International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

# Protecting Critical Infrastructure from Cyber Attacks: A Multifaceted Approach

**[1] Avinash Gupta Desetty, [2]Srinivas Reddy Pulyala, [3] Vinay Dutt Jangampet**
[1]Senior Splunk Engineer, Sony Corporation of America, gupta.splunker@gmail.com,
[2]Cybersecurity Architect, Smile Direct Club, srinivassplunk@gmail.com,
[3]Staff App-ops Engineer, Intuit, Dallas, USA, yanivdutt@gmail.com

**Abstract**
**As the rate of cyberattacks increases year-over-year, safeguarding critical infrastructure against these threats is becoming more crucial than ever before. Recent attacks on oil pipeline infrastructure, hospitals, and government websites demonstrate the vulnerability and widespread impact of such attacks. Attackers use methods such as phishing, zero-day exploits, brute force attacks, DDoS, and malware intrusions. These attacks have resulted in loss of lives and detrimental effects on economies and national security. This paper presents a comprehensive approach to protecting infrastructure against cyber threats. The research will commence with an analysis of the literature about past incidents and response strategies. Drawing from existing research, this paper will then propose a defense approach capable of mitigating these ever-evolving threats.**

**Keywords: Critical Infrastructure, Cyber Attacks, Multifaceted Approach, Threat Landscape, Vulnerabilities, and Threats**

## Introduction:

In an era defined by rapid technological advancement, vulnerabilities within critical infrastructure networks have become a significant concern, frequently making headlines due to escalating cyber threats. In recent years, the have been multiple cyberattacks targeting critical infrastructure in various countries, including the US, Israel, and Ukraine. One notable instance was the ransomware attack on the Colonial Oil Pipeline in 2021, executed by the cybercriminal group DarkSide [1]. This attack disrupted the flow of over 2.5 million barrels of oil products, sending shockwaves through both the energy sector and public consciousness.

These attacks serve as stark reminders of the vulnerabilities present within critical infrastructure networks, demanding attention from relevant stakeholders. The impact of such attacks is keenly felt by millions who rely on this infrastructure for their livelihoods or daily operations. The potential threat's magnitude is staggering, occasionally resulting in fatalities, particularly when targeting health facilities [2].

Despite these challenging prospects, critical infrastructure providers have an opportunity to take ownership of the solution. Understanding emerging cybersecurity threats and responding proactively is crucial in preventing or mitigating the impact of such attacks. Addressing these challenges requires implementing a cybersecurity approach that

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

integrates multiple layers of defense and diverse methodologies.

This paper aims to explore a comprehensive path toward protection and resilience by conducting a thorough analysis of past incidents, understanding the evolving threat landscape, and advocating proactive measures. Additionally, details of simulated cyberattacks will be included to demonstrate their potential impact and highlight how critical infrastructure providers should have responded to them.

## Background

### History of cyberattacks on Critical infrastructure

The landscape of cybercrime traces back to the early days of computer networks, where ransomware attacks emerged as early as the 1980s [3]. However, the increased adoption of digital solutions in control systems within Critical Infrastructure (CI) has amplified vulnerabilities within these essential systems. This has led to an increased number of cyberattacks on CI in the last two decades.

#### *Early Instances*

Among the earliest recorded cyberattacks on critical infrastructure, the Moroochy Water Breach in March 2000 stands out as a notable incident [4]. With this attack, a hacker gained unauthorized access to the Supervisory Control and Data Acquisition (SCADA) system of a wastewater treatment plant in Maroochy Shire, Australia. The breach resulted in the uncontrolled release of over 800,000 liters of untreated sewage into local waterways, showing the potential havoc cyber threats can have on vital infrastructure.

The other notable attacks were executed on multiple critical infrastructures in Estonia Attacks in April and May of 2007 [5]. During this period, Estonia experienced a coordinated cyber-attack targeting numerous crucial sectors, including government portals, ministries, Internet Service Providers (ISPs), financial institutions, and businesses. These attacks, predominantly executed through Distributed Denial of Service (DDoS) tactics, coincided with civil unrest following the Estonian government's decision to relocate the 'Bronze Soldier Memorial' in Tallinn.

### Why attackers target critical infrastructure

Attackers target critical infrastructure for various reasons. Primarily, these attacks are driven by the potential for significant financial gain through disrupting essential services. A recent report by IBM shows that the average data breach costs for $5 million, 12% more than data breaches in other sectors [6]. Attacks on CI have also been also accelerated by the convergence of digital technology with analog systems, creating vulnerabilities that can be exploited. Unfortunately, many operators of critical infrastructure continue to use legacy software and outdated operating systems like Windows 7 or even worse, Windows XP. These legacy systems pose substantial security risks due to their vulnerability to well-known security loopholes that are no longer patched, making them attractive targets for cyber attackers seeking to exploit these weaknesses.

### Methods of execution

Cyberattacks on critical infrastructure typically exploit inherent vulnerabilities within systems such as Supervisory Control and Data Acquisition (SCADA). Attackers employ diverse methods, including the exploitation of system weaknesses and the utilization of social engineering or phishing attacks to gain unauthorized access [4]. Subsequently, upon gaining access, attackers deploy malware to infiltrate and manipulate

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

systems, exploiting known software or hardware vulnerabilities.

Cybercriminals also execute ransomware attacks, which involve encrypting crucial files and demanding a fee for the decryption key [1]. Apart from malware attacks, attackers also execute Distributed Denial of Service (DDoS) attacks, flooding systems with overwhelming traffic they cannot manage [7]. These DDoS attacks are directed at websites or vital platforms of critical infrastructure service providers. The most dangerous bit about DDoS attacks is that the executors don't need to gain internal access to the system.

Impact of Cyberattacks on Critical Infrastructure

Cyberattacks targeting critical infrastructure have far-reaching consequences that are beyond mere system disruptions. These attacks can result in the loss of lives, as evidenced by incidents that target hospitals [3]. These attacks also trigger substantial economic ramifications, potentially causing billions of dollars in losses, especially those targeting financial institutions. Additionally, these attacks significantly impact national security, often leading to social unrest among affected citizens [8].

In light of these grave consequences, fortifying defense systems within critical infrastructure emerges as a crucial concern. Proactive measures, including the integration of cutting-edge technologies like AI into cybersecurity, must be implemented to preemptively prevent and mitigate cyber threats before their occurrence.

Literature Review

Several studies have examined the common threats targeting critical infrastructure and the strategies that providers and other relevant players can employ to address these attacks. In Stoddart and Kristan's research (UK cyber security and critical national infrastructure protection), they identified several common attacks on CI [9]. Their analysis highlighted a broad spectrum of attackers, ranging from novices to highly skilled hackers and state-sponsored groups. They pinpointed vulnerabilities in Computer-Controlled Critical National Infrastructure (CNI) systems as the primary cause of these attacks. Stoddart and Kristan advocate for a multifaceted approach to combatting these attacks, including Enhanced Cyber Resilience, collaboration, Information Sharing between industries, and Regulation and Oversight.

In Jamal Henry's research (Reducing the Threat of State-to-State Cyber Attack against Critical Infrastructure through International Norms and Agreements), critical systems are defined as infrastructure vital to national security, public health, the economy, and safety [10]. The research highlights the susceptibility of industries like energy, telecommunications, and water sectors due to reliance on computer-based control systems. Potential attackers highlighted in this research include computer criminals, terrorists, and state actors, each motivated differently and posing various levels of risk. State actors, particularly, are identified as the most capable due to their access to massive resources and talent. The research also highlights the common causes and methods used in these attacks, including human errors, phishing attacks, and network enumeration to gain access to critical systems.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Given the evolving nature of the cybersecurity landscape and technology, more research is needed, especially in this era of new technologies like generative AI, where attackers have the tools needed to create more sophisticated attacks targeting critical infrastructure. This paper will delve into the common cyber-attacks targeting critical infrastructure and how service providers can proactively prepare to deal with these attacks.

Protecting Critical Infrastructure from Cyber Attacks

To protect CI from cyber-attacks, there is a need to first understand the common attacks that target these industries. These are some of the common attacks that target the critical infrastructure.

Phishing and Spear Phishing

Phishing is a tactic where cybercriminals send deceptive emails, usually appearing as if they're from a trusted source within a company with the aim to trick employees into sharing sensitive information or downloading malware disguised as legitimate files [11]. Spear phishing is a more targeted version, involving extensive research on a company and its employees, making the emails even more convincing.

In 2016, there was a power cut in Western Ukraine that was caused by a spear-phishing attack according to the US Department of Homeland Security (DHS). This attack affected over 80,000 people in Western Ukraine.

Zero-Day Attacks

Zero-day attacks occur when hackers exploit a known weakness in software, hardware, or networks before it is fixed. Even after a fix is released, hackers might continue exploiting the vulnerability since many users don't install patches immediately. The SolarWinds supply chain attack is one of the popular examples of a zero-day attack [13]. An organized cybercrime group exploited a vulnerability that was unknown at the time. This breach compromised various US government agencies and several Fortune 500 companies.

Brute Force Attacks and Password Spraying

Brute force attacks involve trying numerous simple phrases and common passwords in attempts to access a single company account. On the other hand, password spraying involves using a small number of common passwords across multiple accounts, hoping to find at least one vulnerable account. With the increased accessibility to AI, attackers today can use emerging AI tools like PassGAN to crack the most common or leaked passwords with unprecedented ease [14].

A popular brute force attack was executed by The Russian group APT28, also known as "Fancy Bear," which employed password spraying in attacks targeting U.S. entities [15]. Their strategy involved trying a limited set of common passwords across numerous accounts, aiming to exploit any vulnerable accounts with weak passwords.

Malware Attack

Malware refers to malicious software designed to infiltrate systems, enabling activities like spying on communications, data theft, data destruction, or file encryption. It can infiltrate devices through various means, often arriving via methods like phishing emails. Ransomware is a type of malware particularly concerning critical infrastructure. Once in a

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

system, it encrypts useful data, effectively blocking access to files and potentially crippling operations. Hackers then demand a ransom to decrypt the files, but even if paid, there's no guarantee they'll restore access or refrain from causing further damage.

The WannaCry ransomware attack in 2017 is a notable example [16]. This attack infected 1,200 diagnostic devices and forced several United Kingdom hospital emergency departments to close temporarily. This attack showed the devastating impact ransomware can have on critical systems, disrupting essential services and endangering public health by forcing hospitals to divert patients to other facilities.

DoS/DDoS Attack

Distributed Denial-of-service (DDoS) attacks flood a network or device with overwhelming traffic, causing the system to crash or become unresponsive to legitimate user traffic. Unlike other cybercrimes, DoS attacks don't aim to breach the system but rather to render it inoperable for a given period. These attacks can be orchestrated by hacktivists or foreign governments with motives beyond financial gain.

A notable example of a massive DDoS attack occurred on October 21, 2016, targeting Dyn, a major domain name service provider [7]. The attack flooded Dyn's servers with one terabit per second of traffic, setting a new record for DDoS attacks at the time. This attack rendered several high-profile websites, including GitHub, HBO, Twitter, Reddit, PayPal, Netflix, and Airbnb, inaccessible.

*DoS Attack Simulation*

The Internet Control Message Protocol (ICMP) flood DDoS attack on the target organization's network attack was simulated using these steps;

Step 1: Setting up a virtual environment

EVE NG emulation software was used to create the virtual lab that included the network router, our Karli Linux machine, and network gateway as illustrated in Figure 1.

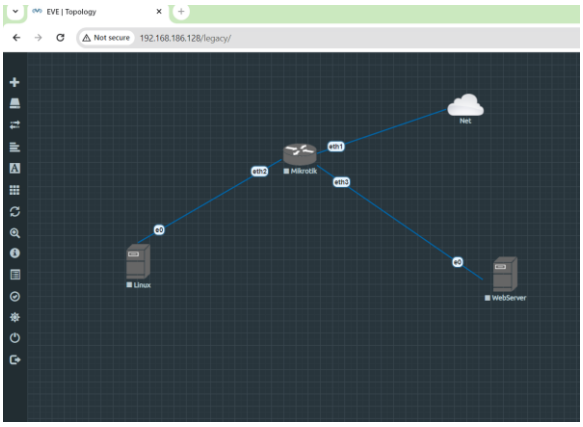


*Figure 1 Virtual Lab*

Step 2: Tracking traffic before the attack

Wireshark was used to track the traffic inflow for the target network before the attack was simulated. As shown in Figure 2, traffic inflow on the network was normal, with roughly one request per two seconds.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362

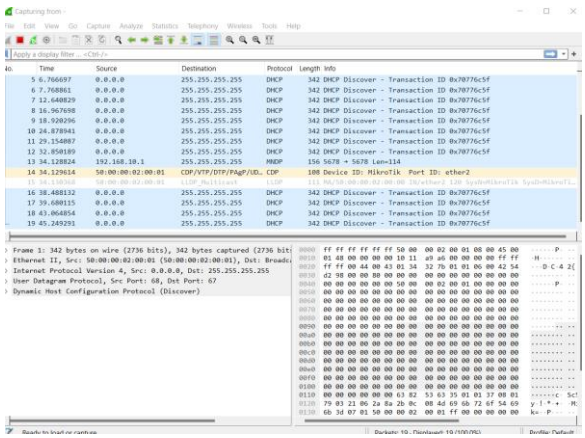

*Figure 2 Normal Traffic inflow before the attack*

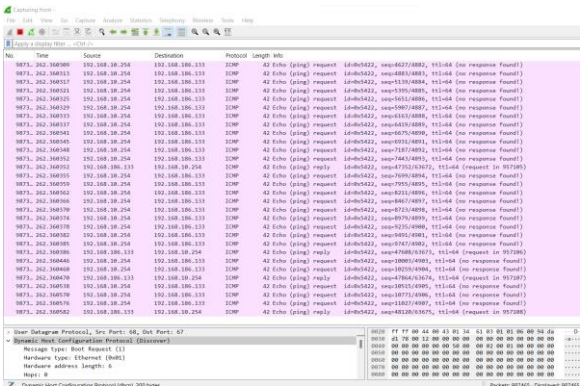

*Figure 4 Massive traffic flow during the attack*

Step 3: Executing the attack

The attack was executed using Terminal (in Karli Linux virtual machine) using the **hping3 -1 —flood -1 192.168.186.133** command, where 192.168.186.133 is the IP address of the target router as shown in Figure 3. With this attack, over 1500 packets per second were sent to the network.

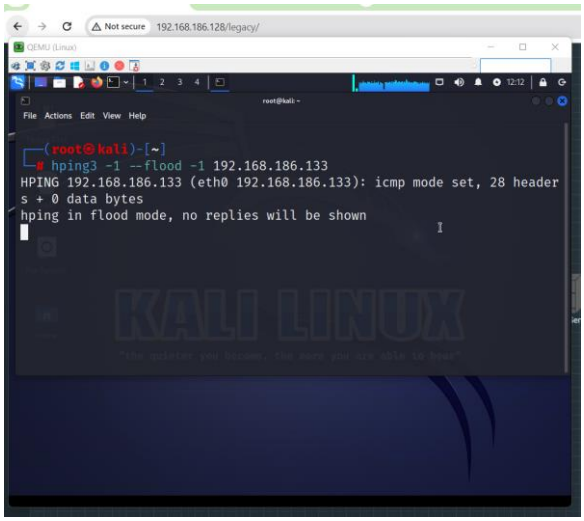


*Figure 3 Executing ICMP attack in Karli Linux*

Step 4: Tracking traffic during the attack

While the attack was being executed, Wireshark was used to monitor traffic inflow on the target network. As shown in Figure 4, thousands of ICMP packets were being sent to the network per second to overwhelm.

Proactively Preventing Cyberattacks on Critical Infrastructure

1. Foster a culture of cybersecurity

Creating a culture that prioritizes cybersecurity involves training all employees, not just the IT team, on common cyber threats and vulnerabilities [17]. This includes educating them about phishing attempts, zero-day attacks, and the risks of weak passwords. Incident response plans should be developed, and knowledge about cybersecurity trends should be disseminated across the organization. Collaboration between cybersecurity experts and other teams such as marketing can help in fostering this culture.

2. Using anti-malware tools

Anti-malware software is designed to detect, prevent, and remove malicious software, such as viruses, worms, and ransomware. For instance, the NotPetya ransomware attack in 2017 affected numerous organizations globally, including Maersk, causing significant disruptions [18]. Anti-malware tools could have potentially identified and blocked the malware before it caused widespread damage.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

3. Securing Networks

Protecting networks from attackers can be done in several ways:

- **Firewalls:** Firewalls act as a barrier between internal networks and external threats by examining incoming and outgoing traffic based on predetermined security rules. For instance, in 2013, the Target data breach occurred due to the compromised credentials of an HVAC vendor [19]. A stronger firewall configuration might have prevented unauthorized access to Target's internal systems.
- **Trust Zones:** Segmented networks or trust zones within an organization's internal infrastructure provide additional layers of security. They help protect sensitive data or critical systems. Had Sony implemented better-segmented networks in 2014, the breach that exposed sensitive employee data might have been contained within specific zones, limiting its impact.
- **Using SIEM tools:** SIEM solutions collect and analyze data from various sources within a network. For example, if we consider the popular Equifax data breach in 2017, a robust SIEM system could have identified suspicious activities, such as unauthorized access to sensitive data, allowing for early intervention to prevent the breach [20].

4. Data Encryption and Multifactor Authentication

Encrypting data at rest and in transit safeguards information from unauthorized access. Data breaches like the one on Anthem in 2015 can be minimized or eliminated by encrypting the stored personal information. Additionally, requiring multiple forms of verification, like a password along with a unique code sent to a user's phone, enhances security. Attacks like the Dropbox branch in 2012, might have been prevented if MFA techniques were implemented [21].

5. Implementing a clear Communication hierarchy

In large organizations managing critical infrastructure, information silos can develop, hindering effective communication and collaboration between different teams and sites. This lack of communication can lead to cyber vulnerabilities. For instance, in the Equifax breach, poor communication about an identified vulnerability in their system led to the exploitation of sensitive customer data. Clear communication and defined leadership roles are crucial in ensuring everyone is aware of potential risks and how to address them.

6. Regular Security Audits

Conducting regular security audits across all devices, networks, and components is essential. Many cyberattacks exploit overlooked vulnerabilities in various devices and networks. Regular security audits are vital for protecting critical data, enhancing security policies, monitoring employee adherence to protocols, evaluating strategy effectiveness, and detecting emerging vulnerabilities. These audits act as a shield, safeguarding sensitive information, shaping adaptable security policies, reinforcing good practices among employees, assessing the success of security strategies, and preemptively identifying potential weaknesses. Experts recommend doing security audits at least once or twice a year [22].

7. Defense in Depth

This strategy involves deploying multiple layers of security controls (technical, procedural, and human) to fortify critical

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

infrastructure [23]. No single security measure can guarantee protection against sophisticated cyber threats. The principle is akin to having a backup plan if one security control fails. For instance, safeguarding a power grid system may require implementing several security layers, including physical security measures like fencing and access controls, network segmentation to isolate critical systems, protecting networks using firewalls and intrusion detection systems, regular vulnerability management, and well-defined incident response procedures.

8. Framework Compliance

Frameworks like NIST, Essential 8, AESCSF, and ISO 27001 provide essential security controls [24]. However, these frameworks should be seen as foundational controls rather than exhaustive. They set a minimum standard but may not cover all emerging threat vectors. Organizations should consider these frameworks as a starting point rather than a comprehensive solution when implementing their multi-face security strategy.

## Conclusion

Securing critical infrastructure from cyber threats necessitates a multifaceted approach integrating multiple defense layers across physical, network, and digital domains. The rising frequency and severity of cyberattacks on crucial infrastructure highlight the urgent need for proactive measures and a comprehensive cybersecurity framework. Previous incidents like the Colonial Oil Pipeline ransomware attack underscore the immense impact cyber threats can have on vital services and societal welfare.

To combat these threats, organizations must instill a cybersecurity culture among employees, implement robust anti-malware tools, secure networks through firewalls and segmentation, employ encryption and multifactor authentication, establish clear communication hierarchies, conduct regular security audits, utilize defense-in-depth strategies, and ensure compliance with foundational security frameworks. This comprehensive approach provides resilient defense against evolving cyber threats, essential for mitigating potential vulnerabilities in critical infrastructure networks.

As technology advances, organizations must remain updated about cyber threats facilitated by these advancements. For example, the expanded accessibility of AI is being exploited by attackers to create more sophisticated threats. Staying ahead in leveraging such technologies and employing sophisticated techniques is crucial to effectively combat these emerging threats.

## References

[1] The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years#:~:text=On%20May%207%2C%202021%2C%20a,get%20their%20kids%20to%20school

[2] Studies show ransomware has already caused patient deaths https://www.techtarget.com/searchsecurity/feature/Studies-show-ransomware-has-already-caused-patient-deaths#:~:text=More%20recently%2C%20authorities%20in%20Germany,away%2C%20where%20she%20later%20died

[3] A history of ransomware and the cybersecurity ecosystem https://securityintelligence.com/articles/a-history-of-ransomware-and-the-cybersecurity-ecosystem/

[4] Lessons Learned from the Maroochy Water Breachhttps://www.researchgate.net/publication/221654716_Lessons_Learned_from_the_Maroochy_Water_Breach

[5] The Estonian Cyberattacks https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks

[6] IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs. https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs#:~:text=Critical%20Infrastructure%20Breach%20Costs%20Break,higher%20than%20the%20global%20average.

[7] DDoS Attacks on DYN Take Down Tech Giants: Github, Twitter, Netflix, and More https://westoahu.hawaii.edu/cyber/regional/gce-us-news/ddos-attacks-on-dyn-take-down-tech-giants-github-twitter-netflix-and-more/#:~:text=On%20Friday%20October%2021%2C%202016,%2C%20Netflix%2C%20and%20many%20more.

[8] Economic Impact of Cyber Attacks on Critical Infrastructures https://www.igi-global.com/chapter/economic-impact-of-cyber-attacks-on-critical-infrastructures/228475

[9] UK cyber security and critical national infrastructure protection https://www.researchgate.net/publication/307551686_UK_cyber_security_and_critical_national_infrastructure_protection

[10] Reducing the Threat of State-to-State Cyber Attack against Critical Infrastructure through International Norms and Agreements https://www.jstor.org/stable/resrep05023?seq=3

[11] What is Phishing https://www.techtarget.com/searchsecurity/definition/phishing

[12] Hackers caused power cut in western Ukraine - US https://www.bbc.com/news/technology-35297464

[13] Zero-Day Exploits: Examples, Prevention and Detection https://www.cynet.com/zero-day-attacks/zero-day-exploit-recent-examples-and-four-detection-strategies/#:~:text=Via%20zero%2Dday%20exploits%2C%20an,majority%20of%20the%20Fortune%20500

[14] AI Cracker Can Guess Over Half of Common Passwords in 60 Seconds https://www.spiceworks.com/tech/artificial-intelligence/news/passgan-ai-password-cracking-time/

[15] 5 Ways to Prevent Cyberattacks on Critical Infrastructure https://www.unearthlabs.com/blogs/cybersecurity-critical-infrastructure#:~:text=The%20Russian%20group%20APT28%20(also,U.S.%20targets%20in%20the%20past.&text=Guarding%20against%20these%20attacks%20is,and%20enable%20multi%2Dfactor%20authentication.

[16] What is WannaCry ransomware? https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[17] Building A Cybersecurity Culture In Your Organization https://www.forbes.com/sites/forbestechcouncil/2022/09/13/building-a-cybersecurity-culture-in-your-organization/

[18] NotPetya: the cyberattack that shook the world https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-

cyberattack-that-shook-the-world/articleshow/89997076.cms?from=mdr

[19] Target to pay $18.5M for 2013 data breach that affected 41 million consumers https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

[20] Equifax Data Breach Settlement https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

[21] Dropbox Confirms 2012 Breach Bigger Than Previously Known https://www.bloomberg.com/news/articles/2016-08-31/dropbox-confirms-2012-breach-bigger-than-previously-known

[22] How often should security audits be? https://cybersecurity.att.com/blogs/security-essentials/how-often-should-security-audits-be

[23] What is Defense in Depth? https://www.fortinet.com/resources/cyberglossary/defense-in-depth#:~:text=Defense%20in%20depth%20is%20a,are%20stopped%20along%20the%20way.

[24] Top 12 IT security frameworks and standards explained https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one