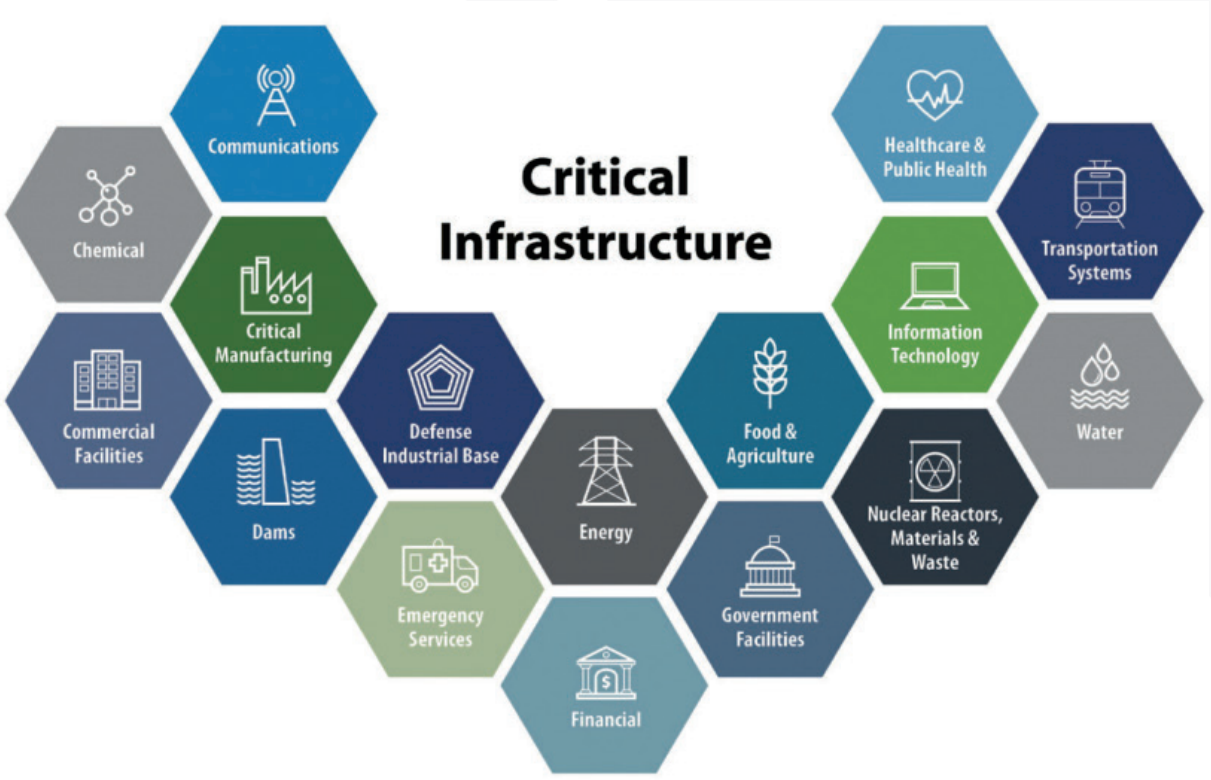
Octal0g1k
ANSWERING YOUR CYBER CHALLENGES

Cybersecurity: Critical Infrastructure Risks and Measures



Cybersecurity threats are exploiting the increased complexity and connectivity of critical infrastructure systems, placing every nation's digital advancements and connectivity at high risk. Every digitally connected nation state is investing and aware of its own security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a nation's economic bottom line. It can drive up costs, affect revenue and most important can render access to digital public goods useless. The need for comprehensive cybersecurity for critical infrastructure is clear. Public accounts are widespread concerning the risk of malicious actors targeting the electrical grid, dams, voting systems and other federally designated critical infrastructure globally both state sponsored and hackers. Some of the cyber attacks that made global headlines in 2020, were successfully targeted Honda and Taiwan's energy utility and a U.S. natural gas facility by ransomware attackers. Israel's water supply was reportedly attacked. The Japanese telecommunications firm NTT has had its internal network breached.

According to the United States (US) guide to the Critical Infrastructure Security and Resilience (CISA)[1], the definition of critical infrastructure is as: "Critical infrastructure includes the assets, systems, facilities, networks, and other elements that society relies upon to maintain national security, economic vitality, and public health and safety". It is thus important for every nation state to prioritize the allocation of available resources to that subset of infrastructure can enhance a nation's security, increase resiliency, and reduce risk and in – addition maintain the continued availability of identified essential services.

There are some lifeline functions that are associated and intertwined with each other corresponding to the functioning of all infrastructure in a country – transportation, water, energy, and communications, which means that their reliable operations are critical and a disruption or loss of one of these functions will directly affect the security and resilience of critical infrastructure within and across numerous sectors. For example, energy generating powerhouses provide essential

1 https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience- 110819-508v2.pdf

power to stakeholders in transportation, communications and water sector. Whereas the energy sector relies on transportation – to deliver fuel for power generation, water for production and cooling in electricity generation and communications – control and operations to maintain proper functioning.

Under the current situation where COVID19 has restricted the travel and movement of people and most of the work has become home based, there has also been a blossoming of attacks on organizations such as healthcare, energy, and education. The need at protecting the critical infrastructure has never been so urgent and it is important that public and private sector enterprises start to give top-priority to cyber generated threats. COVID19 has brought in the security of Cloud based infrastructure under the realm of critical infrastructure, as more and more services are becoming cloud based.

The COVID19 has presented new opportunities for cyber criminals and new avenues such as vaccine supply chains, home office workers with limited cyber awareness and use of IT systems, education sector and healthcare in general. As cloud spending rose during the pandemic, and Linux powering 90% of cloud workloads, attackers have invested heavily in open-source malware. Thus, the need for an optimized incident response in-case of a cyber breach on a critical infrastructure must be made the top priority for every organization. Early identification of cyber risks and minimizing disruption downtime of critical services remains the key to many towards securing critical infrastructure.

The need for continual cyber risk assessment and quantification of cyber risks is critical towards reducing cyberattacks. Cyber risk assessment must become a continued process with regards to an organizations digital inventory, upgrades and introduction of new digital rules and regulations. Continued emphasis on potential vulnerabilities within an organization must include cyber hygiene, confirmation protocols, keeping personal and professional data separate, adhering to cyber ethics guidelines, and confirmation before taking any unknown or suspected action, such as software and hardware upgrades. Auditing of cyber ethics, practices and system compliance must be taken – up regularly and metrics that weighs severity and ease of remediation should be devised to understand severity of an attack and its consequences.

The ability of a critical infrastructure to quantify its cyber risk and its ability to weigh the likelihood of a vulnerability impact and potential severity and addressing that loophole is the key for any cyber risk assessment. Critical infrastructure organizations should deploy ethical cyber hackers to showcase the gap between the organizations cyber risk priorities and what a hacker would term as a cyber attack priority. Thus, cyber risk priorities must be addressed from a cyber criminal's perspective rather than an organizations perspective. As the work from home scenario peaks-up, the vulnerabilities of protecting critical infrastructure have also multiplied. For example, employees are now using VPN to connect to production systems from home and make changes. In addition, some organizations are granting access to third parties to sensitive systems, as there is more focus on getting the job done, rather than cybersecurity. This complicates issues and brings in new bottlenecks.

The need to be cyber security for critical infrastructure shall grow exponentially, as more and more pubic good services take shape of a digital format. The growing number of cyberattacks on a year-on- year basis have multiplied exponentially, yet the need for cybersecurity priorities in some of the developing nation states remains relatively new. Most public sector entities are good at traditional risk management and physical safety initiatives, by cybersecurity assessment, action and compliance to global risk standards remain up to the mark compliance. For example, according to experts the operational technology security (OT) is about 10 years behind the IT security meanwhile the threat landscape of cyberattacks keeps growing. According to the X-Force Threat Intelligence

Index 2020 from IBM, the volume of attacks on industrial control systems in 2019 was higher than the previous three years combined[2].

Critical infrastructure must integrate in creating a comprehensive cyber security policy and practices for their assets which include equipment and devices, network and users, data, workflow and processes, software development processes. Threat detection, response and recovery must be prioritized. Given the complexity of examining risk in critical infrastructure environments, response and recovery must be given a front seat. Identification and removal of cyberthreat quickly is the key and investing in securing strategic assets is important. Proactive cyber security postures involve compliance to ISO 27002 and similar frameworks such as ISA/IEC 62443. The US department of defense has come out with Cybersecurity Maturity Model Certification (CMMC)[3], provides a basic guide for good cyber-hygiene, cybersecurity management and review of cybersecurity activities for effective measurement and standards that add to documentation and relevant units.

Critical infrastructure security risks and threats are shifting rapidly, and becoming proactive requires constantly assessing ones cyber-posture and address what's happening both globally and within a nation state that directly or indirectly impacts the availability of critical infrastructure services and securing and integrating best practices on a continuous basis.

2 https://www.ibm.com/security/data-breach/threat-intelligence

3 https://www.acq.osd.mil/cmmc/