ADMM Cybersecurity and Information Centre of Excellence

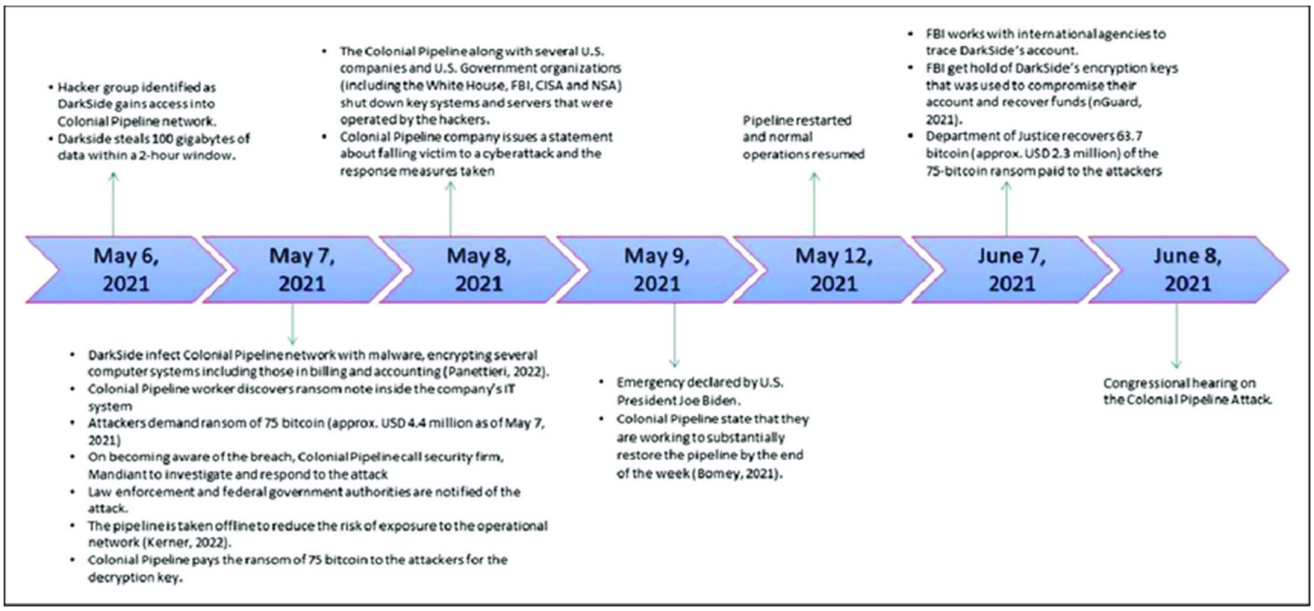
UPDATE ON THE CYBER DOMAIN

Issue 3/24 (March)

Securing Critical Infrastructures from Cyber Attacks – Why it Matters

INTRODUCTION

1. In May 2021, the US' Colonial Pipeline – one of the largest oil pipelines that supplied 45% of the oil and gas used on the east coast of the US – was the victim of a ransomware attack. While Colonial Pipeline's operational network was unaffected, the pipeline remained shut for several days as a precautionary measure to prevent the cyberattack from spreading. This attack was the largest publicly disclosed cyberattack against critical infrastructures in the US. The attack led to shortages of gasoline, diesel, and jet fuel; triggering price increases throughout the US. Panic buying became rampant as consumers feared that gas would run out. In Virginia, North Carolina, Georgia, and Florida, where the Colonial Pipeline was the primary fuel source for many retailers, the respective governors invoke emergency measures to ensure adequate fuel supply. Such measures included putting the Florida National Guard on standby, and issuing fuel transportation waivers to allow fuel to be transported from the ports to cities by alternative means, such as by train or ship.

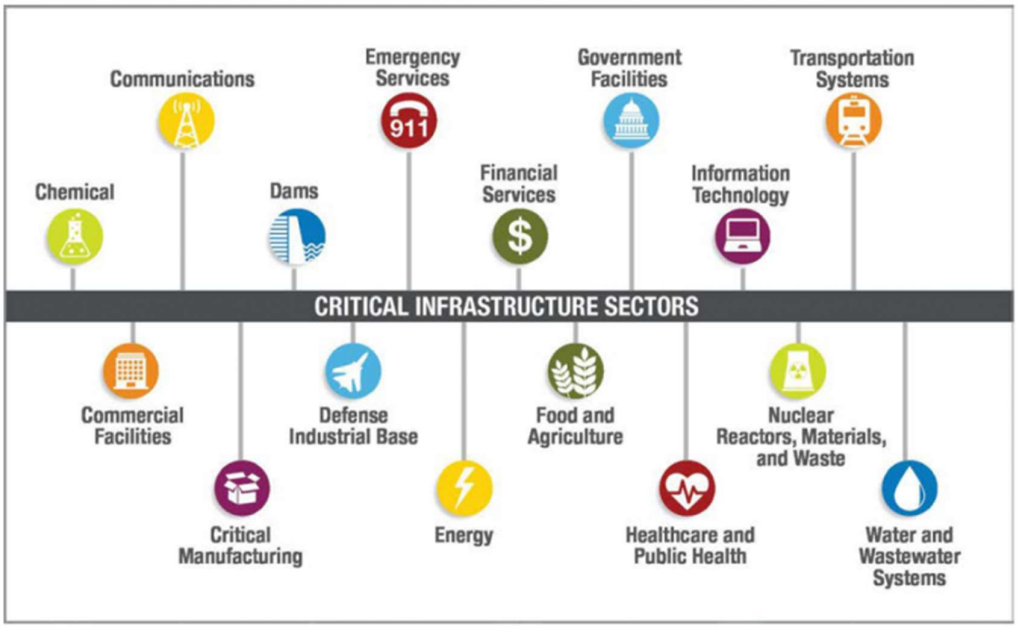


Timeline of Colonial Pipeline Attack (Source: Namita et al.)

2. The success of the Colonial Pipeline ransomware attack highlights how cyber-attacks can be used to target the computer components within critical infrastructures, leading to considerable and severe disruption to physical systems and processes. The frequency of such attacks on critical infrastructures is also increasing. *Security Intelligence* reported a 140% increase in high-impact attacks on critical infrastructures across the world from 2022 to 2023. This month's report will shine a spotlight on cyber-attacks targeting critical infrastructure and highlight best practices for the private and public sector to guard against such cyber-attacks.

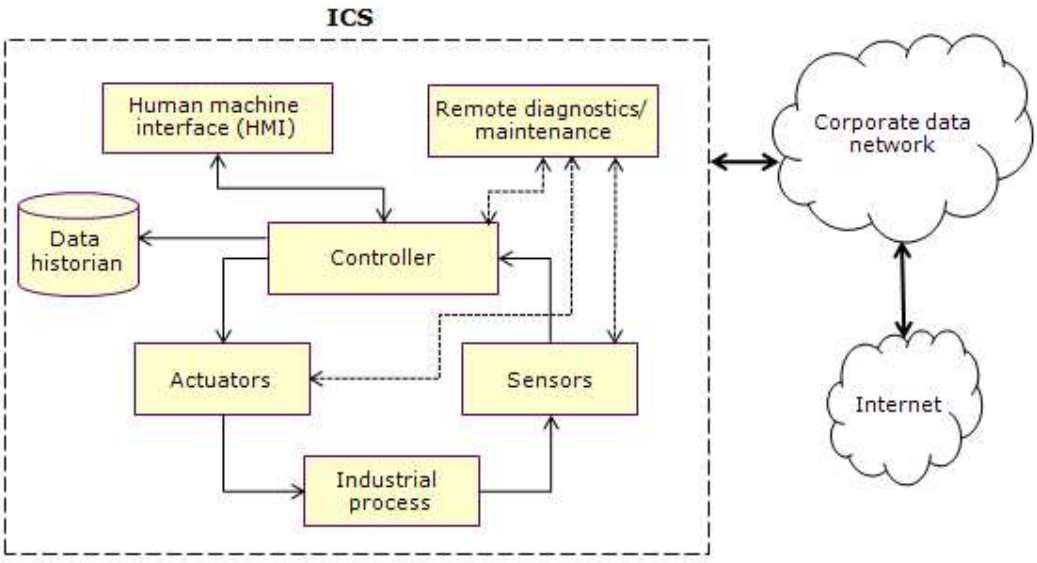
DEFINING CRITICAL INFRASTRUCTURES

3. Critical infrastructures are the backbone of modern societies; they encompass vital systems and assets such as energy grids, water supply networks, transportation systems, and telecommunication networks. These systems are highly interdependent, with the disruption of any one industry potentially having a rapid and escalating effect on society. One example is the 2011 Florida City water treatment plant incident, where a hacker gained access to the plant controls and significantly increased the water supply's levels of sodium hydroxide. At low levels, the corrosive chemical helps to regulate the PH level of potable water; but at high levels, it severely damages any human tissue it touches. Although the intrusion was intercepted and the crisis averted, this shows how cyber-attacks can have a devastating impact on critical infrastructures that provide to our basic daily needs.



Critical Infrastructure Sectors (Source: Peter.eu)

4. Modern critical infrastructures also encompass interconnected digital systems that enable their operation, automation, and management. These systems, also known as Industrial Control Systems (ICS), play a central role in allowing companies and governments to remotely control and monitor the physical processes of critical infrastructures. As such, cyberattacks on ICS can result in critical infrastructures being physically damaged, with their failure consequently compromising national security and public safety.



Typical Components of ICS Architecture (Source: Citicus)

VULNERABILITY OF ICS TO CYBERATTACKS

5. In recent years, cyber-attacks on critical infrastructures have targeted ICS. Historically, ICS were protected at the network level using air-gapping (with the network physically isolated from other networks) and proprietary protocols, making it difficult for external actors to gain access. However, the use of communication protocols linked to the internet (e.g., TCP/IP networks) now expose ICS to cyberattacks.

6. ICS presents an attractive target for hackers due to their age. The control mechanisms were installed over two decades ago and their security measures have become outdated. Additionally, it is challenging to undertake security patch management as changes needed to be kept to a minimum to avoid the risk of disruption to the critical infrastructures through unexpected side effects of the update. As such, ICS often lack robust security features (e.g., two-factor authentication, advanced firewalls), which makes them vulnerable to modern cyberattacks.

7. The use of cyberattacks to disrupt ICS and critical infrastructures is a global phenomenon. In 2016, the CrashOverride malware was used for a cyberattack on Ukraine's electrical grids, resulting in a partial power outage in Kiev. Investigations later revealed that the malware exploited the vulnerabilities in outdated industrial communication protocols (which connect the systems, interfaces, and instruments within an ICS on the internet) to switch off the flow of power. With similar decades-old protocols being utilised globally, researchers from cybersecurity firms ESET and Dragos Inc. warn that the malware may be able to automate mass power outages and cause physical destruction to power grids around the world. More recently, a 2021 attack on the Oldsmar Water Treatment facility was carried out using vulnerable WordPress plugins. The attacker exploited an outdated Windows 7 OS (which no longer had security updates) and the lack of a firewall to remotely access the system, and subsequently attempted to poison the water supply by increasing the level of sodium hydroxide in the water.

THE USE OF SOCIAL ENGINEERING IN ICS ATTACKS

8. As technical security strategies improve, social engineering is being increasingly used to get an initial foothold into targeted ICS. In 2023, Ukraine's Computer Engineering Response Team reported that hackers had targeted a critical energy infrastructure facility with phishing emails containing a malicious script. The email included three images and the following message: *"Hi! I talked to three girls, and they agreed. Their photos are in the archive; I suggest checking them out on the website."* However, the images and the archive contained a file in BAT format – a script used in Windows to automate tasks. When the victim ran the file, it opened a few innocent webpages, but also executed a harmful script in the background, leading to cyberespionage and potential disruption to the critical infrastructure.

9. This incident highlights that human errors can lead to costly mistakes if critical infrastructures are compromised. Humans, with their vulnerability to manipulation and exploitation, expose critical infrastructures to cyberattacks enabled by social engineering. It is critical to implement adequate security measures, policies, and procedures to mitigate and minimise threats arising from social engineering.

RECOMMENDATIONS

Private-Public Cooperation in Critical Infrastructures Cybersecurity Governance

10. Nations and organisations alike are dependent on a variety of privately-owned and operated critical infrastructures to support their growth and functioning. Any attack designed by advanced actors can damage or disrupt critical infrastructures that deliver vital services – such as telecommunications, electricity and water, and financial services – presenting a significant national security challenge. Hence, partnerships between the public and private sector stakeholders are vital for enhancing security, information assurance and cyber defence efforts across critical infrastructure domains. In the US, ongoing public-private information sharing to support critical infrastructure security and resilience is coordinated by the Cybersecurity and Infrastructure Security Agency (CISA). CISA organises awareness and outreach campaigns such as the annual Cybersecurity Awareness Month and broader national awareness programmes that offer partner toolkits and support the sharing of information between the public and private sectors.

11. As the threats faced by critical infrastructures are not constrained by geographic boundaries, CISA also fosters relationships with international partners like the European Union Agency for Cybersecurity (ENISA) to promote collaborative information sharing and partnership models across the globe. Agencies responsible for protecting critical infrastructures within ASEAN could consider similar partnerships, as a means to share best practices amongst like-minded partners in the wake of common cyber challenges.

Social Engineering Awareness Training

12. Organisations should also actively educate their personnel on threat tactics, to empower them to recognise and thwart malicious social engineering attempts. Training can be implemented in various forms – posters, training videos, or a face-to-face training module. Such training instills vigilance and enable employees to identify phishing emails and other deceptive techniques. Following the training, organisations may consider conducting simulated phishing campaigns to ascertain user behaviour, to get a readback on the effectiveness of training throughout their organisation. Through regular training and exercises, employees hone their ability to discern legitimate communications, reducing the risk of falling victim to social engineering ploys and bolstering overall resilience.

CONCLUSION

13. As the management of critical infrastructures becomes increasingly dependent on a network of connected devices, the failure of a single point could result in a devastating chain reaction. It is therefore in the public and private sectors' interest to bolster the cybersecurity in critical infrastructures, so as to protect critical assets in an increasingly volatile threat environment.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

References

1. Colonial Pipeline Ransomware Attack: How to Reduce Risk in OT Environments [https://www.tenable.com/blog/colonial-pipeline-ransomware-attack-how-to-reduce-risk-in-ot-environments]

2. High-Impact Attacks on Critical Infrastructure Climb 140% [https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/]

3. Characteristics of Industrial Control Systems [https://www.citicus.com/Characteristics-of-Industrial-Control-Systems]

4. Hacker Tried to Poison a Florida City's Water Supply, Officials Say [https://www.wired.com/story/oldsmar-florida-water-utility-hack/]

5. Ukraine says an Energy Facility Disrupted a Fancy Bear Intrusion [https://therecord.media/ukraine-energy-facility-cyberattack-fancy-bear-email]

6. Securing Your Critical Infrastructure [https://www.distology.com/news-events/securing-your-critical-infrastructure/]

7. Partnerships and Collaboration – CISA [https://www.cisa.gov/topics/partnerships-and-collaboration]

8. How to Implement Social Engineering Awareness Training [https://purplesec.us/learn/security-awareness-training/#Training]