlight this expanded predominance, spanning both the sum and assortment of assaults and cybercrimes. We look to advance further dialog on cyber dangers, cognitive vulnerabilities, and cyberpsychology through a total reflection on the social and mental angles related to cyber-attacks. Specifically, we are interested in understanding how individuals of the public perceive and lock with a chance; how they are affected amid and after a cyber-attack has happened. The influence of cyberspace on society is undeniable. It has given a platform for prompt communication, commerce, and interaction between individuals and organizations across the globe. As cyberspace has grown in influence, unfortunately, so too has the number and variety of cyber-attacks. Cyber-attacks are defined here as events that aim to compromise the integrity, confidentiality, or availability of a system.

Work Cited

Phishing.org "What is Phishing"? https://www.phishing.org/what-is-phishing#:~:text=Phishing%20is%20a%20cybercrime%20in,credit%20card%20details%2C%20and%20passwords. Access July 20, 2021

Insider Threat "What is an Insider Threat" https://www.imperva.com/learn/application-security/insider-threats/. Access July 20, 2021

Jonathan White NREL Transforming ENERGY "Cybersecurity for the Future Electric Grid" https://www.nrel.gov/grid/cybersecurity.html Access July 20, 2021