KPMG wortell

A decade of ransomware

From scareware to global threat

Contents

Executive summary

A decade of ransomware

> **“No matter what industry you’re in, you must operate with the mindset that you are a target and take action to ensure that your people are aware and equipped.”**

So, how can organisations prepare for an unpredictable and increasingly hostile cyber landscape? The answer lies in a strategic, collaborative approach that prioritizes both proactive and reactive measures.

1. Secure your foundations. Basic cybersecurity hygiene, like keeping software updated, enforcing multi-factor authentication, and securing cloud environments, remains the first line of defense. Regular vulnerability assessments and robust access controls are essential to prevent attackers from exploiting weak links.

2. Prepare for the inevitable. Even with the best defenses, breaches can happen. Incident response plans need to be well-rehearsed, ensuring your team can act quickly to contain damage and recover operations. Investing in Managed eXtended Detection and Response (MxDR) services can provide 24/7 monitoring and immediate threat response.

3. Future-proof your security. The next wave of threats will be driven by technologies like artificial intelligence and quantum computing. AI could enable attackers to customize phishing schemes in real-time, while quantum advancements may render current encryption obsolete. Organisations must start exploring quantum-resistant cryptographic solutions and adaptive security measures now.

4. Collaborate to stay ahead. The global nature of ransomware demands a unified response. Governments, industries, and technology providers must work together to create standardized regulations, share intelligence, and build public-private partnerships. Initiatives like the “No More Ransom” project demonstrate the power of collective action in mitigating threats.

A call to action for leadership

Ransomware is not just a technological issue; it’s a leadership challenge. CEOs, board members, and policymakers must champion a culture of cyber resilience across their organisations and sectors. This means not only investing in advanced technologies but also fostering a workforce that understands the role every individual plays in protecting digital assets.

As the digital and physical worlds grow more intertwined, and geopolitical risks increase, the impact of inaction is too great to ignore. Cyber resilience is no longer optional, it’s a strategic imperative.

Organisations that prioritize security, collaboration, and innovation will not only survive but thrive in an era of constant cyber disruption.

The future of your business, your industry, and even your nation’s security depends on the decisions made today.

Are you ready to lead the charge?

Loss of data & trust

Michael sat at his desk to close out the financial year. The quiet hum of his laptop was the only sound in the office. Then, without warning, his screen went black, replaced by a single, chilling message:

“ Your company’s financial data has been encrypted. Pay $500.000 in Bitcoin to unlock it.“

A wave of panic hit him. His mind raced as he stared at the screen, trying to make sense of it. All essential financial records, sensitive data, and company files were being held hostage by an unseen attacker, compromising the security and integrity of his business.

This is the unsettling world of ransomware, a malicious software that silently infiltrates your computer, often through an innocent-looking email or a compromised website. Disguised as a legitimate attachment or link, it slips past your defenses when you click unknowingly. Once inside, it swiftly encrypts your files, making them inaccessible and unusable.

The attackers leverage advanced encryption algorithms, effectively putting your data in a digital safe to which only they have the key. They count on your desperation, betting that you'll pay the ransom to regain access. To add pressure, they might threaten to delete your files permanently or increase the ransom if you don't comply quickly.

Behind the scenes, these cybercriminals operate anonymously, usually demanding payment in untraceable cryptocurrencies. They prey on individuals and organisations alike, causing billions in damages worldwide.

The aftermath is not just about the ransom paid; it's the loss of valuable data, trust, and peace of mind.

Trust as a business enabler

Today, organisations have a laser-sharp focus on trust. Trust in your business is the currency that resonates with all stakeholders – employees, regulators, investors, analysts, communities, and beyond. Trust is today’s ultimate business enabler, positioning organisations to innovate, build a stronger brand, and grow responsibly.

With ransomware causing fear, uncertainty, and financial loss across every sector, it is easy to think of it as just another form of cybercrime, one that targets businesses or governments and demands a ransom to restore access to critical data.

Individuals, businesses, and institutions are forced to confront the reality that the systems they rely on can be corrupted, and that their most sensitive information can be used as leverage against them in various forms.

Because we are increasingly focused on a trust-based model, the damage isn't just the immediate disruption or financial hit, but also the long-lasting impact on reputation, relationships, and the trust organisations once had as a brand.

Historical context

“By the early 2010s, ransomware had exploded into a full-blown epidemic”

"When I was at school, computers were tools, not the lifeblood of our daily existence," says Maarten Goet, CTO of Wortell. "A ransomware attack might have disrupted a few files, but it didn’t paralyze entire systems. Today, the distinction between physical and digital life is blurred, and every attack on digital infrastructure has the potential to cause far more damage—even chaos.“

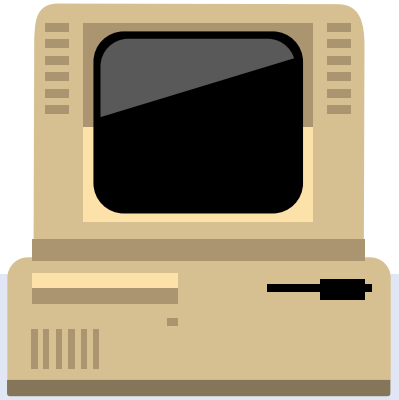
"I believe it was 1989, and this was something entirely new. Computers were still relatively isolated tools, used mostly in specific industries or by hobbyists, but the idea of using them to extort people—that was unheard of. When the AIDS Trojan hit, with that floppy disk labeled 'AIDS Information—Introductory Diskette,' it was a shock to the system. People were curious, so they inserted the disk, thinking they’d get some useful information. Days later, their screens displayed a ransom demand—$189 to a P.O. box in Panama. Their files were locked behind encryption, which was completely novel at the time.“

"As the '90s came, the internet started connecting more people and machines globally, and it opened the door for cybercriminals to expand their reach. By 2004, GPCode came onto the scene, using advanced encryption to lock people out of their files. It wasn’t just a prank or a small-scale attack anymore—this was the beginning of a much more dangerous trend. Early versions were cracked by savvy programmers, but GPCode evolved, each iteration more formidable than the last. The stakes were escalating.”

"By 2006, things had become even more complicated. That’s when Archiveus, a new computer virus designed for extortion, appeared—and it was unlike anything before. Instead of demanding cash, attackers forced victims to purchase products from specific online pharmacies to unlock their "My Documents" folder. It was bizarre and alarming. Ransomware had evolved from a mere nuisance into a sophisticated extortion tool. It wasn’t just about money anymore—it was about exploiting digital systems in increasingly creative and malicious ways.”

"Three major forces were converging behind the scenes to supercharge ransomware’s rise. First, advanced encryption methods gave hackers the lock—making it nearly impossible for victims to regain access without paying up. Second, the rapid expansion of global internet access meant there was an enormous pool of potential targets.”

“Suddenly, anyone with an internet connection was vulnerable, and anonymous payment systems like cryptocurrencies provided attackers an untraceable way to collect ransoms. By the early 2010s, ransomware had exploded into a full-blown epidemic. Ransomware-as-a-Service popped up on the dark web, enabling even novices to launch attacks easily. The digital underworld thrived, leaving no one—businesses, governments, or individuals—safe. It's a relentless race between those who seek to exploit and those who strive to protect—a high-tech thriller playing out on the world's digital stage.”



Evolution of ransomware

Between 2013 and 2015, the world of cybersecurity changed dramatically. Before this, cybercriminals mainly used scareware—malicious programs that tricked people with fake warnings, trying to scare them into buying fake antivirus software or paying fake fines. These scareware attacks were annoying, but they didn't cause serious damage to people's data.

As people became more aware and security tools got better, scareware became less effective. So, cybercriminals started using more dangerous methods.

One of the biggest changes was the rise of encryption-based ransomware. Unlike scareware, this new type of ransomware used strong encryption to lock people's files, making them impossible to access without a special key. The game-changer came in 2013 with the arrival of CryptoLocker.

This virus spread mostly through malicious email attachments and botnets (like Gameover and ZeuS) and infected thousands of computers worldwide. Once it took hold, CryptoLocker encrypted many types of files and demanded a ransom—often paid in Bitcoin—to unlock them. The encryption was so strong that victims had no choice but to pay or lose their files forever.

In May 2017, the WannaCry ransomware attack took advantage of a weakness in Microsoft Windows called EternalBlue, a tool reportedly created by the U.S. National Security Agency (NSA) and leaked by hackers. The attack affected over 200,000 systems in more than 150 countries, disrupting hospitals, telecoms, and businesses. The UK's National Health Service (NHS) was hit hard, leading to canceled surgeries and ambulances being redirected. WannaCry highlighted the risks of unpatched software and showed how ransomware could cause widespread damage and chaos.

In June 2017, just a month after WannaCry, the NotPetya ransomware outbreak raised even more alarm. At first, it seemed like another ransomware attack demanding payment to unlock files. However, it was later found to be a type of malware meant to destroy data rather than make money. Like WannaCry, NotPetya used the EternalBlue flaw to spread quickly across networks.

While it mainly targeted Ukraine's government, banks, and energy companies, it also affected global companies like Maersk and Merck. The attack caused billions in damages, highlighting the severe impact of cyberattacks on the global economy.

2013-2015

The emergence of modern ransomware

2016 -2017

Global ransomware epidemics

Evolution of ransomware

Wake-up call

The WannaCry and NotPetya attacks exposed serious gaps in cybersecurity readiness and international coordination. These attacks demonstrated how cyber weapons, once leaked or stolen, could be repurposed by malicious actors to launch large-scale attacks with real-world consequences.

These incidents were a wake-up call, pushing organisations to rethink their approach to security. Key lessons included the importance of regular software updates, reliable backup systems, and strong incident response plans to reduce the risk of future attacks. Investing in these measures was no longer optional but critical for protecting operations and reputation.

2018-2019

Professionalization and Ransomware-as-a-Service (RaaS)

During 2018-2019, ransomware attacks became more organized with the rise of Ransomware-as-a-Service (RaaS).

Cybercriminals began running their operations like businesses, hiring developers, negotiators, and even customer support teams to deal with victims. This led to more advanced attacks, focusing on large organisations capable of paying bigger ransoms. RaaS allowed individuals with limited technical expertise to launch ransomware attacks by providing them with ready-made malware and infrastructure.

In exchange for a subscription fee or a share of the profits, RaaS operators offered continuous updates, encryption algorithms, and decryption keys. This model lowered the barrier to entry, resulting in a surge of new attackers entering the ransomware space. High-profile RaaS offerings like GandCrab became notorious for their widespread use and profitability.

The growth of affiliate programs further amplified the reach of ransomware campaigns. Ransomware developers recruited affiliates to distribute their malware, offering them a significant portion of the ransom payments—sometimes up to 70-80%. These affiliates utilized various methods to infect victims, including phishing emails, exploit kits, and Remote Desktop Protocol (RDP) attacks.

2016 -2017

Double Extortion and Targeted Attacks

The affiliate model created a mutually beneficial relationship: developers expanded their distribution network without directly engaging in attacks, while affiliates profited from successful infections.

During the years 2020 and 2021 cybercriminals adopted a strategy known as double extortion. This approach involved not only encrypting the victim's data but also stealing sensitive information before encryption.

By threatening to publicly release the stolen data, attackers added additional pressure on victims to pay the ransom.

Evolution of ransomware

Strategic targets

Double extortion proofed to be highly effective, as the threat of reputational damage and legal fallout from a data breach often outweighed the disruption caused by encryption alone.

By combining data theft with encryption, attackers shifted to targeting high-value organisations. They conducted detailed reconnaissance to find critical assets and used advanced persistent threats (APTs) to stay hidden in networks. Stolen data often included sensitive business information, customer details, and intellectual property, raising the stakes for victims.

This marked a shift toward more strategic, targeted attacks focused on maximizing impact.

One of the most notable incidents illustrating this trend was the Colonial Pipeline attack in May 2021. Operated by the DarkSide ransomware group, it forced the shutdown of one of the largest fuel pipelines in the United States, causing widespread fuel shortages along the East Coast.

The attackers encrypted the company's data and exfiltrated nearly 100 GB of sensitive information. The incident exposed vulnerabilities in critical infrastructure and highlighted the national security risks of ransomware attacks.

2022-2023

Emerging trends

the past years cybercriminals adopted even more aggressive tactics such as triple extortion, adding a third layer of pressure. Attackers not only encrypt and exfiltrate data but also target the victim's customers, partners, or other stakeholders with threats or Distributed Denial-of-Service (DDoS) attacks. This multi-pronged strategy aims to maximize leverage over the primary victim by causing broader disruption and reputational damage, thereby increasing the likelihood of ransom payment.

Another significant trend was the targeting of cloud services. As more organisations migrated their operations to cloud-based platforms, ransomware groups started exploiting cloud vulnerabilities. By compromising cloud service providers or exploiting misconfigurations in cloud settings, they could deploy ransomware at scale, affecting multiple clients simultaneously. This shift underscored the challenges of securing cloud environments and the importance of robust cloud security practices.

Ransomware operators began focusing on supply chain attacks, targeting third-party vendors and suppliers instead of organisations directly. By compromising one supplier, they could access the networks of multiple companies. The Kaseya VSA attack showed how ransomware delivered through a software update could impact hundreds of businesses globally. These incidents highlighted the need for strong security across entire supply chains, not just individual organisations.

Impact analysis

Operational disruption

“The ransomware attack on a German hospital led to redirection of an emergency patient, who later died”

Over the past decade, ransomware attacks have increasingly caused significant operational disruptions, particularly within critical infrastructure sectors such as healthcare, energy, and transportation. These sectors are vital to societal functioning, and interruptions can have cascading effects on public safety and the economy.

The operational halts resulting from ransomware attacks underscore the severity of the threat and the necessity for robust cybersecurity measures.

In the healthcare sector, ransomware has jeopardized patient care and safety. A prominent example is the 2017 WannaCry attack, which severely impacted the United Kingdom's National Health Service (NHS). The ransomware encrypted patient records and medical devices, forcing hospitals to cancel thousands of appointments and divert emergency cases to other facilities. This operational standstill not only strained medical resources but also delayed critical treatments. In another case, a 2020 ransomware attack on a German hospital led to the redirection of an emergency patient, who later died, marking one of the first reported fatalities indirectly linked to a cyberattack (source: Microsoft Digital Defense Report 2020).

The energy sector has also been a target for ransomware, with attacks causing substantial operational disruptions. In 2021, the Colonial Pipeline, which supplies nearly half of the U.S. East Coast's fuel, fell victim to a ransomware attack. The company pre-emptively shut down its pipeline operations to contain the threat, leading to fuel shortages, price hikes, and panic buying across several states. This incident highlighted the vulnerability of critical energy infrastructure and prompted federal responses to improve cybersecurity defenses in the industry.

Transportation systems have faced similar threats, with ransomware attacks disrupting global logistics and supply chains. In 2017, shipping giant Maersk experienced a ransomware attack that crippled its IT systems worldwide. The company had to halt operations at 76 port terminals across four continents, resorting to manual processes to keep goods moving.

This operational halt not only cost Maersk up to $300 million (source: Microsoft Digital Defense Report 2020) but also caused significant delays in the global shipping industry, affecting countless businesses and consumers reliant on timely deliveries.

Societal and psychological effects

Ransomware attacks deeply affect societal perceptions and psychological well-being. Public trust in digital infrastructures and essential services has been eroded as ransomware incidents become more frequent and severe.

Impact analysis

> **“Maersk had to halt operations at 76 port terminals across four continents, costing up to $300 million”**

High-profile attacks on hospitals, educational institutions, and government agencies have not only disrupted services but also shaken confidence in the ability of these institutions to safeguard sensitive information and maintain uninterrupted operations.

Fear and anxiety have become prevalent among the public due to the constant widespread media coverage of cyber attacks.

Individuals worry about the security of their personal data, the reliability of critical services, and the potential for identity theft or financial loss. This pervasive fear can lead to increased stress and a sense of helplessness, as people feel they have little control over these unseen threats.

Black-out

Governments, like individuals, are becoming increasingly alert and are preparing both themselves and their citizens for potential widespread chaos. A recent example is a nationwide blackout simulation on Dutch television, supported by the government, aimed at raising awareness among civilians. The program posed a chilling question: what if the Netherlands, or parts of it, lost power due to a cyberattack on a national grid operator? While the scenario may still feel far-fetched, it is more plausible than ever. Viewers were immersed in a fictional narrative grounded in a highly realistic and concerning possibility.

Governments and organisations that proactively communicate their commitment to cybersecurity can enhance confidence and differentiate themselves in the geopolitical landscape or market. It is this shift in expectations that compelled us to prioritize cyber resilience not only to protect our assets but also to maintain and build trust.

Impact analysis

Hiding from security tools

Ransomware changes how it looks or operates (called obfuscation) to avoid detection. Some types don't even leave files on the computer, staying hidden in the memory instead. It can detect if it's being analyzed by cybersecurity experts and won't activate unless it's in a real environment. It may even delay launching to make detection harder.

Phishing e-mails

Attackers send fake emails that look like they're from trusted sources, such as banks, colleagues, or government agencies. These emails trick people into clicking bad links or opening infected attachments, giving hackers access to the system.

Remote desktop hacks

Remote Desktop Protocol (RDP) lets people access computers from anywhere. If it's not secured properly, attackers can guess weak passwords or use stolen login details to break in, spreading ransomware across the network.

Unpatched software

Hackers take advantage of outdated software with known weaknesses. If systems aren't updated regularly, these gaps allow attackers to sneak in without needing any action from the user.

Payment and negotiation strategies

The payment and negotiation landscape of ransomware attacks has evolved significantly. One of the most notable changes is the widespread adoption of cryptocurrencies, particularly Bitcoin, as the primary means for ransom payments. Cryptocurrencies offer a level of anonymity and decentralization that make them attractive to cybercriminals, allowing them to receive funds without easy traceability by law enforcement agencies. The use of cryptocurrencies has facilitated the growth of ransomware by simplifying the payment process and reducing the risk of interception or identification.

Ransom demands have also evolved in terms of sophistication and scale. Early ransomware attacks often targeted individual users with relatively small ransom amounts, typically a few hundred dollars. However, modern ransomware campaigns frequently focus on larger organisations, demanding payments that can reach millions of dollars. Attackers conduct thorough research on their targets to set ransom amounts that are significant yet potentially affordable, increasing the likelihood of payment. Additionally, some ransomware groups employ double extortion tactics, not only encrypting data but also threatening to publicly release sensitive information if the ransom is not paid.

Negotiation tactics have become a critical aspect of the ransomware ecosystem. Cybercriminals now often provide professionalized communication channels, such as dedicated negotiation websites or chat portals, to facilitate discussions with victims. They may offer proof of decryption capabilities by decrypting sample files and may even provide customer support to assist victims in making payments. Some attackers employ pressure tactics, such as countdown timers or increasing ransom amounts over time, to compel quick payment. On the other side, organisations are increasingly engaging cybersecurity professionals and negotiators to handle communications with attackers, aiming to reduce ransom amounts or buy time to implement recovery strategies.

“Attackers conduct thorough research on their targets to set ransom amounts that are significant yet potentially affordable, increasing the likelyhood of payment”

Ransomware economy

Ransomware-as-a-Service (RaaS)

“In a typical revenue-sharing model, affiliates receive up to 70-80% of the ransom payments”

Ransomware-as-a-Service (RaaS) is a pivotal component in the ransomware ecosystem. RaaS operates similarly to legitimate software-as-a-service models but within the cybercriminal underworld. It enables individuals with limited technical expertise to launch ransomware attacks by providing them with ready-made ransomware tools. This democratization of ransomware has significantly lowered the barrier to entry for cybercriminal activities, leading to a surge in ransomware incidents globally.

The operation structure of RaaS involves a symbiotic relationship between developers and affiliates. Developers are skilled programmers who create sophisticated ransomware strains and maintain the underlying infrastructure. They handle tasks such as coding the ransomware, updating it to bypass security measures, and managing payment systems for ransom collection, often using cryptocurrencies for anonymity. Affiliates, on the other hand, are responsible for distributing the ransomware to potential victims. They employ various tactics like phishing emails, malicious downloads, or exploiting network vulnerabilities to infiltrate target systems.

The business models within RaaS are primarily based on revenue-sharing agreements or subscription fees. In a typical revenue-sharing model, affiliates receive a significant percentage of the ransom payments—sometimes up to 70-80%—while the developers take the remaining share (source: Microsoft Digital Defense Report 2022). This incentivizes affiliates to maximize their distribution efforts. Alternatively, some RaaS platforms operate on a subscription basis, where affiliates pay a regular fee to access the ransomware tools and support services. This model provides a steady income for developers and may include tiered packages offering different levels of features and support. The flexibility and profitability of these business models have contributed to the proliferation of RaaS, making ransomware attacks more frequent and sophisticated.

Ransomware economy

> **“State-sponsored actors and cybercriminal groups are two prominent forces in the cyber threat landscape”**

Cryptocurrencies and the Dark Web

Cryptocurrencies and the Dark Web have become essential components of the ransomware landscape. Cryptocurrencies like Bitcoin and Monero offer a level of anonymity and decentralization absent in traditional financial systems, making them the preferred medium for ransom payments. These digital currencies enable cybercriminals to receive payments from victims without revealing their identities or locations, thereby minimizing the risk of detection and legal repercussions. The irreversible and pseudonymous nature of cryptocurrency transactions complicates efforts by law enforcement to trace and recover ransom funds.

The Dark Web serves as a hidden network where cybercriminals can operate with relative impunity. Accessible through specialized software like Tor, it hosts numerous marketplaces and forums dedicated to illicit activities, including the buying and selling of ransomware tools.

These platforms allow ransomware developers to market their malicious software and offer services such as customer support, updates, and customization. Affiliates and aspiring cybercriminals can easily acquire these tools, often through straightforward transactions facilitated by cryptocurrencies, further fueling the proliferation of ransomware attacks.

Together, cryptocurrencies and the Dark Web have facilitated anonymous transactions and created a thriving marketplace for ransomware. This synergy has lowered the barriers to entry for cybercriminals and expanded the ransomware ecosystem. The ability to anonymously monetize attacks and access sophisticated tools has not only increased the frequency of ransomware incidents but also their sophistication and global reach.

State-sponsored actors versus cybercriminal groups

State-sponsored actors and cybercriminal groups are two prominent forces in the cyber threat landscape, each driven by different motivations and equipped with varying resources. State-sponsored actors are typically linked to national governments and focus on advancing geopolitical objectives, such as intelligence gathering, surveillance, or disrupting the operations of other nations. In contrast, cybercriminal groups are generally motivated by financial gain, engaging in activities like ransomware attacks, fraud, and data theft to profit illegally. State-sponsored actors have access to substantial resources, including advanced technologies, significant funding, and intelligence assets. They often conduct sophisticated, long-term campaigns known as Advanced Persistent Threats (APTs), targeting government agencies, critical infrastructure, and key industries. Their operations are characterized by stealth, persistence, and the use of zero-day vulnerabilities—previously unknown security flaws that are difficult to defend against. Notable groups include NOBELIUM (also known as APT29 or Cozy Bear), which has been attributed to Russia and is known for its espionage activities against political organisations and vaccine research facilities.

Another example is China's BARIUM (also known as APT41), involved in both state-sponsored espionage and financially motivated attacks.

Cybercriminal groups, on the other hand, operate primarily for personal enrichment and are often more opportunistic in their targeting. They may lack the extensive resources of state actors but compensate with agility and a willingness to exploit widely known vulnerabilities.

Ransomware economy

These groups frequently utilize the ransomware-as-a-service (RaaS) platforms and other tools readily available on the Dark Web.

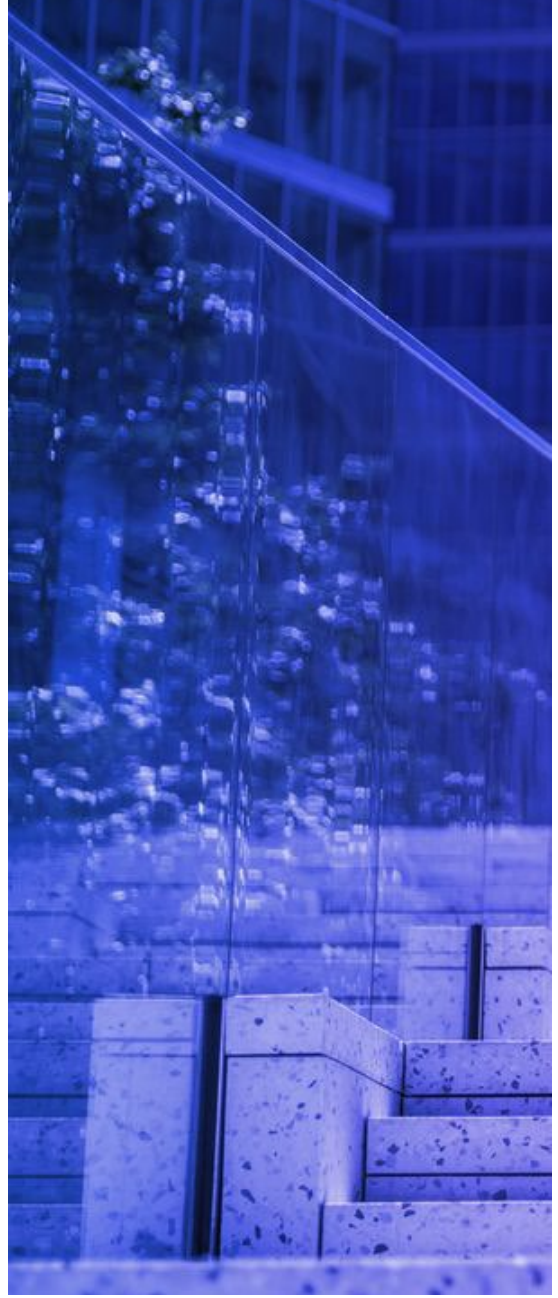
Cybercriminal groups like Revil, are responsible for high-profile ransomware attacks demanding multi-million-dollar ransoms from companies worldwide.

Another group, DarkSide, gained notoriety for its attack on the Colonial Pipeline in 2021, disrupting fuel supplies in the Eastern United States.

Attribution in cyberattacks is notoriously challenging due to tactics like spoofing and the use of anonymizing technologies. However, cybersecurity firms and government agencies employ advanced forensic methods to trace activities back to specific groups.

Understanding the motivations and resources of these actors is crucial for developing effective defense strategies. State-sponsored actors require robust, intelligence-driven security measures due to their advanced capabilities and long-term focus. In contrast, defenses against cybercriminal groups often emphasize rapid patching of known vulnerabilities, employee training to prevent phishing attacks, and robust backup systems to mitigate ransomware threats.

“Cybercriminal groups like Revil, are responsible for high-profile ransomware attacks demanding multi-million-dollar ransoms from companies worldwide.”



Preventative measures

“Frameworks such as NIST offer guidelines and best practices”

It’s clear that preventative measures are more crucial than ever. One of the most critical steps in safeguarding against these attacks is implementing robust vulnerability management. Regularly updating and patching software systems reduces exploitable weaknesses that cybercriminals often target. Conducting frequent vulnerability assessments helps organisations identify and remediate security gaps before they can be leveraged in an attack.

In addition to technical defenses, employee training and awareness programs play a vital role in prevention. Human error remains one of the leading causes of successful ransomware infiltrations. By educating employees about phishing schemes, social engineering tactics, and safe online practices, organisations can significantly reduce the risk of inadvertent malware introduction. Regular training sessions and simulated cyberattack exercises can keep security protocols fresh in employees' minds and promote a culture of vigilance.

Implementing robust cybersecurity frameworks provides a structured approach to managing and mitigating ransomware risks. Frameworks such as the NIST Cybersecurity Framework or CIS offer guidelines and best practices for establishing a comprehensive security posture. Adopting these frameworks helps organisations create standardized policies and procedures, ensuring all aspects of cybersecurity—from prevention to response—are systematically addressed. This holistic approach not only enhances defense mechanisms but also facilitates compliance with regulatory requirements.

Detection and Response

The ability to detect and respond swiftly is essential for minimizing damage.

In other words, ‘Rapid Response’. A critical first step in this process is developing a robust incident response plan. This plan serves as a roadmap for organisations to follow when a ransomware incident occurs, outlining specific procedures for identifying the threat, containing its spread, eradicating malicious elements, and recovering affected systems. Regular drills and updates to the incident response plan ensure that all team members are familiar with their roles and can act decisively under pressure.

Incorporating Managed eXtended Detection and Response (MxDR) services can significantly enhance an organization's security posture. MDR providers offer specialized expertise and advanced technologies to monitor networks continuously, detect anomalies, and respond to threats in real-time. These services leverage artificial intelligence and machine learning to identify suspicious activities that might be missed by traditional security measures. By outsourcing detection and response capabilities to seasoned professionals, organisations gain access to cutting-edge resources and 24/7 support without the need for extensive in-house teams.

Defense mechanisms

Combining incident response planning with MDR services creates a comprehensive strategy against ransomware. While the incident response plan ensures internal readiness and coordination, MxDR services provide external support and advanced threat intelligence.

This dual approach enables organisations to not only react promptly to incidents but also to proactively identify and mitigate potential threats before they escalate. Together, these measures strengthen an organization's ability to withstand ransomware attacks and safeguard critical assets.

“Incorporating Managed Detection and Response (MDR) services can significantly enhance an organization’s security posture”

Rapid Response

Being prepared with a comprehensive rapid response plan can significantly minimize the time and resources required to address any occurring incidents.

Identification of evidence
Identify the areas where electronic indications and evidence can be found, taking into account locally available data sources and network structures with external data pools (e.g. cloud services). Focus investigation on all available data storage media – from laptops to Unix mainframes, from smart phones to tablet devices.

Preservation of evidence
All evidence must be inventoried and secured to preserve its integrity; the aim is to map the digital footprint in a way that is admissible as evidence in court. This can be best carried out a Forensic Technology laboratory. Locate deleted or hidden files (or fragments) and preserve evidence that the perpetrators believed to be untraceable. Neither the original data nor the systems are compromised or impaired in this process.

Analysis of evidence
With the use of powerful systems and tools, you can analyse the secured data in a laboratory environment according to case specific requirements and put the jigsaw together, enabling differentiated evidence management.

Presentation of evidence
Secured evidence (initially available only in electronic form) should be processed in accordance with formal legal requirements and presented in a way that can be used in court. Make sure the results are always clearly traceable, repeatable and transparent and take care of expert witness testimonies if required.

Defense mechanisms

Recovery strategies

Effective recovery strategies are crucial for organisations to bounce back swiftly after a ransomware attack, minimizing operational downtime and financial losses. A fundamental component of these strategies is implementing robust data backup and restoration practices. Regularly scheduled backups of critical data ensure that, in the event of an attack, information can be restored without yielding to ransom demands. It's essential to store backups in secure, immutable environments, preferably offsite or in the cloud, to prevent them from being compromised alongside primary systems. Additionally, periodically testing the restoration process verifies the integrity of backups and the organization's readiness to recover data when necessary.

Complementing data backups, comprehensive business continuity planning is vital for sustaining operations during and after a ransomware incident. A business continuity plan outlines the procedures and resources required to maintain essential functions, even when primary systems are disrupted. This includes identifying alternative workflows, designating key personnel responsibilities, and establishing communication protocols with stakeholders. By preparing for various disruption scenarios, organisations can reduce downtime, maintain customer trust, and ensure regulatory compliance.

Integrating data backup and restoration practices with business continuity planning creates a resilient defense against the lasting impacts of ransomware. While backups address the technical aspect of data recovery, business continuity plans focus on maintaining operational integrity. Together, they enable organisations to not only restore lost data but also to continue critical business functions with minimal interruption. Regular reviews and updates of these strategies are necessary to adapt to evolving threats and organizational changes, ensuring that recovery plans remain effective and aligned with best practices.

"In a significant move to enhance cybersecurity resilience for organisations across the Netherlands, KPMG and Wortell have announced a strategic partnership that combines their unique strengths for a unified approach to digital security. Wortell, a leading IT service provider, will spearhead the offering of a 24/7/365 Managed eXtended Detection and Response (Mx\DR) service to joint customers. This service ensures continuous monitoring and swift response to cyber threats, providing businesses with the confidence that their digital assets are protected around the clock, both from external attacks and internal vulnerabilities.

Complementing this, KPMG will bring its extensive expertise in advanced cybersecurity services to the partnership. By offering specialized solutions such as Incident Response, Forensics, and Red Teaming, KPMG will enable organisations to not only respond effectively to cyber incidents but also proactively identify and mitigate potential vulnerabilities. Their seasoned professionals are adept at navigating the complexities of cyber threats, ensuring that businesses can operate securely in an increasingly challenging digital landscape.

Together, KPMG and Wortell are crafting a comprehensive cybersecurity framework that leverages the strengths of both organisations. This "better together" story is about more than just a partnership; it's a commitment to providing unparalleled security services that address the full spectrum of cyber risks. By uniting continuous threat monitoring with advanced incident response and forensic capabilities, they are setting a new standard for cybersecurity, ensuring that organisations are well-protected today and prepared for the challenges of tomorrow."

"KPMG and Wortell strengthen cybersecurity in the Netherlands through strategic partnership"

International laws and policies

“In November 2021, international law enforcement agencies arrested multiple individuals associated with the Revil ransomware group”

Over the past decade, the surge in ransomware attacks has compelled a concerted global response from governments and international bodies. Globally a tsunami of “Digital Law” activities is noticed which calls for a step up for Legal and Regulatory actions. Recognizing that cyber threats transcend national borders, there has been a concerted effort to develop international laws and policies to combat cybercrime effectively.

This has led to the establishment of various legal frameworks aimed at harmonizing national laws, enhancing investigative capabilities, and fostering international cooperation. Focus of regulators is on regulating (big) Platforms/Tech, AI, Data and Cyber. Such along nine “themes”.

Globally, cybercrime legislation has evolved to address the complexities of ransomware and other cyber threats. A cornerstone in this effort is the Council of Europe's Budapest Convention on Cybercrime, the first international treaty designed to tackle internet and computer crimes by standardizing national laws and facilitating cross-border collaboration. Additionally, organisations like the United Nations are working towards formulating a comprehensive global cybercrime treaty to further unify international responses. Many countries have updated their national laws to criminalize ransomware activities explicitly, increase penalties, and provide law enforcement agencies with advanced tools for investigation and prosecution.

Despite these advancements, significant challenges persist in cross-border enforcement of cybercrime laws. Jurisdictional issues often arise when perpetrators operate from countries with different legal systems or less stringent cybercrime laws, making extradition and prosecution difficult. Differing legal definitions and procedural requirements can hinder mutual legal assistance and the execution of international warrants. Moreover, resource disparities mean that some nations lack the technical expertise or infrastructure to effectively participate in international enforcement efforts.

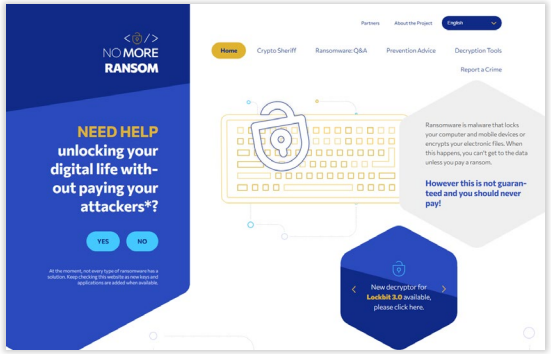
Government and law enforcement initiatives

Governments and law enforcement agencies worldwide have intensified their efforts to combat the escalating threat of ransomware. Recognizing the transnational nature of cybercrime, these entities have established specialized task forces and collaborative frameworks to enhance their response capabilities. In 2021, the U.S. Department of Justice launched the Ransomware and Digital Extortion Task Force, aiming to coordinate national efforts, improve intelligence sharing, and take action against ransomware operators. This initiative underscores a strategic shift towards a more unified and proactive stance in addressing ransomware threats.

Legal and regulatory responses

International collaboration has also been pivotal in tackling ransomware on a global scale. Europol's Joint Cybercrime Action Taskforce (J-CAT) has been instrumental in facilitating cooperation among European law enforcement agencies.

Additionally, the No More Ransom initiative, launched in 2016 by Europol, the Dutch National Police, and cybersecurity firms, exemplifies public-private partnerships aimed at disrupting ransomware activities. This platform provides decryption tools to victims and educates the public on preventive measures, significantly reducing the impact of ransomware attacks.



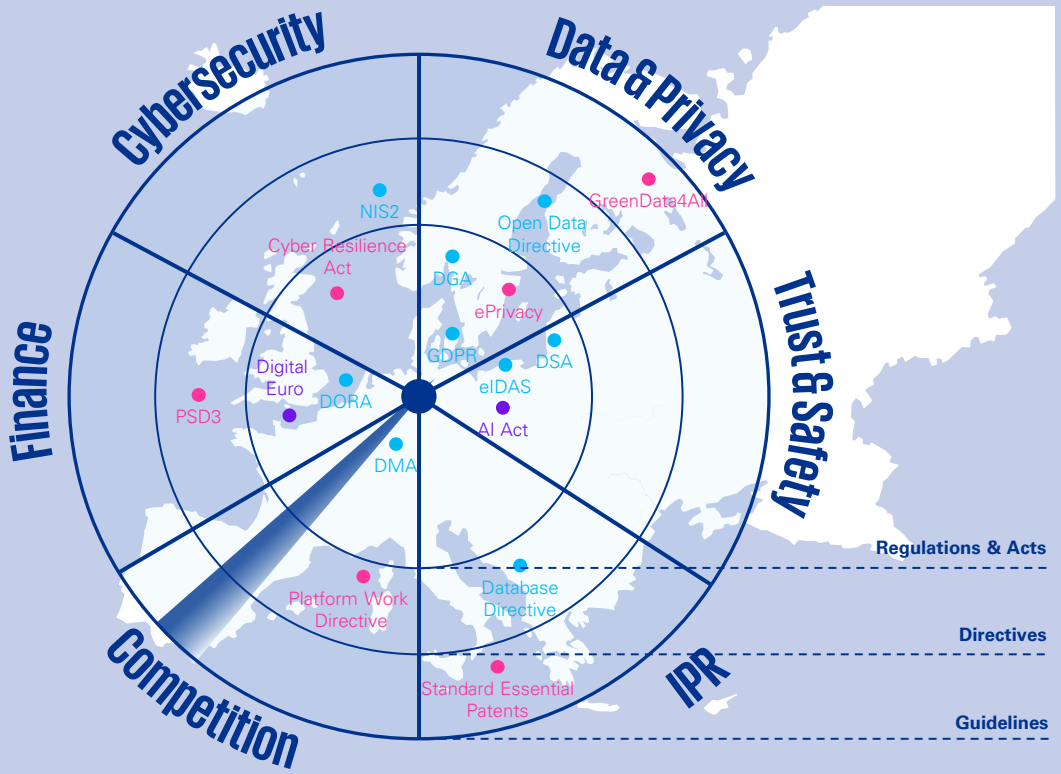
These concerted efforts have led to several notable takedowns and arrests, disrupting major ransomware operations.

In November 2021, international law enforcement agencies arrested multiple individuals associated with the REvil ransomware group, responsible for numerous high-profile attacks worldwide. Similarly, Ukrainian authorities, collaborating with the French National Gendarmerie and Europol, dismantled the Egregor ransomware network in early 2021. In 2018, coordinated actions led to the shutdown of the GandCrab ransomware operation, one of the most prolific ransomware families at the time. These successes highlight the increasing effectiveness of global law enforcement initiatives in apprehending cybercriminals and mitigating ransomware threats.

Compliance requirements

In response to the escalating ransomware threat over the past decade, compliance requirements have become more rigorous, particularly concerning data protection regulations.

Regulatory Radar



Note: This image is indicative, it does not contain all EU L&R
Legend: In force Approved Proposed

Legal and regulatory responses

Building on the foundation of GDPR, the European Union introduced the NIS2 Directive in 2022 to further strengthen cybersecurity across member states.

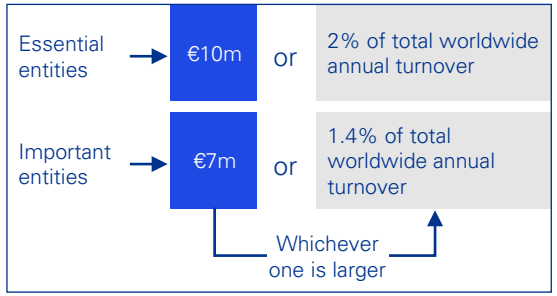
The NIS2 Directive expands the scope of sectors considered essential and imposes stricter security and reporting obligations on organisations. Entities covered by NIS2 are required to implement comprehensive risk management measures and are subject to more rigorous supervisory and enforcement actions. The directive emphasizes the need for enhanced cooperation between member states to address cross-border cybersecurity threats, including ransomware attacks. Obligations for reporting incidents have become a critical component of compliance frameworks like GDPR and NIS2 in the European Union.

How will your organization be impacted?

The most difficult question on NIS2 is how the Directive will be enforced in each Member State. As seen with the GDPR legislation, thoroughly understanding the data protection requirements and actions required by organisations grew over time. Although this will likely also be the case for NIS2, based on the current information, organisations will need to take the necessary available steps now in order to be prepared.

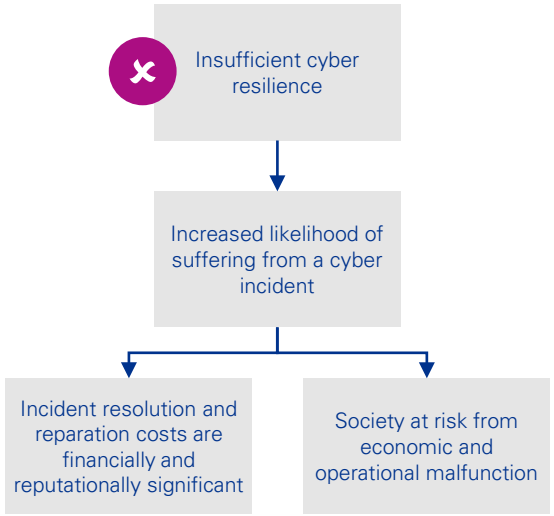
Compliance-led internal impact

The complexity of this new regulation requires organisations to start preparing now to understand the extent and potential impact of this regulation on their business. In case of non-compliance, essential and important entities risk facing financial penalties as shown below:



External impact

Those organisations that fall within the scope of NIS2 must realise they are considered a critical entity that contributes to a safe, effective and efficient society.



If critical organisations fail to protect themselves, they may be putting the wider society at risk. Besides compliance looking great on paper, meeting the security obligations of NIS2 also enhances the operational resilience of your organisation as the security posture is significantly hardened, thereby contributing to a resilient society.

Legal and regulatory responses

Questions to ask yourself

Does our company provide a critical service or essential function directly to end clients or as a key supplier that could impact public safety or economic stability?

Does our company operate in a sector that is covered by the NIS2 Directive, such as those listed here.

Is our company based outside of the EU, but offering critical services within the EU? If so, this Directive also applies to you!

Does the *lex specialis* principle apply? (Where a sector-specific EU legal act provides equivalent cybersecurity requirements or incident notification obligations, these sector-specific acts take precedent - e.g. DORA, PSD2.)

Keep an eye out!

Multinational organisations must assess whether they are considered (part of the supply chain of) critical infrastructure in each Member State in which they are present, and what legislation they must comply with in each of the Member States. Also those organisations based outside the EU, but offering critical services within the EU have to pay attention as the Directive will also apply to them.

The human factor

Role of social engineering

Over the past decade, ransomware attacks have increasingly leveraged social engineering to exploit the human element within organisations. Attackers use psychological manipulation to deceive individuals into divulging confidential information or performing actions that compromise security. Phishing has emerged as one of the most prevalent techniques, where cybercriminals send deceptive emails or messages that appear legitimate, enticing recipients to click malicious links or download infected attachments.

Spear phishing, a more sophisticated and targeted form of phishing, has become particularly concerning in the landscape of cybersecurity. Unlike generic phishing attempts that are broadcast to a wide audience, spear phishing involves attackers conducting thorough research on specific individuals or organisations.

This research enables them to craft personalized messages that appear highly credible.

For instance, an email might reference a project the recipient is working on or appear to come from a trusted colleague or superior, increasing the likelihood that the recipient will engage with the content.

The effectiveness of spear phishing lies in its personalization and the exploitation of trust within professional relationships. Attackers often utilize information gathered from social media profiles, company websites, and other publicly available sources to tailor their messages. This attention to detail makes it challenging for individuals to discern fraudulent communications from legitimate ones.

High-profile incidents underscore the impact of spear phishing on organisations. For example, in several cases, attackers have successfully infiltrated corporate networks by obtaining employee login credentials through deceptive emails. Once inside, they deploy ransomware to encrypt critical data, disrupting operations and causing substantial financial losses due to ransom payments and downtime.

Legal and regulatory responses

Insider Threats

Over the past decade, insider threats have emerged as a critical concern in the realm of cybersecurity and ransomware attacks. Insider threats refer to risks posed by individuals within an organization who have authorized access to its systems and data. These insiders can significantly compromise security, either inadvertently or deliberately, leading to data breaches, system disruptions, and facilitating ransomware infiltration. The dual nature of insider threats—encompassing both unintentional and malicious actions—makes them particularly challenging to detect and prevent.

Unintentional insiders are employees or associates who, without malicious intent, contribute to security breaches through negligence, lack of awareness, or simple human error. Examples include clicking on phishing links, using weak passwords, mishandling sensitive information, or failing to follow security protocols. These actions can unwittingly open the door for cybercriminals to deploy ransomware within the organization's network. The increasing complexity of social engineering attacks, as discussed earlier, often exploits these human vulnerabilities, making unintentional insiders a significant vector for ransomware attacks.

In contrast, malicious insiders intentionally seek to harm the organization for personal gain, revenge, or under external influence.

These individuals might deploy ransomware themselves, sell access credentials to cybercriminals, or assist in breaching security defenses. Malicious insiders often have a deep understanding of the organization's systems and can bypass security measures that are designed to thwart external threats. Their insider knowledge and access make them particularly dangerous, as they can operate under the radar and cause substantial damage before being detected.

Building a security culture

In the fight against ransomware and other cyber threats, building a robust security culture within an organization is paramount. A security culture is not just about implementing the latest technologies but fostering an environment where every individual understands their role in protecting the organization's assets. This cultural shift moves security from being solely the responsibility of the IT department to a collective responsibility embraced by all employees. By embedding security awareness into the daily routines and values of the organization, the human factor transforms from a vulnerability into a strength.

Central to building a security culture is the commitment to continuous education and training.

Cyber threats are constantly evolving, and so must the knowledge and preparedness of the organization's workforce. Regular training sessions should be more than just obligatory presentations; they need to be engaging, up-to-date, and relevant to employees' roles. Topics should cover the latest ransomware tactics, social engineering schemes like spear phishing, and best practices for data protection. Interactive workshops, webinars, and e-learning modules can cater to different learning styles and keep employees informed about emerging threats. By investing in ongoing education, organisations empower their staff to recognize and respond appropriately to potential security incidents.

Another critical component of a strong security culture is encouraging proactive reporting. Employees should feel comfortable and obligated to report suspicious activities, potential security breaches, or even their own mistakes without fear of reprimand.

Establishing clear reporting channels and response procedures ensures that threats are addressed promptly. Organisations can implement anonymous reporting systems and promote an open-door policy where security concerns are welcomed and promptly investigated.

Recognizing and rewarding employees who demonstrate vigilance can further reinforce the importance of proactive reporting. This approach not only aids in early detection of threats but also fosters a collaborative environment where security is a shared priority.

Legal and regulatory responses

By cultivating a security culture that emphasizes continuous learning and open communication, organisations can significantly mitigate the risks associated with the human factor in ransomware attacks. When employees are educated, vigilant, and engaged, they become the first line of defense against cyber threats, transforming potential vulnerabilities into a resilient security posture.

74%

of breaches involved the human element.

“By embedding security awareness into the daily routines and values of the organization, the human factor transforms from a vulnerability into a strength”

Essential practices for cyber security awareness training

Set the tone by making cyber security compliance accessible, fun and immersive while demonstrating to your workforce that cyber security is everybody’s responsibility.

Gamify your cyber security training via virtual or in-person cyber escape rooms which foster team building and reinforce cyber security principles in a fun and dynamic way.

Deliver next-gen learning backed by science leveraging next generation training based on neuroscience and advanced adult learning principles.

Provide a seamless user experience with a human risk quantification and behaviour change program via a dynamic platform or through your existing established channels.

Align with best practice cyber security frameworks where services are mapped to relevant local and global cyber security frameworks and regulations.

Mature with speed by implementing a sector aligned, ready-to-go human risk management and change program which can be deployed at pace.

Future outlook

Emerging threats

“Algorithms enable ransomware to adapt in real-time, evading traditional security measures by learning from the defenses”

As ransomware continues to evolve, emerging threats are set to amplify its sophistication and impact in the coming years. Cybercriminals are increasingly adopting advanced technologies, making ransomware more adaptable and harder to detect. These developments pose significant challenges for individuals, organisations, and governments striving to protect sensitive data and critical infrastructure.

One of the most significant emerging threats is the integration of artificial intelligence (AI) and machine learning into ransomware operations. Attackers can utilize AI to automate and enhance various aspects of their campaigns, such as crafting personalized phishing emails that are more likely to deceive recipients. Machine learning algorithms enable ransomware to adapt in real-time, evading traditional security measures by learning from the defenses they encounter. This level of sophistication makes attacks more efficient and increases the potential for widespread disruption.

Quantum computing presents another looming challenge with profound implications for ransomware. Quantum computers have the potential to break widely used encryption methods that currently secure data transmissions and storage. If cybercriminals harness quantum computing capabilities before organisations upgrade to quantum-resistant encryption, they could decrypt sensitive information at unprecedented speeds. This development would not only make data more vulnerable but could also empower more devastating ransomware attacks.

In addition to technological advancements, the intersection of cyberwarfare and ransomware is becoming a critical concern. State-sponsored actors may employ ransomware to target critical infrastructure and essential services, such as power grids, healthcare systems, and financial institutions. Attacks on these sectors can lead to significant economic damage, undermine public trust, and even threaten national security. As geopolitical tensions manifest in cyberspace, the risk of ransomware being used as a tool for large-scale disruption increases.

Recommendations

In light of the evolving ransomware landscape, organisations must take proactive measures to safeguard their assets and data. Investing in robust cyber-security infrastructure is paramount. This includes deploying advanced detection & response systems, implementing regular software updates, and developing a comprehensive security program. Employee training programs are essential to raise awareness about phishing schemes and social engineering tactics commonly used to deliver ransomware. Additionally, organisations should develop incident response plans to quickly address and mitigate the effects of any potential attack.

Future outlook

For policymakers, enhancing international cooperation is crucial to effectively combat ransomware, which often involves actors operating across borders. Collaborative efforts can lead to the development of standardized legal frameworks and the sharing of vital information to track, take down and prosecute cybercriminals. Investing in cybersecurity research and fostering public-private partnerships can also accelerate the development of advanced defense mechanisms.

Policies that promote the adoption of quantum-resistant encryption and other emerging security technologies will be essential in preparing for future threats.

Individuals play a vital role in strengthening cybersecurity on a personal level. Adopting strong personal cybersecurity practices can significantly reduce the risk of falling victim to threats. This includes using modern identity methods and enabling multi-factor authentication or going passwordless. Regularly updating devices and software helps protect against known vulnerabilities. Being cautious with unsolicited emails and avoiding clicking on suspicious links or attachments can prevent ransomware from infiltrating personal systems.

Conclusion

Over the past decade, ransomware has transformed from isolated attacks into a sophisticated global threat, evolving rapidly in both scope and complexity. Early attacks, such as CryptoLocker in 2013, were relatively simplistic compared to later iterations like WannaCry, NotPetya, and Colonial Pipeline, which demonstrated ransomware's capacity to disrupt critical infrastructure and national economies. The rise of Ransomware-as-a-Service (RaaS) has further exacerbated the problem by making sophisticated attack tools accessible to less-skilled cybercriminals, fueling an increase in global incidents.

Ransomware has also shifted in tactics, with modern attacks incorporating double and triple extortion, where cybercriminals not only encrypt data but also steal and threaten to release sensitive information. The growing focus on critical infrastructure, energy, healthcare, and transportation sectors, highlights the existential threat ransomware poses to essential services.

Collective action

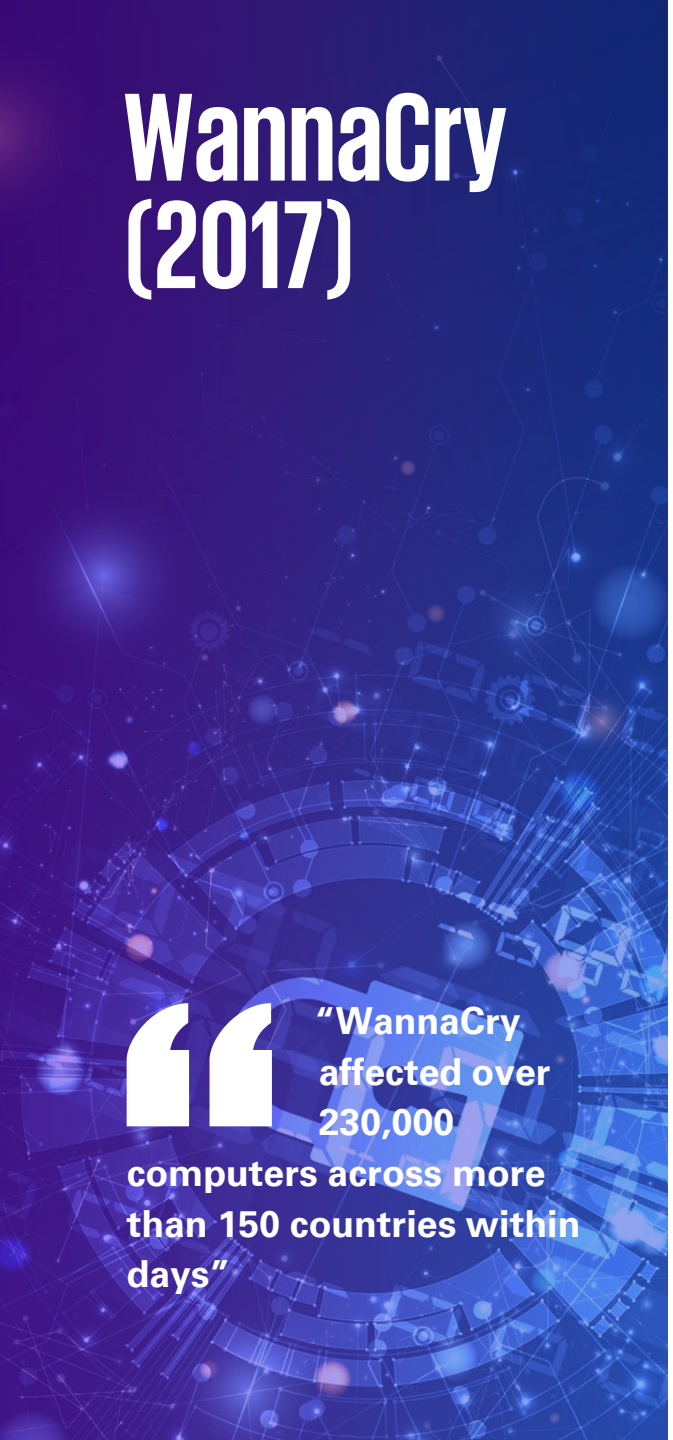
Effectively combating ransomware requires collective action from businesses, governments, and individuals. Governments must play a pivotal role by implementing and enforcing stringent cybersecurity regulations, encouraging international cooperation, and sharing intelligence to neutralize cross-border threats. Public-private partnerships are essential to developing robust defense mechanisms and decryption tools that mitigate the impact of attacks. Industry sectors need to align on best practices, focusing on advanced cybersecurity frameworks and continuous investment in security infrastructure. Organisations must prioritize cybersecurity as a core element of their operational strategy, adopting multi-layered defenses, regular software updates, and comprehensive employee training to reduce vulnerabilities. Encouraging collaboration across industries and between governments will increase resilience and enhance the ability to respond quickly to evolving ransomware threats. On an individual level, adopting stronger personal cybersecurity habits and remaining vigilant against phishing and social engineering attacks are crucial.

Mitigating the growing ransomware threat requires a proactive and adaptive approach. Organisations need to invest in robust cybersecurity solutions, including Managed eXtended Detection and Response (MxDR) services. Regular vulnerability assessments, incident response plans, and employee training are key to preventing and responding to attacks.

KPMG wortell

Ransomware cases

WannaCry (2017)



> **“WannaCry affected over 230,000 computers across more than 150 countries within days”**

In May 2017, the world witnessed one of the most widespread and disruptive ransomware attacks in history: WannaCry. This ransomware exploited a critical vulnerability in Microsoft Windows operating systems, known as EternalBlue. The vulnerability targeted the Server Message Block (SMB) protocol, which is used for sharing files and printers across local networks. EternalBlue was initially developed as an exploit by the U.S. National Security Agency (NSA) but was leaked to the public by a hacking group called the Shadow Brokers in April 2017.

Despite Microsoft releasing a security patch (MS17-010) for the vulnerability in March 2017, many organisations failed to apply the update promptly. WannaCry capitalized on this lapse by combining the EternalBlue exploit with a ransomware payload, creating a self-propagating worm.

Once a system was infected, WannaCry encrypted files and displayed a ransom note demanding payment in Bitcoin for the decryption key. The malware also scanned for other vulnerable systems on the network, allowing it to spread rapidly without user intervention. The WannaCry attack had a profound global impact, affecting over 230,000 computers across more than 150 countries within days (source: Microsoft Digital Defense Report 2020). Critical sectors were notably hit, including healthcare, telecommunications, transportation, and manufacturing. One of the most severely affected organisations was the United Kingdom's National Health Service (NHS), where the attack led to the cancellation of medical procedures, diversion of emergency services, and inaccessible patient records. Other major entities impacted included Spain's Telefónica, Germany's Deutsche Bahn, FedEx in the United States, and numerous universities and government agencies worldwide.

Economically, the attack caused estimated damages ranging from hundreds of millions to billions of dollars. Costs were incurred not only from ransom payments—which were relatively minimal as few victims paid—but also from system downtime, data loss, and extensive recovery efforts. The widespread disruption underscored vulnerabilities in critical infrastructure and highlighted the reliance on outdated or unpatched systems in essential services.

The immediate response to WannaCry involved a global cybersecurity effort to contain the malware and mitigate its effects. A significant breakthrough occurred when a security researcher, Marcus Hutchins (known online as MalwareTech), discovered a kill switch within the malware's code. By registering a specific domain name embedded in WannaCry, he effectively halted its spread.

Microsoft took the unusual step of issuing emergency patches for unsupported operating systems like Windows XP and Windows Server 2003 to help users protect their systems. The attack ignited debates over cybersecurity responsibility, particularly concerning the role of governments and intelligence agencies in stockpiling vulnerabilities versus disclosing them to vendors for patching. It also prompted organisations worldwide to reassess their cybersecurity practices, emphasizing the importance of timely updates and robust security protocols.

Investigations into the origin of WannaCry pointed to the Lazarus Group, a hacking organization linked to North Korea. This attribution raised geopolitical tensions and brought attention to the use of cyberattacks as tools of state-sponsored aggression.

The incident prompted international discussions on cybersecurity norms and the need for collaborative defense strategies against such threats.

The WannaCry attack served as a pivotal moment in cybersecurity history. It highlighted the critical risks associated with unpatched systems and the potential for cyber vulnerabilities to cause widespread disruption. The lessons learned from WannaCry continue to influence cybersecurity policies, practices, and international cooperation efforts aimed at preventing future large-scale cyberattacks.

NotPetya (2017)

In June 2017, shortly after the WannaCry ransomware outbreak, a new and more destructive malware attack emerged: NotPetya. Initially mistaken for a variant of the Petya ransomware due to similarities in its encryption methods and ransom note, NotPetya was later identified as a wiper disguised as ransomware. This distinction meant that its primary purpose was data destruction rather than financial gain.

NotPetya's initial infection vector was a compromised update mechanism of a widely used Ukrainian accounting software called M.E.Doc. Attackers infiltrated M.E.Doc's servers and pushed malicious updates to thousands of businesses operating in Ukraine. Once inside a network, NotPetya employed multiple propagation techniques.

It exploited the same EternalBlue vulnerability in Microsoft Windows' SMB protocol that WannaCry had utilized. Additionally, it used the EternalRomance exploit and leveraged credential-stealing tools like Mimikatz to harvest user passwords, allowing it to spread rapidly within and across networks.

The NotPetya attack had a devastating global impact, affecting organisations across various sectors, including shipping, pharmaceuticals, logistics, and energy. Major corporations such as Maersk, Merck, FedEx's TNT Express, and the advertising giant WPP were significantly disrupted. Maersk, one of the world's largest shipping companies, experienced a complete shutdown of its IT systems, leading to port closures and logistical chaos worldwide. The company later reported losses of up to $300 million due to the attack.

Unlike traditional ransomware, NotPetya encrypted the Master Boot Record (MBR) and overwrote critical system files, rendering computers inoperable. Even if victims paid the ransom, data recovery was virtually impossible because the malware lacked a functional decryption mechanism. This behavior indicated that the attack was intended to cause maximum disruption rather than generate ransom payments.

Economically, the attack resulted in estimated damages of over $10 billion globally. The widespread disruption underscored the vulnerabilities in global supply chains and the interconnected nature of modern business operations. The attack also highlighted the risks associated with third-party software and the importance of securing supply chain components.

NotPetya differed from traditional ransomware in several critical ways:

1. **Destructive intent**: traditional ransomware is designed to encrypt data and extort victims for financial gain, with the possibility of data recovery upon payment. NotPetya, however, was a wiper masquerading as ransomware. Its primary objective was to irreversibly destroy data, making recovery impossible even if the ransom was paid.
2. **Non-functional payment mechanism**: the payment process in NotPetya was ineffective by design. The malware directed victims to send ransom payments to a single hardcoded Bitcoin wallet and contact an email address for the decryption key. Shortly after the attack began, the email provider shut down the account, eliminating any possibility of communication with the attackers.
3. **Advanced propagation techniques**: while traditional ransomware often relies on user interactions like phishing emails to spread, NotPetya used sophisticated methods to self-propagate. It combined multiple exploits and credential-stealing techniques to move laterally within networks without user intervention.
4. **Targeted attack disguised as global ransomware**: NotPetya appeared to be a global ransomware campaign but was, in fact, a targeted attack against Ukrainian infrastructure. The initial infection through M.E.Doc, a software predominantly used in Ukraine, suggested a specific focus. The global impact was collateral damage resulting from the interconnectedness of international networks.

NotPetya (2017)

Internationally, the attack heightened tensions and sparked discussions on cyber warfare. Intelligence agencies from the United States, United Kingdom, and other nations attributed NotPetya to the Russian military, specifically the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). The attack was viewed as part of ongoing hostilities between Russia and Ukraine, using cyber means to destabilize critical infrastructure.

Legal and insurance sectors also felt the impact. Companies faced challenges in claiming insurance payouts, as insurers categorized the attack as an act of war—a common exclusion in insurance policies. This led to lawsuits and debates over the definition of cyber warfare and the responsibilities of insurance providers.

The NotPetya incident underscored the evolving nature of cyber threats, where malware can serve dual purposes of disruption and strategic geopolitical signaling. It highlighted the necessity for global cooperation in cybersecurity and the development of international norms and laws to address state-sponsored cyberattacks.

Colonial Pipeline attack (2021)

> **“The Colonial Pipeline ransomware attack was a pivotal event that highlighted the severe implications of cyber threats on critical infrastructure”**

In May 2021, the United States faced one of its most significant cyberattacks targeting critical infrastructure: the ransomware attack on Colonial Pipeline. Colonial Pipeline is one of the largest fuel pipeline operators in the U.S., responsible for transporting approximately 45% of the East Coast's fuel supply, including gasoline, diesel, jet fuel, and heating oil (source: Microsoft Digital Defense Report 2021). The attack underscored the vulnerabilities of essential services to cyber threats and highlighted the potential for ransomware to cause widespread societal disruption.

The breach was attributed to a cybercriminal group known as DarkSide, believed to be based in Eastern Europe or Russia. DarkSide operated under a ransomware-as-a-service (RaaS) model, providing malware to affiliates who then carried out attacks and shared profits with the developers. The attackers gained access to Colonial Pipeline's network through a compromised password for a legacy Virtual Private Network (VPN) account that did not have multi-factor authentication enabled. Once inside, they deployed ransomware to encrypt data and demanded a ransom payment for decryption and the promise not to leak stolen information.

The attack forced Colonial Pipeline to proactively shut down its entire pipeline system to contain the threat, marking the first time in the company's history that it had halted all operations. This shutdown had immediate and cascading effects on the fuel supply chain along the East Coast:

- **Fuel shortages**: the disruption led to panic buying and fuel shortages in several states, including North Carolina, South Carolina, Georgia, and Virginia. Many gas stations reported running out of fuel, leading to long lines and increased prices at the pump.
- **Economic consequences**: the interruption affected various sectors dependent on fuel, such as transportation, aviation, and logistics. Airlines had to adjust flight operations due to concerns over jet fuel availability, and trucking companies faced increased operational costs.
- **Government response**: in response to the crisis, the U.S. Department of Transportation issued emergency declarations to allow for increased flexibility in fuel transportation by road. The Federal Motor Carrier Safety Administration relaxed regulations on drivers' hours of service to expedite fuel delivery.
- **National security concerns**: The attack raised alarms about the security of critical infrastructure and the potential for cyberattacks to threaten national security. It prompted discussions on the resilience of essential services and the need for robust cybersecurity measures across industries vital to the nation's functioning.

Under pressure to restore operations swiftly, Colonial Pipeline paid a ransom of approximately 75 Bitcoin (around $4.4 million at the time) to the attackers (source: Microsoft Digital Defense Report 2021). The company received a decryption tool but found it inefficient, resorting to using their backups to restore systems. The pipeline resumed operations after a six-day shutdown, but the incident had already exposed significant vulnerabilities.

The Colonial Pipeline ransomware attack was a pivotal event that highlighted the severe implications of cyber threats on critical infrastructure. It demonstrated how cyberattacks could transcend digital boundaries and cause tangible, widespread disruption to everyday life. The incident prompted a reevaluation of cybersecurity strategies at the highest levels and emphasized the urgency of protecting essential services from evolving cyber threats. It serves as a case study for the potential impact of ransomware on critical infrastructure and the importance of proactive measures to safeguard against such attacks.

Healthcare sector attacks

> **“In 2021, ransomware was the most significant cybersecurity threat in the healthcare sector”**

Over the past decade, the healthcare sector has become an increasingly attractive target for ransomware attacks. The critical nature of healthcare services, combined with the sensitive personal data they hold, makes hospitals and medical institutions particularly vulnerable. Cybercriminals exploit these vulnerabilities, knowing that disrupting healthcare operations can have dire consequences, thereby pressuring organisations to pay ransoms quickly.

The healthcare sector has been a prominent target for ransomware attacks, as highlighted in the Dutch Z-CERT reports from 2021 to 2023. These reports emphasize the increasing severity of ransomware threats faced by healthcare institutions, impacting not only hospitals but also broader care facilities such as nursing homes and mental health organisations.

In 2021, ransomware was the most significant cybersecurity threat in the healthcare sector. The number of incidents spiked considerably across Europe and the Netherlands, with 31 healthcare institutions affected, disrupting services at 116 locations. The nature of these attacks was not limited to direct hits on healthcare providers but also extended to critical suppliers. For instance, several Dutch healthcare institutions were impacted by ransomware attacks on their suppliers, causing delays in medical equipment maintenance, data access, and overall operational functionality. This ripple effect demonstrated how a single attack on a supplier could create significant disruption across multiple healthcare facilities.

By 2022 and 2023, the complexity and sophistication of ransomware attacks had escalated. Attackers increasingly exploited known vulnerabilities in software like Microsoft Exchange, leading to widespread disruptions. The impact was not merely operational; the theft of patient data became a potent tool for extortion.

Threat actors not only encrypted systems but also threatened to leak sensitive medical data unless a ransom was paid. Some incidents caused hospitals to revert to manual systems for days, further emphasizing the critical nature of these attacks on healthcare operations.

The 2023 report pointed to the persistence of ransomware threats despite improved cybersecurity measures. Z-CERT highlighted the trend of ransomware-as-a-service (RaaS), where attackers use commercialized ransomware platforms to launch attacks more efficiently. Healthcare institutions with weak remote access protections, such as poorly secured RDP (Remote Desktop Protocol) systems, remained particularly vulnerable. The reports also noted that even when ransoms were paid, not all data was recoverable, leaving healthcare institutions to manage the long-term effects of data loss and operational disruptions.

In 2023, Joris Zorg, a healthcare provider in the Netherlands, was targeted by the ransomware group LockBit. Hackers infiltrated their systems, stealing 100 GB of sensitive client and employee data, which was subsequently leaked online. The breach exposed personal information, including medical details, putting residents at risk of identity theft. Joris Zorg warned its clients to be vigilant against potential scams and advised some to replace their passports and IDs.

Lessons learned

The ransomware attacks on WannaCry, NotPetya, Colonial Pipeline, and the healthcare sector highlight critical lessons about cybersecurity vulnerabilities and the importance of proactive defense measures. A common vulnerability exploited in these incidents was the failure to promptly apply security patches. Both WannaCry and NotPetya capitalized on the EternalBlue vulnerability in Microsoft's SMB protocol, which had been patched prior to the attacks. Organisations that delayed updates left themselves exposed to exploits targeting known weaknesses.

Outdated and legacy systems played a significant role, especially in the healthcare sector, where many institutions relied on unsupported software lacking modern security features. This reliance made them susceptible to attacks that could have been mitigated with updated technology and regular maintenance. The interconnectedness of networks and devices increased the attack surface, complicating security efforts and allowing malware to spread rapidly across systems.

Weak authentication practices were another critical vulnerability. The Colonial Pipeline attack occurred because attackers accessed the network through a compromised VPN account without multi-factor authentication. This underscores the necessity of robust access controls and the implementation of multi-factor authentication to prevent unauthorized entry.

Threat actors not only encrypted systems but also threatened to leak sensitive medical data unless a ransom was paid. Some incidents caused hospitals to revert to manual systems for days, further emphasizing the critical nature of these attacks on healthcare operations.

The 2023 report pointed to the persistence of ransomware threats despite improved cybersecurity measures. Z-CERT highlighted the trend of ransomware-as-a-service (RaaS), where attackers use commercialized ransomware platforms to launch attacks more efficiently. Healthcare institutions with weak remote access protections, such as poorly secured RDP (Remote Desktop Protocol) systems, remained particularly vulnerable. The reports also noted that even when ransoms were paid, not all data was recoverable, leaving healthcare institutions to manage the long-term effects of data loss and operational disruptions.

About the authors

Maarten Goet

Maarten Goet is a distinguished expert in cybersecurity and cloud computing, currently serving as the Director of Cybersecurity at Wortell, a leading IT consultancy based in the Netherlands. With over two decades of experience in the IT industry, Maarten has become a prominent figure in the Microsoft technology community. He holds the prestigious titles of Microsoft Regional Director and Microsoft Most Valuable Professional (MVP), recognitions that underscore his significant contributions to the field and his deep expertise in Microsoft technologies.

In addition to his role at Wortell, Maarten is the founder of Experts Live, an international series of events that bring together IT professionals to share knowledge and insights on Microsoft solutions. He is a sought-after speaker at global industry conferences, where he discusses topics such as cloud security, digital transformation, and enterprise mobility.

Maarten's dedication to advancing the IT industry is evident through his active participation in technical communities and his commitment to mentoring emerging professionals in the field.

Henrik Smit

Henrik Smit is a seasoned cybersecurity professional who serves as the Director of Cyber Defense & Response at KPMG. With over two decades of experience in the information security sector, Henrik specializes in developing robust cyber defense strategies and leading incident response teams. At KPMG, he oversees a team of experts dedicated to protecting clients from evolving cyber threats, implementing advanced security technologies, and ensuring compliance with international security standards. His leadership has been pivotal in enhancing the cybersecurity posture of organisations across various industries, including finance, healthcare, and technology.

Prior to his tenure at KPMG, Henrik held key positions in other leading firms where he was instrumental in designing and implementing comprehensive security architectures. He is a certified information security manager and holds advanced degrees in computer science and cybersecurity. Henrik is also a sought-after speaker at industry conferences and contributes regularly to professional journals on topics such as threat intelligence, risk management, and cyber defense strategies. His commitment to the field extends to mentoring aspiring cybersecurity professionals and participating in various industry working groups aimed at advancing global cybersecurity practices.

Contact us

Henrik Smit
Director, KPMG
Smit.Henrik@kpmg.nl
KPMG.nl

Maarten Goet
CTO, Wortell
Maarten.Goet@wortell.nl
Wortell.nl

Document Classification: Public