POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

Cyber Incidents in Critical Infrastructures: the NotPetya Attack on Maersk's Global Logistics Operations

Author(s): **Elena Casaleggi - 10706547**
Matteo Lo Giudice - 10829241
Veronica Fatigati - 11095787

Academic Year: 2024-2025

Contents

1 | Background & Context

1.1. Maersk: Integrated Transport and Logistics Company

A.P. Møller – Mærsk A/S, commonly referred to as *Maersk*, is a Danish multinational corporation established in 1904 by Arnold Peter Møller and his father, Peter Mærsk Møller [3]. The investment company **A.P. Moller Holding** oversees a diverse portfolio in which Maersk represents the most prominent and strategic investment of the **A.P. Moller Group**, a group of companies active across multiple sectors and industries. Headquartered in Copenhagen, Denmark, Maersk operates in over 130 countries and employs more than 100,000 people worldwide. The company is a global leader in integrated logistics, with its primary focus on transport and energy services.

Maersk core business lies in container shipping, with Maersk Line recognized as one of the world's largest operators in the sector [2]. Facilitating approximately 18% of global seaborne trade, the company plays a pivotal role in connecting continents and ensuring the efficient movement of goods across international markets [8]. Its extensive fleet of vessels facilitates the distribution of products across continents, ensuring efficient global trade. This capacity has established Maersk as a key player in international commerce, contributing significantly to supply chain optimization and connectivity among global markets.

The organization is celebrated for its cutting-edge contributions to maritime transportation, such as the development of the Triple E-class container ships, which prioritize economies of scale, energy efficiency, and environmental sustainability. In 2023, the company reported revenues of $51.1 billion, reflecting its vast scale of influence and impact.

Beyond maritime transport, Maersk has diversified its offerings to include comprehensive logistics and supply chain management solutions. The company provides warehousing, distribution, and supply chain integration services, aimed at improving supply chain efficiency for its customers. This vertical integration allows Maersk to offer end-to-end solutions tailored to meet evolving market needs and challenges.

Furthermore, the company plays a significant role in port operations through its subsidiary, APM Terminals. This division manages numerous harbour terminals worldwide, streamlining

cargo handling and ensuring efficient transportation of goods. APM Terminals is central to the company's strategy to maintain a strong presence in global trade infrastructure.

In recent years, Maersk has actively pursued initiatives to reduce the environmental impact of its operations. The company's commitment to sustainability is evident in its investments in green technologies. A landmark achievement was the launch of the *Laura Maersk* in September 2023, the world's first container vessel powered by methanol, signaling a major step toward decarbonizing the maritime shipping industry.

1.2. The Global Attack of NotPetya

The **NotPetya** attack, which began on June 27, 2017, stands as a landmark event in the history of cyberattacks due to its unprecedented scale and destructiveness [5, 7]. The attack was initiated in Ukraine and primarily targeted Ukrainian businesses and governmental institutions through a compromised software update of **M.E.Doc**, an accounting software widely used in the country. M.E.Doc, developed by the Ukrainian firm Intellect Service, was utilized by approximately 1 million businesses in Ukraine, accounting for about 80% of the country's enterprises [9]. Attackers reportedly stole an employee's password and exploited a server that had not been updated in four years. Once inside Intellect Service's systems, they elevated the user's privileges to administrator and inserted several backdoors[1] into the company's software updates. After successfully directing customers to the modified updates, the attackers used these backdoors to propagate their malware to organizations that had installed M.E.Doc on their own machines. The attack utilized what appeared to be a ransomware mechanism, encrypting victims' files and demanding a ransom payment of approximately $300 in Bitcoin. However, unlike conventional ransomware, it was a wiper[2] in disguise, causing irreversible data loss regardless of payment. This demonstrated the true intent: not financial gain, but widespread destruction and disruption.

NotPetya's timing, launched on the eve of Ukraine's Constitution Day, further underscores its role as a component of hybrid warfare, aimed at destabilizing Ukraine. Evidence suggests that the operation was orchestrated by actors linked to the Russian government, as part of broader geopolitical tensions following the annexation of Crimea. Despite the absence of concrete proof directly implicating the Russian Federation, the circumstantial evidence and broader geopolitical context led to strong international condemnation and attributions by multiple states.

[1] **Backdoor** refers to a method by which unauthorized access is gained to a computer system or software, bypassing normal authentication procedures. It is often installed by attackers to maintain persistent access and control over the compromised system.

[2] **Wiper** refers to a destructive malware designed to erase or corrupt data on a targeted system, leaving it inoperable. This type of malware seeks to disrupt operations and hinder or completely prevent data recovery.

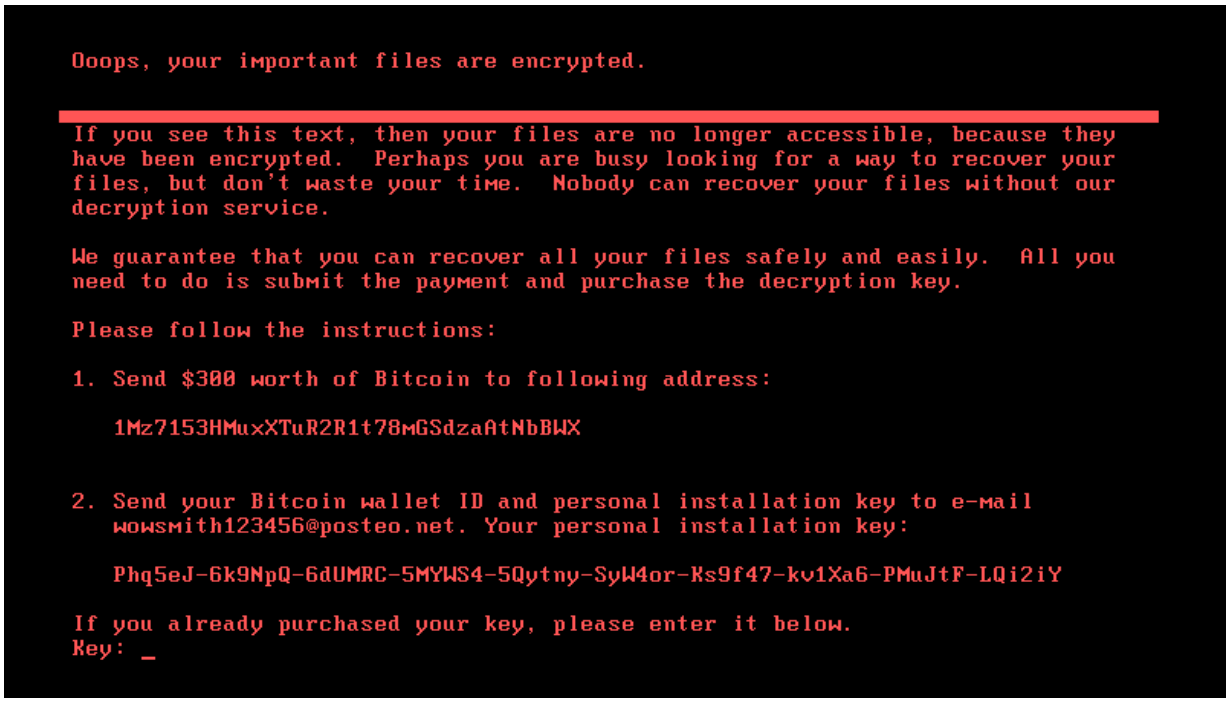

Figure 1.1: The ransom message shown on computers infected by NotPetya. Source: Forbes article by Thomas Brewster (2017).

NotPetya employed a multifaceted approach to infiltrate and propagate within target systems, leveraging both advanced and well-documented cyber techniques. Central to its strategy was the exploitation of the EternalBlue vulnerability and the deployment of credential-harvesting tools such as Mimikatz.

EternalBlue, identified as CVE-2017-0144, is a critical vulnerability in Microsoft's Server Message Block (SMB) protocol, a network file-sharing protocol used in Windows to enable shared access to files, printers, and other resources over a network. Originally discovered by the *National Security Agency* (NSA) and later leaked by the Shadow Brokers[3] in 2017, this exploit enables remote execution of arbitrary code on unpatched Windows machines. By targeting weaknesses in the SMB protocol, attackers can gain unauthorized access, execute malicious code, and facilitate lateral movement across networks with minimal user intervention. NotPetya capitalized on EternalBlue to achieve rapid and widespread dissemination within and across organizational networks.

In addition to EternalBlue, NotPetya incorporated **Mimikatz**, a post-exploitation tool developed by French security researcher Benjamin Delpy. Originally created as a proof-of-concept to demonstrate that Windows passwords could be extracted from system memory, Mimikatz quickly became a powerful tool in cyber intrusions. Delpy's work highlighted significant secu-

[3] **Shadow Broker** is a hacker group known for leaking NSA-developed hacking tools and exploits.

rity weaknesses in Windows, particularly through the WDigest[4] authentication protocol, which stored not only encrypted passwords but also their decryption keys in memory. This allowed attackers using Mimikatz to extract these keys and gain access to plaintext passwords, enabling repeated access to compromised systems. Microsoft initially downplayed the vulnerability, arguing that attackers would need prior access to reach such sensitive system memory areas. However, Delpy's demonstration proved otherwise, showing that administrative privileges could unlock critical credentials, posing a significant risk.

This capability became an important part of NotPetya's strategy. Once Mimikatz was deployed on a compromised system, it allowed attackers to harvest credentials stored in memory, escalate their privileges, and authenticate to other machines within the network. By extracting legitimate user credentials, NotPetya facilitated lateral movement across connected devices, even those without the SMBv1 vulnerability exploited by EternalBlue. This dual-pronged approach significantly enhanced NotPetya's propagation capabilities. While EternalBlue allowed attackers, believed to be linked to the Russian GRU (the Main Intelligence Directorate of Russia's military), to remotely execute code on systems with the unpatched SMBv1 vulnerability; Mimikatz enabled the malware to target devices that would not have been affected by EternalBlue alone. With Mimikatz's ability to mine and utilize user credentials, the attackers could pivot from one system to others within the same network, granting them extensive reach and control.

Beyond these primary mechanisms, NotPetya employed several supplementary techniques to enhance its propagation and impact. Upon execution, the malware attempted to escalate privileges by acquiring specific rights, including *SeDebugPrivilege*, *SeTcbPrivilege*, and *SeShutdownPrivilege*. These privileges granted the malware access to critical system components and the ability to initiate system shutdowns, thereby facilitating its destructive objectives.

NotPetya also conducted network enumeration to identify potential targets within the local network. It retrieved the infected machine's hostname, IP address, and subnet mask, and determined whether the machine functioned as a server or workstation. If identified as a server, the malware enumerated DHCP[5] leases to discover connected devices and attempted to propagate using EternalBlue. For workstations, it similarly sought to connect to other machines via the same exploit. This enumeration process was executed at regular intervals to ensure continuous propagation.

[4] **Digest Authentication** is a challenge/response protocol that was primarily used in Windows Server 2003 for LDAP and web-based authentication. It utilizes Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges to authenticate.

[5] **Dynamic Host Configuration Protocol** is a network management protocol used to automatically assign IP addresses and other network configuration details to devices on a network, simplifying the process of connecting devices to the network.

To further facilitate its spread, NotPetya utilized legitimate administrative tools such as *PsExec* and *Windows Management Instrumentation* (WMI). By leveraging these tools, the malware could execute commands on remote systems, thereby extending its reach within the network. This combination of exploiting known vulnerabilities, harvesting credentials, and utilizing legitimate administrative utilities underscores the sophisticated and multifaceted nature of NotPetya's propagation strategy.

The combination of EternalBlue and Mimikatz made NotPetya highly effective at infiltrating systems and quickly compromising entire networks. The malware's lateral movement capabilities and worm-like behavior meant that a single point of entry was sufficient to cause widespread damage. Beyond Ukraine, where the attack was primarily targeted, numerous high-profile global companies, including Merck, FedEx's European subsidiary TNT Express, Saint-Gobain, Mondelez International, and Reckitt Benckiser, were severely affected. The attack inflicted billions of dollars in damages and underscored the catastrophic potential of state-backed or highly sophisticated cyber campaigns.

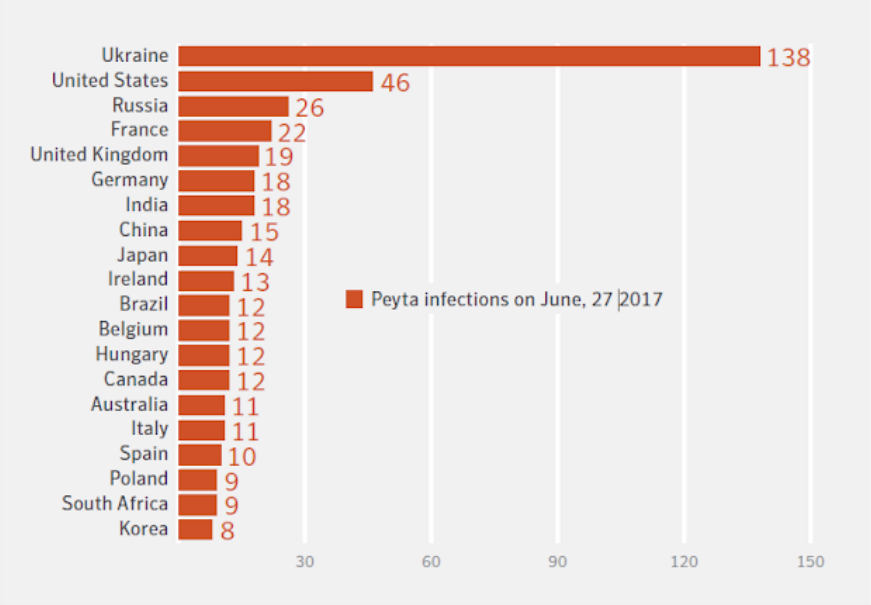

Figure 1.2: NotPetya attacks by country. Source: Report on NotPetya by Menshaway Blog (2019).

1.3. The Impact on Maersk

The NotPetya cyberattack had severe implications for Maersk, starting with a single infected computer at the company's office in Odessa, Ukraine [12]. The malware gained entry through a compromised update of the widely used M.E.Doc tax software. Once inside, NotPetya exploited the EternalBlue vulnerability and utilized Mimikatz to harvest credentials, enabling it to spread laterally across Maersk's global IT network. Within minutes, critical systems were en-

crypted and rendered inoperable, exposing the company's reliance on an unsegmented network architecture[6], which allowed the malware to propagate unhindered.

The disruption to Maersk's operations was instant and far-reaching. 17 major terminals, including vital hubs in Rotterdam and Los Angeles, became non-operational, halting cargo handling and delaying shipments. Employees were forced to use manual processes, handwritten logs and messaging apps (WhatsApp and Gmail), to manage basic logistics tasks. *Maerskline.com*, its core booking platform crucial for global shipping, was rendered inaccessible, and over 49,000 endpoints, including laptops and servers, were compromised leaving customers unable to track or schedule shipments. Approximately 20% of the company's trading capacity was lost during the attack, compounding its logistical and operational challenges.

In the immediate aftermath of the malware's spread, the company's staff scrambled for two hours to disconnect its global network in an attempt to halt further propagation. Maersk then enlisted Deloitte[7] to lead the recovery operation, which was headquartered at an emergency operations center in the UK. The operation brought together as many as 600 personnel, including Maersk's IT staff flown in from across the globe and Deloitte's specialists, who worked to rebuild the company's network.

Initially, the recovery team managed to locate backups for most of Maersk's individual servers. However, the situation worsened when they discovered that the network's domain controllers[8], around 150 servers that mapped the network and managed user access, had been entirely wiped out. These controllers had been designed to restore one another in case of failure, but the system did not account for a scenario where all were simultaneously compromised. Without these critical controllers, Maersk had no way to recover its logistical data, a cornerstone of its global operations.

During this crisis, a vital breakthrough arose from an unexpected stroke of fortune. After contacting hundreds of local IT staffers across its global offices, the recovery team learned that a single intact domain controller had survived in Maersk's corporate office in Tema, Ghana. A power outage had disconnected the office from the global network at the time of the attack, inadvertently sparing the controller from infection. However, the office's low bandwidth made it impossible to transmit the data online. To retrieve it, Maersk dispatched a Ghanaian employee

[6] **Network segmentation** is a cybersecurity practice that divides a network into smaller, isolated segments to restrict the lateral movement of threats. By isolating systems and limiting access between segments, organizations can contain potential breaches, minimizing their impact on critical infrastructure.

[7] **Deloitte** is one of the "Big Four" accounting and professional services firms, providing services in audit, consulting, tax, and advisory. With a global presence in over 150 countries, Deloitte is renowned for its expertise in helping organizations manage complex challenges, including cybersecurity and crisis recovery.

[8] A **domain controller** is a server within a computer network that manages security, user authentication, and access permissions. It is responsible for validating credentials when users log in and determining which resources they can access, acting as a central point for network administration in systems using directory services like Microsoft Active Directory.

to Nigeria, where they handed off the domain controller to another staff member, who then flew it to the UK emergency operations center. This hard drive, holding the only surviving copy of Maersk's domain controller data, became the key to restoring the network.

With the domain controller data in hand, Maersk began the painstaking process of recovery. Priority was given to port operations, which were partially restored within a few days, followed by booking systems. However, it took over a week for the global terminals to achieve even a semblance of normalcy, and nearly two weeks before employees regained access to their personal computers. The reconstruction of Maersk's network, including 4,000 servers, 45,000 PCs, and 2,500 applications took 10 days of relentless work, while full operational recovery spanned almost two months. This extraordinary effort underscored both the vulnerabilities in Maersk's pre-attack infrastructure and the resilience and determination of its recovery team.

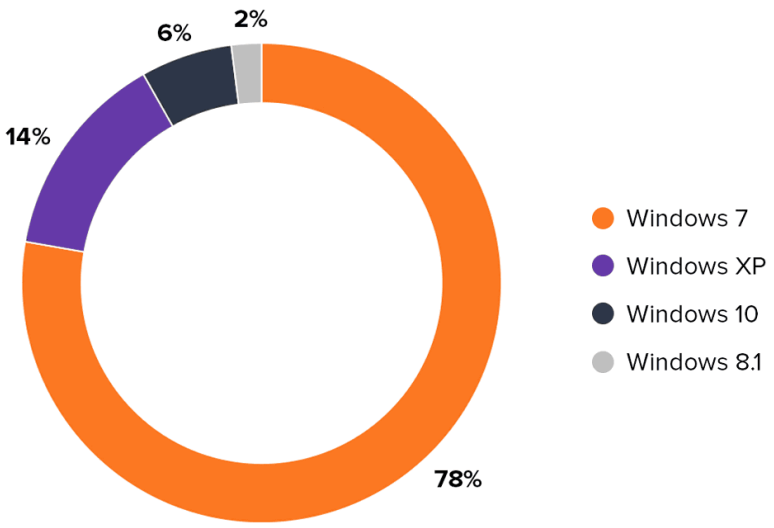

Figure 1.3: Targeted Machines by Operating System. Source: Gigazine article (2017).

The financial toll of the attack was equally severe with recovery efforts cost between $300 and $350 million. These expenses were exacerbated by lost business and compensation payouts, making NotPetya one of the costliest cyberattacks in history. Despite the immediate market capitalization drop, Maersk's reputation as a resilient organization helped it recover relatively quickly.

In addition, Maersk's transparent communication strategy proved pivotal in preserving stakeholder trust. Regular updates through Twitter, WhatsApp, and email reassured customers, while senior leadership, including the CEO, *Jim Snabe*, played an active role in managing the crisis. This approach was widely praised as a benchmark in corporate crisis management, highlighting the importance of honesty and engagement during critical situations. Despite the operational and financial toll, Maersk's effective handling of the crisis positively impacted its reputation. Within a year of the attack, the company's brand value increased by 43%, reflecting stakeholder confidence in its resilience and transparency.

Figure 1.4: Maersk's first public announcement on Twitter. Source: Maersk Tweet (2017).

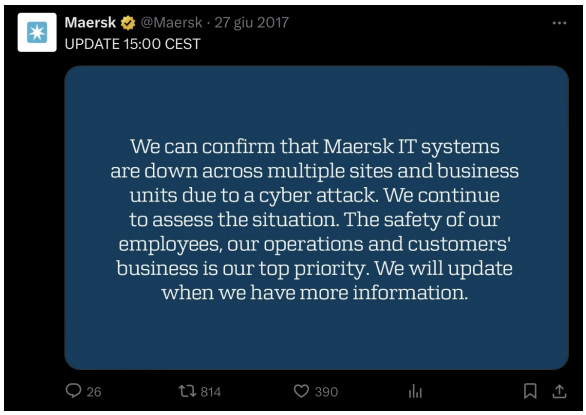

Figure 1.5: Maersk's Twitter update. Source: Maersk Tweet Update (2017).

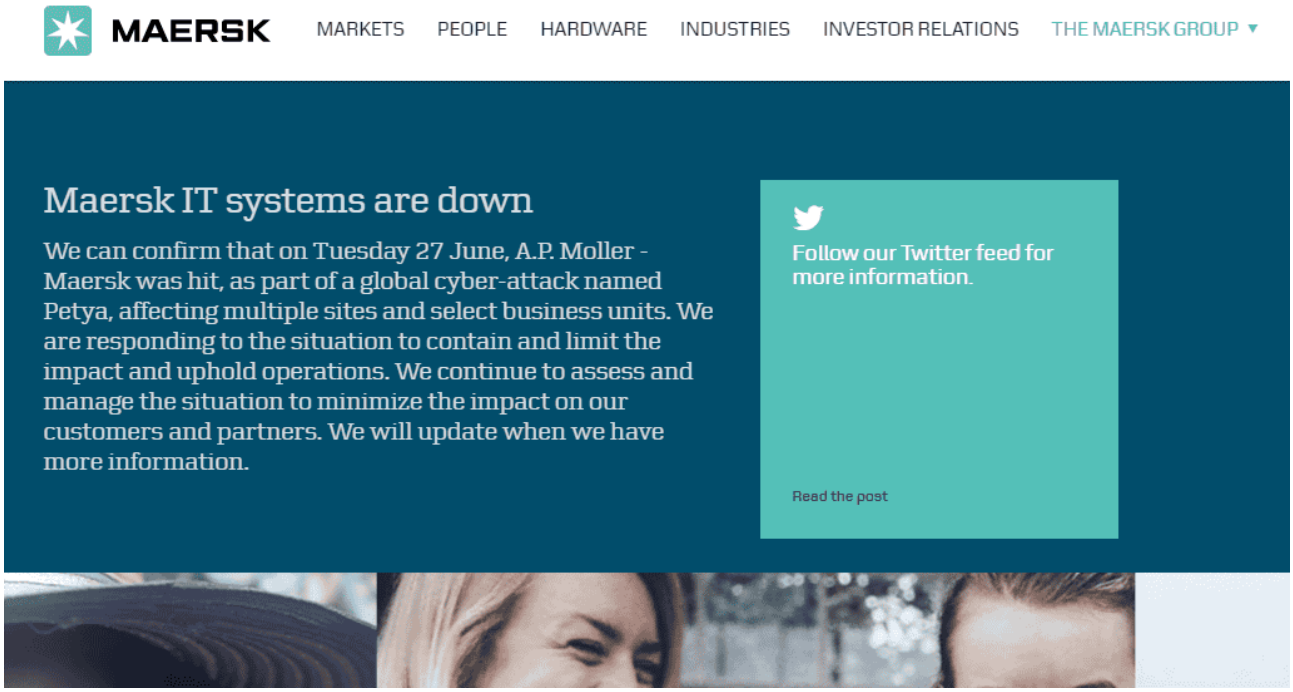

Figure 1.6: Screenshot of Maersk's website during the NotPetya attack. Source: Gigazine article (2017).

The NotPetya attack had a transformative impact on Maersk, prompting significant investments in automated threat detection, incident response training, and IT infrastructure overhauls. It also sparked a cultural shift, embedding cybersecurity as a core pillar of the company's strategy while underscoring the importance of cyber insurance for financial stability. Beyond these changes, the attack exposed the vulnerabilities of interconnected systems and highlighted the catastrophic risks of state-backed cyber campaigns, serving as a costly but vital lesson in resilience and risk management.

2 | Model-Based in-Depth Analysis

Building on the background and context of the NotPetya attack and its severe impact on Maersk's global operations, this chapter delves into a systematic exploration of the underlying vulnerabilities and defensive failures that facilitated the crisis. By employing established analytical methodologies, the analysis aims to uncover the interaction of technical and organizational factors that converged to allow the attack's progression. These tools break down the sequence of events but also provide a structured framework for understanding systemic weaknesses and identifying actionable insights to improve organizational resilience. This chapter marks a key shift from recounting the attack's narrative to an in-depth evaluation of its root causes and broader implications.

2.1. Technical Reconstruction of Incident Failures

In the investigation of the NotPetya attack that infiltrated Maersk's IT infrastructure, **Fault Tree Analysis (FTA)** was employed as a retrospective tool to uncover the dependencies and causal relationships that led to the total compromise of the company's systems. Unlike a forward-looking risk assessment, where potential failure scenarios are hypothesized, this retrospective approach focuses exclusively on the sequence of events that occurred, isolating the active factors and their interdependencies. This analytical method provides a structured framework to clarify how individual vulnerabilities converged to produce the observed outcome and enables a deeper understanding of the systemic weaknesses that contributed to the event.

At the core of the FTA is the identification of the **top event**: the total compromise of Maersk's global IT systems. This event serves as the focal point of the analysis that proceedes by systematically deconstructing this top event into its constituent causes, represented as a hierarchical structure that maps the logical dependencies between different failure points.

The hierarchical breakdown beneath the top event identifies three main branches: the infection of Maersk's endpoints via the compromised M.E.Doc software, the exploitation of weaknesses in the company's network infrastructure, and the lack of sufficient network access controls. These branches, connected by an *AND* gate, illustrate how each element was indispensable in enabling the total compromise of the company's IT systems.

The first branch highlights the manipulation of legitimate administrative tools, such as PsExec

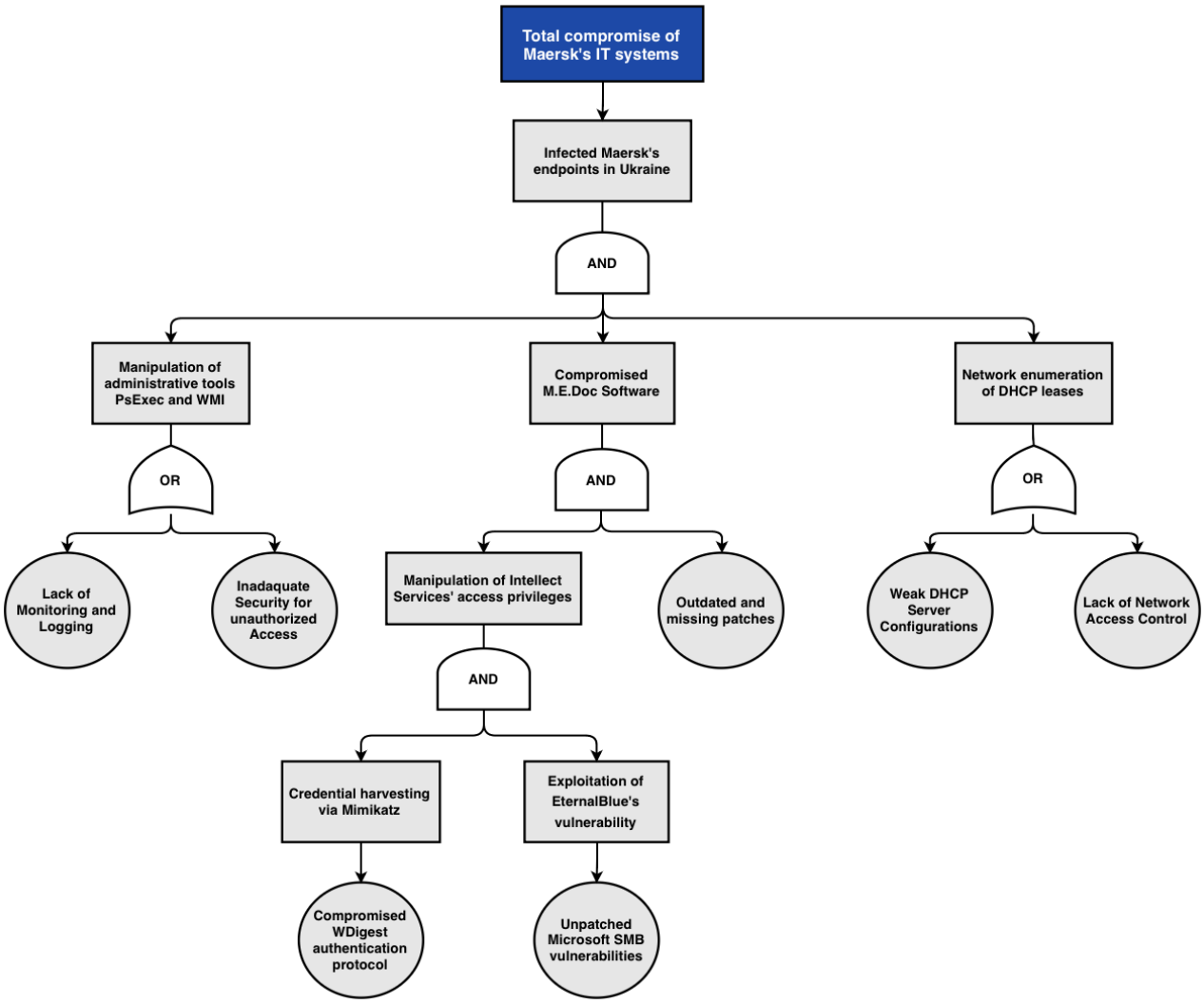

Figure 2.1: Fault Tree Analysis

and WMI, as critical enablers for lateral movement within Maersk's unsegmented network. The lack of centralized monitoring and logging, combined with inadequate security measures for controlling administrative access, created an environment where attackers could exploit these tools without detection. This interdependence, represented by an *OR* gate, signifies that either factor alone could have sufficed to facilitate this phase of the attack.

The second branch focuses on the compromised M.E.Doc software, which served as the initial infection vector. However, the subsequent propagation of the malware was dependent on the exploitation of privilege escalation techniques, particularly through the use of Mimikatz for credential harvesting and EternalBlue for leveraging unpatched SMB vulnerabilities. These elements are linked through an *AND* gate, reflecting the necessity of their combined presence to achieve the widespread impact observed.

Finally, the third branch examines the network enumeration of DHCP leases, which was enabled by weak DHCP server configurations and the absence of effective network access controls. These vulnerabilities, connected by an *OR* gate, illustrate how either could independently facilitate the lateral spread of malware. The broader failure to implement network segmentation further compounded the impact, allowing the malware to traverse the entire infrastructure unimpeded.

This retrospective FTA clarifies the dynamics of Maersk's systemic vulnerabilities, shedding light on the interaction and convergence of specific failures that enabled the NotPetya attack. Beyond merely mapping causal pathways, the analysis reveals critical dependencies and operational redundancies, providing a detailed understanding of how localized weaknesses cascaded into a global compromise. This structured decomposition forms the analytical foundation for evaluating mitigation strategies and systemic resilience in subsequent discussions, underscoring the importance of addressing both technical and organizational interdependencies in defending against complex cyber threats.

2.2. Structured Assessment of Organizational Weaknesses

The **Swiss Cheese Model** outlines the sequential breakdowns across Maersk's defensive layers during the NotPetya attack [13]. This representation reveals how weaknesses can align creating a pathway for incidents to escalate unnoticed. The model highlights the coexistence of **technical** and **organizational barriers** reflecting the interplay between system design and policy implementation, while the holes within these layers symbolize vulnerabilities or operational flaws.

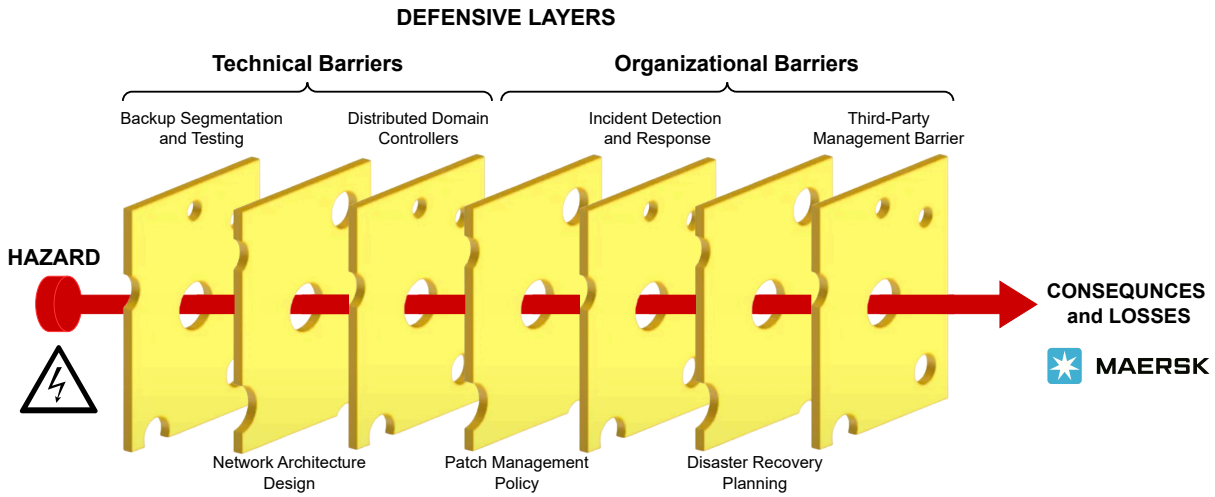

Figure 2.2: Swiss Cheese Model

The technical barriers displayed critical gaps during the attack. As underlined in the FTA, the lack of network isolation allowed the malware to propagate laterally without restriction. Similarly, the insufficiency of backup segmentation and testing left the infrastructure vulnerable to simultaneous, widespread data loss. The absence of real-time incident detection further delayed an effective response, compounding the issues identified earlier. These failures illustrate how weaknesses in technical barriers aligned to aggravate the systemic vulnerabilities already discussed in the FTA.

Organizational barriers, including third-party management and disaster recovery planning, were equally pivotal. The compromised M.E.Doc software update identified limitations in vendor security management, a critical vulnerability in preventing supply chain attacks. Furthermore, the disaster recovery strategy lacked adaptability to the unprecedented scenario of all domain controllers being wiped simultaneously. This reliance on predefined recovery pathways created a **single point of failure (SPOF)**[9] that the attackers exploited.

Despite these failures, certain defensive mechanisms showcased resilience, preventing total operational collapse. The fortuitous preservation of a domain controller in Tema, Ghana, and the rapid mobilization of global IT staff underscored the importance of redundancy and human coordination in mitigating damages. However, these outcomes were more reactive than preventive, revealing a pressing need for integrated planning between technical and organizational layers.

The Swiss Cheese Model proves invaluable for our analysis; by illustrating how misaligned defenses enabled the attack's escalation, it provides a comprehensive lens for understanding systemic failures. Beyond diagnosing the event, the model's visual and layered structure makes it a powerful tool for deriving actionable insights, as it bridges the gap between in-depth technical analysis and broader strategic planning. In this case, the model underscores the need for tighter integration between operational safeguards and management policies, emphasizing that cybersecurity resilience depends as much on organizational preparedness as on technical robustness.

[9] A **Single Point of Failure** refers to a critical component in a system whose failure would cause the entire system to fail or significantly disrupt its operation.

3 | Critical Discussion

Drawing from the analysis conducted in the second chapter, the focus now shifts toward the consequences and broader implications of the NotPetya attack on Maersk. Through different tools we examine how the crisis unfolded into significant operational, financial, and reputational impacts, highlighting the critical role of resilience in mitigating such events. This section aims to critically discuss the effectiveness of the countermeasures implemented and distill the lessons learned to inform future strategies, not only for Maersk but for the broader industry. By bridging analysis with actionable insights, this chapter underscores the importance of adapting to an evolving threat landscape in order to safeguard business continuity and improve safety performance across critical infrastructure.

3.1. Mapping the Threat-to-Consequence Pathway

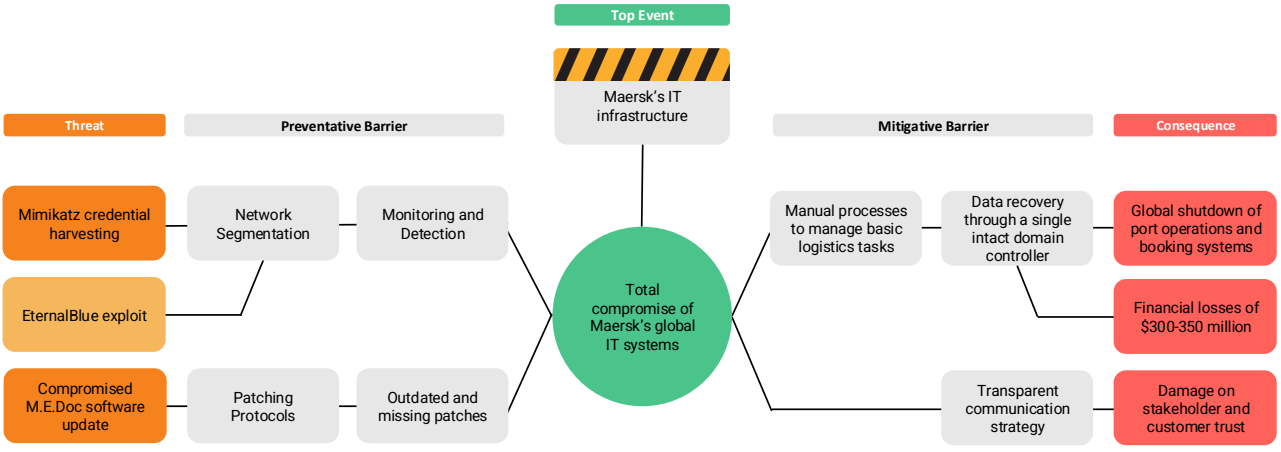

Figure 3.1: Bow-Tie Diagram

The **Bow-Tie Model** serves as a comprehensive framework for connecting the technical and organizational vulnerabilities identified in the previous analyses to their resulting consequences. Acting as a visual representation of cause and effect, the model bridges the findings from the Fault Tree Analysis and Swiss Cheese Model to offer a more integrated understanding of how the convergence of various failures led to significant operational disruptions and financial losses.

At the center of the Bow-Tie diagram is the **top event**: the total compromise of Maersk's global IT systems. This central node connects the antecedent technical and organizational

failures to the subsequent consequences, providing a holistic view of the incident's progression.

Financially, the attack inflicted substantial losses, with estimates ranging between $300 million and $350 million. These figures encompass not only immediate remediation costs but also the broader economic impact of halted operations and lost business opportunities.

Beyond the tangible financial and operational setbacks, the attack eroded stakeholder and customer trust [10]. The inability to fulfill commitments and the perceived vulnerability of Maersk's systems led to reputational damage, the effects of which extended beyond the immediate recovery period.

The Bow-Tie Model served as a key tool to encapsulate the trajectory from initial vulnerabilities to severe consequences, helping us to understand the critical need for robust preventive and mitigative measures. As we analyze further, the consequences and impacts of this critical incident extend beyond immediate technical failures, affecting operational continuity, financial stability, and organizational reputation.

3.2. From Disruption to Continuity

From the consequences identified through the Bow-Tie Model, the **Business Impact Analysis (BIA)** allows us to delve deeper into the specific operational, financial, and reputational disruptions caused by the NotPetya cyberattack on Maersk [1]. By linking these consequences to targeted solutions, the BIA provides a roadmap for ensuring business continuity in the face of future incidents, while the lessons learned from this case offer a broader perspective on resilience in the increasingly interconnected digital landscape.

To assess the consequences, we adopted recognized standards for evaluating impacts in critical scenarios. These frameworks guided the classification of *Operational*, *Financial*, *Legal and Regulatory*, and *Reputational Impacts*, ensuring a structured and consistent approach to measuring severity. In addition, given Maersk's role in the global supply chain, disruptions to its services had far-reaching consequences, affecting businesses worldwide that rely on its operations for continuity and stability. Each category has been analyzed across three severity levels, *High*, *Medium*, and *Low*, allowing us to qualitatively describe the extent of disruption and highlight the resources required to mitigate each impact effectively.

Moreover, the following activities represent Maersk's core logistics and supply chain offerings, each tailored to address specific operational needs and industry requirements while ensuring efficiency and resilience across the global network.

- **Transport**: Ocean Transport (ensures stable rates and dependable space for shipping large cargo across oceans), Intermodal Transport (integrates sea and inland transport, enabling smooth cargo movement between ports and inland destinations), Less-than-

Container Load (LCL) (facilitates small-volume cargo shipments, combining loads to optimize costs), Air Freight (provides expedited delivery for urgent shipments by air), and Maersk Ground Freight Transport (covers full truckload (FTL) and less-than-truckload (LTL) services for inland cargo movement).

- **Store**: Warehousing (offers facilities for storing goods with efficient end-to-end distribution capabilities), Depot (functions as key stopover points for cargo management and redistribution), and Cold Storage (maintains the integrity of temperature-sensitive goods with reliable refrigeration systems to ensure unbroken cold chains).
- **Clear & Protect**: Maersk Customs Services (simplifies customs procedures globally with localized expertise, ensuring smooth clearance processes) and Value Protect (provides insurance-like coverage to safeguard cargo from damage, loss, or accidents during transportation).
- **Logistics Management**: E-Commerce Logistics (supports direct shipping from production sites to consumers for online businesses), Cold Chain Solutions (guarantees timely and efficient delivery of refrigerated goods, ensuring product quality), Lead Logistics (offers specialized partner services to manage complex supply chains for customers), Maersk Project Logistics (handles large-scale and industrial logistics projects, delivering tailored solutions for oversized or specialized cargo), and Decarbonizing Logistics (provides logistics solutions that focus on reducing greenhouse gas (GHG) emissions, supporting sustainability initiatives).

LEVEL	HIGH	MEDIUM	LOW
Operations Impact	Operational activities are blocked or clogged and cannot continue	Operational activities can partially continue	Low impacts on the the operational actitivies
Financial Impact	High damage that may imply huge financial loss	Medium damage that may require additional resources to mitigate the financial loss	Low financial loss since the impact is mitigated
Legal and Regulatory Impact	High sanctions with legal consequences affecting operation in the short term	Medium sanctions affecting operation in the short term or medium impact on global customs with each local expertise	Low/no sanctions with no impact on operations
Reputational Impact	High global reputation and image damages with consequent media resonance and with high impacts on the company's customers and stakeholders trust	Medium reputation and image demages with few impacts on the company's customers and stakeholders trust	Low reputation or image damages
Supply Chain Impact	Severe disruption to supply chain operations, causing global delays, halts in logistics activities, and significant cascading effects across dependent industries.	Medium disruption to supply chain operations, requiring additional resources to address delays while partially maintaining critical activities.	Low impact on supply chain operations, with manageable delays and no significant interruptions to critical processes

Figure 3.2: Impacts Criteria

The BIA emphasizes the need for refined strategies to address vulnerabilities exposed by the systemic collapse, with a focus on operational continuity, supply chain resilience, and customer

trust. While Maersk's recovery demonted remarkable agility, the implemented countermeasures, as rapid infrastructure reconstruction and temporary manual operations, were largely reactive. This highlights the necessity for more robust, pre-emptive measures to safeguard critical operations. For transport, the suggested implementation of system redundancy and isolated networks for operational technology (OT) is essential to contain malware propagation and ensure cargo tracking continuity. Backup and recovery solutions fitted to transport systems will prevent prolonged service shutdowns, addressing a core operational risk.

In logistics and warehousing, the proposed strategies go beyond temporary fixes to establish long-term resilience. Real-time inventory tracking systems, supported by redundant data backups and IoT[10]-enabled monitoring, can significantly reduce the risks associated with storage disruptions. This is particularly critical for cold storage, where maintaining uninterrupted power through backup generators ensures the protection of temperature-sensitive goods. Additionally, pre-established agreements with third-party providers for overflow management offer a practical solution for maintaining operational capacity during crises. For logistics management, integrating predictive analytics and end-to-end visibility platforms addresses the most severe operational impacts, while alternative partnerships for large-scale projects provide immediate contingency support. These solutions not only minimize downtime but also enhance the adaptability and robustness of core business functions.

A critical lesson from the Maersk incident is the importance of rigorous compliance and risk management when engaging with third-party vendors. The root cause of the NotPetya attack stemmed from Maersk's reliance on the M.E.Doc accounting software, which was widely used in Ukraine and served as the initial infection vector. While Maersk's operations in Ukraine were legitimate, the lack of comprehensive third-party risk assessments exposed the company to vulnerabilities that could have been mitigated. This underscores the need for organizations to scrutinize the cybersecurity posture of external vendors, particularly in regions with heightened geopolitical risks or known cyber threats. Regular audits, strict compliance standards, and third-party software isolation within segmented environments are essential to minimizing such risks. By ensuring that third-party solutions align with internal security policies, organizations can reduce the likelihood of supply chain attacks, safeguarding operations against threats originating beyond their direct control.

The appropriateness of these countermeasures lies in their ability to address both short-term disruptions and long-term systemic vulnerabilities. Prioritizing resilience at every layer (technical, operational, and organizational) emphasizes the importance of transitioning from reactive crisis management to proactive risk mitigation, ensuring that operations remain stable, efficient, and capable of withstanding disruptions in an increasingly volatile digital landscape.

[10] The **Internet of Things (IoT)** refers to a network of connected devices that communicate and share data over the internet.

Process: Maersk												
Activities	Impacts evaluation							MTPD	Justification on MTPD	Peak periods	Business Continuity Impact	Inclusion in the BCP	Suggested BC solutions/strategies
		0-2 hours	2-4 hours	4-8 hours	8-12 hours	1 day	3 days						
Transport	Operations Impact	Low	Medium	Medium	High	High	Medium	8-12 hours	Transports, being one of the core businesses, suffered a significant slown down and then shutdown of the activities.	Business days	High	YES	Maersk should prioritize system redundancy and backup solutions for core transport operations, ensuring continuity in cargo tracking and shipping monitoring. Additionally, implementing robust cybersecurity measures tailored to transport-specific systems, such as isolated networks for operational technology (OT) and rapid recovery protocols, will help maintain service reliability.
	Financial Impact	Low	Low	Low	Low	Medium	Medium						
	Legal and Regulatory	Low	Low	Low	Low	Low	Low						
	Reputational Impact	Low	Low	Medium	Medium	High	High						
	Supply Chain Impact	Low	Medium	Medium	Medium	High	High						
Store	Operations Impact	Low	Medium	Medium	High	High	Medium	8-12 hours	Storage and warehousing systems are highly correlated to the transports and therefore are considerably affected.	Business days	High	YES	The company should implement resilient systems for real-time inventory tracking and management, with redundant backups to prevent data loss. For cold storage, priority should be given to maintaining uninterrupted power supply through backup generators and monitoring systems to safeguard temperature-sensitive goods. Clear protocols for rerouting goods and managing inventory overflow during crises are essential, along with pre-established agreements with third-party storage providers to handle temporary capacity needs.
	Financial Impact	Low	Low	Low	Low	Medium	Medium						
	Legal and Regulatory	Low	Low	Low	Low	Low	Low						
	Reputational Impact	Low	Low	Medium	Medium	High	High						
	Supply Chain Impact	Low	Medium	Medium	Medium	High	High						
Clear & protect	Operations Impact	Low	Low	Low	Medium	Medium	Medium	3 days	The clear and protect activities have a larger margin of tolerance before becoming seriously impacted.	Emergency situations	Medium	YES	Robust digital platforms for customs processing and cargo protection should have secure, redundant systems and isolated backups to prevent disruptions in critical services like customs clearance and value protection offerings. Streamlined workflows for customs documentation, supported by local expertise and automated solutions, can minimize delays during crises. For value protection, proactive risk assessment and insurance solutions tailored to specific cargo types will safeguard goods against potential damages, maintaining customer confidence and service reliability.
	Financial Impact	Low	Low	Low	Low	Medium	Medium						
	Legal and Regulatory	Low	Medium	Medium	Medium	Medium	Medium						
	Reputational Impact	Low	Low	Medium	Medium	Medium	Medium						
	Supply Chain Impact	Low	Low	Medium	Medium	Medium	High						
Logistics Management	Operations Impact	Medium	High	High	High	High	High	2-4 hours	Logistics suffered the most direct consequences having the systems completely out of service.	Potentially always	High	YES	The focus should be on integrating advanced digital platforms with real-time visibility and predictive analytics to manage end-to-end logistics processes effectively. For cold chain solutions, leveraging IoT-enabled monitoring for temperature control and backup refrigeration systems is critical to protect perishable goods. To address disruptions in large-scale or specialized logistics projects, pre-arranged partnerships with alternate service providers can provide immediate operational support.
	Financial Impact	Low	Low	Medium	Medium	Medium	Medium						
	Legal and Regulatory	Low	Low	Low	Low	Low	Low						
	Reputational Impact	Low	Medium	High	High	High	High						
	Supply Chain Impact	Medium	Medium	High	High	High	High						

Figure 3.3: Business Impact Analysis

3.3. Lessons Learned and Conclusions

The Maersk NotPetya incident stands as one of the most consequential cyberattacks in modern history, not only for the maritime and logistics industry but for global business operations at large. In its aftermath, the world witnessed a turning point in cybersecurity preparedness, exposing systemic vulnerabilities and forcing a radical reevaluation of resilience strategies across all sectors. As Maersk's Chief Information Security Officer, *Andy Powell*, later reflected, "*It was a wake-up call for everyone. It taught us that cyberattacks are no longer a distant or theoretical risk, they are an operational reality that can cripple businesses overnight*" [11]. We echo this sentiment, recognizing that the attack shattered the illusion that certain industries, particularly those outside finance or defense, are insulated from cyber threats. In today's hyperconnected world, where every organization operates online and shares an implicit link to global networks, no sector is immune.

The most eye-opening realization for Maersk, and indeed for all industries, was that their assumption of being an unappealing target had left them exposed. This stresses a vital lesson: cyber resilience is not industry-specific but universal. Regardless of size, sector, or perceived geopolitical importance, every business is a potential target, as every business relies on digital systems for its operations. The interconnectedness of supply chains, critical infrastructure, and commerce amplifies the scale of potential fallout, making cyber preparedness as indispensable as physical security measures.

The attack's global reverberations prompted significant shifts in both regulatory frameworks and organizational strategies. Institutions such as the **International Maritime Organization (IMO)** responded by mandating the incorporation of cyber risk management into safety systems through *Resolution MSC.428(98)*, which took effect in 2021 [6]. This landmark directive underscored the urgent need for industries to treat cybersecurity as a fundamental operational priority rather than an ancillary IT concern. On a broader scale, the introduction of the **General Data Protection Regulation (GDPR)** in 2018 reinforced the financial and legal consequences of poor cyber preparedness, ensuring that data security and incident reporting are now paramount across all European businesses [4].

From a business continuity perspective, NotPetya highlighted the devastating financial implications of large-scale cyber incidents. Maersk's losses of over **$300 million** were major but survivable for a global leader of its scale. For smaller enterprises, such disruption can lead directly to bankruptcy. Recognizing this existential risk has accelerated the adoption of proactive strategies: robust offline backups, network segmentation, disaster recovery planning, and third-party vendor scrutiny are now foundational elements of cyber risk mitigation.

Crucially, Maersk's resilience, fueled by decisive leadership, decentralized decision-making, and transparent communication, offered a powerful blueprint for recovery. Employees, relying on

innovation and resourcefulness, kept operations afloat through manual workarounds while IT systems were painstakingly restored. This demonstrated that, while technological solutions are essential, human adaptability remains a critical line of defense during crises.

Reflecting on the broader landscape, NotPetya was not an isolated event but part of a larger trend of escalating cyber threats. In the years since 2017, the scale, sophistication, and frequency of attacks have increased exponentially, making cybersecurity not just an operational requirement but a matter of business survival. The lessons learned from Maersk emphasize that resilience is a journey, not a destination: businesses must continuously evolve to anticipate emerging risks, as complacency in the digital age paves the way for disaster.

In conclusion, the Maersk NotPetya attack serves as a monumental case study in modern cybersecurity, illustrating both the catastrophic potential of cyberattacks and the transformative power of resilience. It is a sobering reminder that preparedness, leadership, and adaptability are non-negotiable components of survival in an increasingly volatile digital landscape. As we move forward, businesses must internalize that cyber resilience is not merely about defense but about ensuring continuity, safeguarding trust, and growing stronger. The ultimate lesson is clear: the cost of inaction far exceeds the investment in preparedness, and those who fail to adapt risk becoming footnotes in future cyber disasters.

Bibliography

[1] N. Abbatemarco, G. Salviotti, C. D'Ignazio, and L. M. De Rossi. *Understanding Leadership Competencies in Cyber Crisis Management: Insights from the Maersk Global Supply Chain Meltdown*. 2024.

[2] S. T. Anwar. *Global strategy gone astray: Maersk's big box boats and the world shipping industry*. *Thunderbird International Business Review*, 62(2):183–196, 2020.

[3] A.P. Moller Holding. *A.P. Moller - Mærsk*, 2024. URL https://apmoller.com/portfolio/a-p-moller-maersk/.

[4] GDPR Info. *General Data Protection Regulation (GDPR)*, 2024. URL https://gdpr-info.eu.

[5] A. Greenberg. The untold story of notpetya, the most devastating cyberattack in history. *Wired*, August 2018. URL https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Accessed: 2024-06-16.

[6] International Maritime Organization (IMO). *Cyber Security in the Maritime Sector*, 2024. URL https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

[7] C. Krasznay. *Case study: The notpetya campaign*. *Információés kiberbiztonság*, pages 485–499, 2020.

[8] Maersk. *About Maersk*, 2024. URL https://www.maersk.com/about.

[9] M. Menshaway. *NotPetya Tactical Report*, 2019. URL https://menshaway.blogspot.com/2019/07/notpetya-tactical-report.html.

[10] C. Pownall. *The Context and Impact of Maerk's NotPetya cyber attack*. *Cpc & Associates*, 2019.

[11] Riviera Maritime Media. *Protect and survive: How Maersk learned from the NotPetya cyber attack*, 2019. URL https://www.rivieramm.com/news-content-hub/news-content-hub/protect-and-survive-how-maersk-learned-from-the-notpetya-cyber-attack-55284.

[12] S. Steinberg, A. Stepan, and K. Neary. *NotPetya: A Columbia University Case Study*. Technical report, Columbia University, School of International and Public Affairs (SIPA), 2021. Case Number: SIPA-21-022.1.

[13] Team GAIT. The NotPetya Case: Attack against Ukraine on 27th of June 2017, 2017. Case Study for ELEC-E7470 - Cybersecurity P.