MILLIMAN WHITE PAPER

The law of unintended consequences:

When companies are collateral damage in a cyberattack

Chris Harner, FRM
Chris Beck
Blake Fleisher

Milliman

It's no secret that cybersecurity is a major concern for most companies. Recent examples of a hacker accessing information from over 100 million Capital One customers, and the rumored state actor involvement in the breach of 500 million records of consumer data from Marriott, demonstrate that cyber is a critical risk.

Due to headlines and lawsuits, management is increasingly focused on how to address cyber risk. Many companies will look to conventional risk management methods—in particular, classic risk assessments (aka "list management") and insurance coverage—to try to mitigate or transfer cyber risk. In our view, the results of managing cyber risk, like any other operational or business risk, will be limited. Cyber is proving itself to be the ultimate enterprise risk, encompassing not only information technology (IT), but also risks involving vendors (including cloud service providers), people, legal questions, and reputation, all while moving with stealth and a velocity that is extremely difficult to cope with.

What often flies under the radar is the risk posed to companies that are not, in fact, the direct target of cyberattacks: who could have predicted that an attack targeting Ukraine would simultaneously affect global shipping, a pharmaceutical company in the United States, and a chocolate factory in Australia? This type of risk event was unprecedented until the release of NotPetya on June 27, 2017.

Although NotPetya occurred almost three years ago, it takes time for the full impact of these events and the lessons learned to emerge. In particular, Danish shipper Maersk's experience stands out. During the World Economic Forum in Davos, Maersk chair Jim Hagemann Snabe estimated that NotPetya cost the company between $250 million and $300 million.[1]

A major theme in risk and security circles is cyber resilience, advocating some combination of awareness, risk assessments, controls frameworks, business continuity planning, etc. However, current approaches for cyber resilience typically assume that an organization will function in a crisis like it does during business as usual. But as most risk events highlight, this is seldom the case. All too often contingency plans, personnel, and controls do not perform well, if it all, under unexpected or extreme stress.

The attack on Maersk is a shining example of the law of unintended consequences when it comes to cyber. NotPetya's impact on the shipping giant perfectly illustrates the "Three R's" of complex risks like cyber: robustness, resiliency, and redundancy.

- **Robustness** asks the question: can my system maintain its basic functionality under duress?
- **Resilience** asks the questions: can my system adapt to shocks by changing its operations without losing function; and, how dynamic are my core activities?
- **Redundancy** asks the question: are there parallel components and functions that can replace other components and functions that fail?

In this article, we will view Maersk's experience and response, through the lens of the "Three R's." We believe this framework provides a more thoughtful and realistic approach to understanding the complexity of a cyberattack. For a detailed exposé on NotPetya, refer to Andy Greenberg's article in Wired magazine.[2]

We will not recount the entire NotPetya attack in detail here; rather, we wish to highlight key themes from the risk event; apply the "Three R's" to Maersk's response; and then conclude with event takeaways.

[1] Olenick, D. (January 26, 2018). NotPetya attack totally destroyed Maersk's computer network: Chairman. Cyber Risk Alliance. Retrieved March 4, 2020, from https://www.scmagazine.com/home/security-news/ransomware/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/.

[2] Greenberg, A. (August 22, 2018). The untold story of NotPetya, the most devastating cyberattack in history. Wired. Retrieved March 4, 2020, from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/?verso=true.

A glossary of key cyber risks, as seen through the lens of NotPetya

GEOPOLITICAL RISK AND STATE ACTORS

On February 22, 2014, Ukraine experienced a fundamental change in government often referred to as the Euromaidan revolution, ushering in a pro-Western government. Five days later, Russian troops seized strategic sites throughout Crimea. On March 16, Crimea held a status referendum and was then incorporated into Russia two days later. That month, fighting broke out between the Ukrainian government and separatists in the Donbass and Luhansk regions, which remain effectively autonomous today.

With this backdrop, it is believed that the NotPetya worm[3] was developed by hackers from Russia's military intelligence agency GRU to target Ukrainian critical infrastructure. If true, the attack demonstrates the effectiveness of the state actor threat vector whose capabilities significantly exceed traditional threats such as criminal organizations or hackers.

DECEPTION

While NotPetya initially seemed like ransomware, that was just a facade. It was actually a sophisticated piece of malware designed to destroy systems. Paying the ransom of $300 worth of Bitcoin did not lead to the decryption of files, reinforcing the view that NotPetya was a state-sponsored attack as opposed to a cybercrime.

GLOBAL INTERCONNECTEDNESS

The NotPetya attack demonstrated how fragile modern infrastructure has become due to communications interconnectedness. Within Ukraine, the worm is reported to have knocked out no less than six power companies, two airports, and over 22 banks, ATMs, and credit card payment systems, as well as more than four hospitals and several government agencies. Ten percent of all computers in Ukraine were wiped clean. Organizations ranging from corporations to government agencies had never seen this level of disruption and were not appropriately prepared.

In a matter of hours after NotPetya was deployed, the malware spread to companies across the world. With a large number of global companies operating in Ukraine, the worm was not only able to infect the intended targets, but also propagated to endpoints outside of Ukraine, including the pharmaceutical company Merck, a chocolate company in Tasmania, and, most importantly, the largest shipper in the world—A.P. Moller-Maersk Group.

Maersk handles 20% of all goods on the busiest shipping routes in the world. It operates in over 130 countries, servicing 76 ports including Odessa (a major transport hub in Ukraine). Given the company's vital role in global shipping, the economy of many countries rely, in part, on its services.[4]

UNKNOWN UNKNOWNS

The means by which the GRU allegedly deployed NotPetya is a classic "unknown unknown" problem for Maersk, namely an event or outcome that is impossible to predict. M.E. Doc, a popular Ukrainian tax software similar to Turbo Tax in the United States, was exploited to propagate the worm. Tax software is a particularly clever delivery vehicle for a discrete, sophisticated cyberattack: tax returns must be prepared annually and it could be reasonably assumed only Ukrainian entities would use local software to prepare their tax returns. Given its nondescript, innocuous nature, tax software is unlikely to be perceived as a threat, yet it provided the attackers with a backdoor into thousands of personal computers in Ukraine.[5]

PEOPLE

When it comes to securing a computer system, people are typically the weakest link. From unauthorized downloads to falling for phishing attacks, it is virtually guaranteed that attackers will be able to gain access to a company's computer system through exploiting human nature. A study by FAU found that 56% of email recipients and roughly 40% of Facebook users clicked on a link from an unknown sender. Large companies with global reach are particularly at risk given the sheer number of employees with access to their networks and differing global norms when it comes to the culture of cyber hygiene.[6]

At first glance, one would anticipate that an attack using the M.E. Doc software would be more or less localized to Ukraine because preparing tax returns is focused on a particular jurisdiction. This was not the case. NotPetya's entry into Maersk's system could not have been simpler. Reports say that a local finance executive asked that M.E. Doc be loaded onto that person's computer. Although there was a legitimate business need, this request should have been evaluated within the context of cyber hygiene policy. Yet, as with many firms, the executive request was honored and done so without most likely creating an information security exception. Human behavior, including the desire for convenience by the executive and deference to authority by IT, allowed for NotPetya to directly enter Maersk's systems.

---

[3] A worm is a self-contained program that does not need a host and self-propagates. This contrasts with a virus, which requires a host program and human intervention to run an infected file.

[4] See the Maersk website at https://www.maersk.com/.

[5] National Cyber Awareness System (July 2017). Alert (TA17-181A): Petya Ransomware. Retrieved March 4, 2020, from https://www.us-cert.gov/ncas/alerts/TA17-181A.

[6] FAU (August 25, 2016). One in two users click on links from unknown senders. News release. Retrieved March 4, 2020, from https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders/.

TIGHT COUPLING

Maersk's computer network was "tightly coupled," meaning its hardware and software components were highly interconnected and dependent on each other. Once the worm entered the Odessa office, it spread and shut down Maersk's operations globally.

Second- and third-order effects: Maersk's computer system was shut down for 10 days. Not only did this prevent Maersk from booking new shipments, but also its current shipments were unable to leave port. Cranes were halted and containers could not be transferred from ship to ground transportation. This was unprecedented in the history of shipping and the attack happened to the world's leading shipper.

Applying the lenses of robustness, resilience, and redundancy

We have broken down the ways in which NotPetya affected Maersk, demonstrating the complexity of cyber and the inability to predict risk based on past events. How the attack manifested itself was a classic case of the interaction of people, processes, and technology, which is often referred to as operational risk. It would be unreasonable to expect that Maersk could have predicted this specific event. Rather, the question we should ask is: how could the "Three R's" have helped Maersk better understand its cyber exposure before an extreme event like NotPetya?

Robustness requires that a system maintain its basic functionality under duress. Without a working computer system, Maersk's operations were seen to grind to a halt. This type of impact often indicates that a company lacked effective defenses to detect and quarantine the malware while the interconnected design of the company's IT infrastructure allowed the worm to gain access to virtually all of its infrastructure worldwide. While this level of connectedness makes sense from an operating efficiency view, it also makes companies ripe for rapid and uncontrolled malware propagation. Networks and operations that are not designed to compartmentalize an attack struggle to cope with and contain the initial shock.

Resilience is the ability of a system to adapt to shocks by changing its operations without losing core operational function. The frenzied response by Maersk indicates that it was unprepared for such a devastating attack. This type of response often means that a company's business continuity or disaster recovery plan made fundamental assumptions such as that key components within the IT infrastructure would remain intact for recovery. In the case of Maersk, the shipping company was able to recover in 10 days, not because of innate cyber resiliency, but because of sheer luck. According to Greenberg's article, only one out of Maersk's 150 or so domain controllers (i.e., servers that respond to security authentication requests) was found to have survived the attack. It was located in a remote office in Ghana and survived only due to a coincidental power outage before the attack, disconnecting the computer from the network. Without a power outage in Africa, Maersk would have been compelled to rebuild its entire system from scratch.[7]

Maersk's IT and shipping system could not adapt to the attack while its core activities, such as loading and unloading ships in port, were paralyzed: without the electronic manifests, everything ground to a halt, disrupting the global supply chain. Maersk set up ad hoc WhatsApp groups to try to move cargo.

Redundancy is the state where there are parallel components and functions that can replace the components and functions that fail. A company with redundant protocol as part of its cyber risk mitigation strategy would not have needed the good fortune of one of its domain controllers offline. The principle of redundancy would include the assumption that all the operational domain controllers could fail. Even with the surviving copy of Maersk's domain controllers, the company still had to purchase and reinstall more than 4,000 servers, 45,000 personal computers, and 2,500 applications. Two hundred Deloitte consultants flooded the recovery center in Maidenhead, England, frantically working with about 400 Maersk employees to facilitate the recovery. Maersk did not have any surviving parallel backup systems to replace damaged infrastructure. Rather, it had to buy new equipment and hire outside help to restore the network.

Lessons learned

Every major company is a potential target in cyberspace. However, no one imagined a state actor would launch such a destructive attack that significantly impeded the world's largest shipper. Given NotPetya's entry point through Ukrainian tax software, it is apparent that it was not specifically designed to target Maersk, but rather Ukraine. In all likelihood, Maersk was probably collateral damage indicative of the 21st century's asymmetric and non-kinetic battlefield.

Without a clear picture of the complex web of cyber risks and controls, Maersk likely made many important business decisions without fully considering the implications for its cyber exposure. The assumed decision to have the networks from Maersk's various offices connect is a logical business decision from the perspective of adding speed and transparency to operations.

[7] Greenberg, The untold story of NotPetya, op cit.

However, a large centralized connected network means that a single cyberattack can cripple an organization.

More likely than not, NotPetya's developers simply did not care about the unintended consequences of the malware's non-Ukrainian casualties. There are a number of key takeaways from Maersk's experience with NotPetya.

- **Law of unintended consequences**: It is doubtful that Maersk was a primary or secondary target of the malware. Rather, the company was collateral damage in what is believed to be a nonconventional action by Russia to harm Ukraine.
- **Normalcy bias**: Extreme events are underestimated while it is believed systems will function as assumed. It is highly unlikely that anyone at Maersk imagined that its entire shipping network would be immobilized by an obscure attack via the Odessa office. Clearly, its systems and any contingency plans failed under duress. Firms must use data-driven analysis to challenge ingrained views of the threat landscape. By understanding how their risks, controls, infrastructure, and people are connected, firms can model previously unpredictable risks. If Maersk had truly mapped its environment, and tested its current assumptions with internal and external data, it could have seen that its global and connected network structure, along with potential deference to seniority, created a significant cyber vulnerability.
- **Propagation velocity**: The worm spread globally within hours. The lightning speed that the malware travelled, compounded by interconnectedness, made it virtually impossible to stop in real-time.
- **Cascading failure**: The worm spread throughout Ukraine, taking down national infrastructure from banks to hospitals to payment systems. Multiple endpoints facilitated the cascade across the globe. Unlike natural disasters or blackouts, it is virtually impossible to predict how a cyberattack will cascade.
- **Recovery serendipity**: Although Maersk was back online in 10 days, it was lucky. Companies should not be complacent about surviving "near death" experiences. Companies that fail to recognize themselves as potential targets or collateral damage of a state actor attack are likely to be unprepared and far less lucky than Maersk. Even more concerning, there is little reason to believe that cybersecurity at other large corporations is any better.

Cybersecurity is not enough; companies need to first understand the interconnected landscape of threats and defenses that define their holistic cyber risk profiles. Relying on compliance assessments, risk frameworks, and control checklists has proven lacking. Understanding the nonlinear relationships within its complex operating environment would have exposed Maersk's fundamental cyber vulnerabilities while recovery capabilities were limited. Applying the principles of robustness, resiliency, and redundancy to cyber and enterprise risk management programs will enhance companies' capabilities to cope with future attacks.

Milliman

CONTACT

Chris Harner
chris.harner@milliman.com

Chris Beck
chris.beck@milliman.com

Blake Fleisher
blake.fleisher@milliman.com