



Ransomware in control

A study report by NOREA

Authors:

S. Gangaram Panday, MSc RE CISA – Schuberg Philis
L. Zwakenberg, MSc – PwC

©2023 NOREA, All rights reserved
PO box 7984, 1008 AD Amsterdam
phone: +31 20-3010380
The Netherlands
e-mail: norea@norea.nl

www.norea.nl

Table of contents

1	Introduction	3
1.1	Motivation	3
1.2	Executive summary	4
1.3	Ransomware today	5
1.4	Goal	7
1.5	Research methods and approach	8
1.6	Scope limitations	8
2	Ransomware	9
2.1	What is ransomware?	9
2.2	A brief history	9
2.3	Ransomware's evolution	10
2.4	Damage and statistics	12
2.5	Ransomware kill chain	14
2.6	Existing security frameworks	18
3	Ransomware in control	20
3.1	NOREA ransomware kill chain	20
3.2	Mitigation strategies	21
3.3	How to start	22
3.3.1	The pragmatic approach: Prevention first	22
3.3.2	The advanced approach: Threat assessment	23
3.3.3	Suggestion for further prioritization for both approaches	24
3.4	NOREA Ransomware Framework	24
3.4.1	Major point of attention: Rebuild capability	26
3.4.2	Framework maintenance	28
4	Conclusion	59
	References	60
	Appendix 1. ENISA attack model	67
	Appendix 2. A more detailed history of ransomware	68
	Appendix 3. Overview of cybersecurity frameworks	70
	Appendix 4. NOREA Ransomware framework attack steps	72

1 Introduction

1.1 Motivation

After seeing one too many news reports in the Netherlands and internationally on ransomware attacks, we felt compelled to create a control framework that could help protect organizations against this increasingly dire cyber threat. We were motivated not just by concern for the massive devastation that ransomware has the potential to cause, but the reality that at the time of writing no such control framework existed. The framework we developed selects the most relevant controls organizations can take to boost their defenses against ransomware and responses to an attack. Its goal is to help organizations protect themselves, their customers or end users, and ultimately society as a whole. As we learned from our research, the complexity of ransomware attacks is growing drastically within very short timespans. Meanwhile, our hope for a safer digital world has gained even more urgency as the past few years have shown that for the vital industries, the impact has transcended any individual organization. Security incidents affecting hospitals, grocery stores, financial institutions, and mail delivery have the potential to cause, at best, chaos, and, in worst-case scenarios, destruction to lives and livelihoods.

Accordingly, digital resilience has received greater attention over the past few years in the European Union (EU). The EU has put into place an elaborate Digital strategy to address Cybersecurity and increase digital resilience. The EU introduced the Digital Operational Resilience Act (DORA), a regulation that entered into force in early 2023 and will become mandatory from early 2025 to better protect society's dealings in the financial sector. Another major law that entered into force in early 2023 is the NIS2 Directive, which succeeds the Network and Information Security Directive (NIS) to strengthen cybersecurity across the EU. A notable difference between NIS2 and NIS is the large expansion of the scope to 16 sectors – now newly including food, pharmaceuticals, healthcare, telecommunications, digital service providers, water suppliers, postal and courier services – fall in the scope of the directive. These new laws emphasize the seriousness of security breaches and their highly disruptive power, which we are only seeing more and more of globally.

To contextualize the technological and social climates in which ransomware has taken hold, to share insights and guidance from interviews we held with IT experts, and to explain why we chose particular controls, we decided to present our framework via this study report. For readers seeking present-day and background information about ransomware, it may be useful to read the study report in full. For those eager to start applying the controls, focusing on the contents of chapter 3 and the framework itself, presented in section 3.4, will suffice.

The NOREA Ransomware Framework is published as an open source tool because we want to keep improving the selection and application of controls. Writing this in early 2023, we want to enable the framework to evolve with the same efficiency and sophistication that we're observing of waves of ransomware attacks. We therefore invite interaction, shared experiences, and feedback from interested parties or individuals, particularly those from the vital industries, as we all aim to keep ransomware in control.

From the authors,

Sandeep Gangaram Panday - sgangarampanday@schubergphilis.com

Leon Zwakenberg - leon.zwakenberg@pwc.com

Link to the Excel (full) version of the NOREA Ransomware Framework, also accessible to non-GitHub account holders.



1.2 Executive summary

The NOREA Ransomware Framework presented in this study report is the first of its kind created in such a holistic way and freely disseminated. The framework selects the most relevant controls for organizations to take so as to increase their defenses against and responses to ransomware attacks. The framework is the result of a considered curation process, drawing from the CIS Critical Security Controls Version 8, one of the most detailed cybersecurity frameworks to date, and a controls selection process informed by many interviews that the paper's authors conducted with cybersecurity experts and IT professionals. Additionally, all internationally available official guidelines have been used as input to supplement the controls and tailor them to the specific context of ransomware. This includes, among others, the recommendations of national cyber defense organizations and International Sharing and Analysis Centers (ISACs).

This offering is unique because the framework maps each control to a specific step in the ransomware kill chain (see paragraph 2.5 for the kill chain that has been created). Organizations can now determine which control maps to which specific kill chain step.

To determine how and where to start with the control framework, we propose two approaches: the pragmatic approach and the advanced approach. Focused on prevention, the pragmatic approach is appropriate for organizations that prefer to use a more general best-practices sequence of control implementation that they can begin right away. The advanced approach is appropriate for organizations with the capacity and capability to conduct a threat assessment based on their own context-specific circumstances and, according to the kill chain mapping, to select only controls that are relevant for them.

Crucially, all organizations can benefit in some way from this study report and the control framework. If a rigorous implementation method, such as that outlined in the aforementioned approaches, cannot be undertaken, the framework still offers useful insights into the most important mitigation activities to consider.

In addition, the study report provides information detailing the origin and evolution of ransomware, its various types, occurrences, and ensuing damage as well as descriptions and comparisons of other security frameworks.

The NOREA Ransomware Framework itself is presented in section 3.4.

1.3 Ransomware today

“Ransomware is the biggest cybersecurity threat facing the world today, with the potential to significantly affect whole societies and economies – and the attacks are unrelenting.”

LINDY CAMERON, HEAD OF THE NATIONAL CYBER SECURITY CENTRE (NCSC) [1]

As of the start of 2023, ransomware still holds first place as the most impactful form of cyberattack in history. An ING study found that from mid-July 2019 to the first half of 2021, ransomware attack attempts tripled [4]. What’s more, they have evolved from involving single to double to currently triple extortion. That means they have the ability to severely disable an organization’s operations if not simply end the business within a week’s time. So ransomware is certainly not just a security issue, but an existential threat to business everywhere. What’s more, the attacks are not exclusively targeted at businesses but increasingly also at governments, healthcare institutions, and other public services, thus increasing the damage to society. As such, ransomware has been classified as a national security issue in the US, and the American government has begun to leverage a range of criminal, diplomatic, economic, and military capabilities to combat the ongoing ransomware threat [100].

“Ransomware creates unworkable processes and irreversible damage,” states the National Coordinator for Counterterrorism and Security (hereafter NCTV) [2]. Gartner research concludes that ransomware is the top key risk area that audit departments and organizations’ management need to consider. One reason audit strategies now prioritize ransomware is that organizations are experiencing progressively complex attack attempts on their IT infrastructure [3]. And yet, a study by Thales revealed that 50% of large organizations worldwide lack a formal ransomware response plan [13]. Most governmental cyber defense guidance on ransomware still focuses on only basic cybersecurity controls. Meanwhile, as routine activity theory (RAT) finds, crime is encouraged by factors such as the absence of proper security controls and security guardians (employees who defend the organization against cyberthreats) [29]. The link between ransomware and RAT is clear; companies that do not invest in cybersecurity tools and security guardians for the sake of improving routines security practices become more attractive to criminals and are likelier to become victims of ransomware. This awareness has permeated the boardroom, with executives now knowing the urgency of investing in cybersecurity controls [3]. Several Dutch cybersecurity experts interviewed conclude that if management does not invest in their organizations’ cyber resilience, ransomware is due to become a national crisis [5].

Why is ransomware everywhere?

Before turning to chapter 2’s look back on how ransomware emerged, we put forward several reasons for its prominence today, as based on our literature review.

A first reason for the prominence of ransomware is the evolution of the product itself, both technologically and socioeconomically. With the earliest detected attack being in 1989,

ransomware has had over three decades to develop further. Currently, it's a booming revenue model [2] commonly known as "ransomware-as-a-service" (hereafter RaaS). Enabling criminals to make money by lending out software used for ransomware attacks [8], this service model allows people with little technical expertise to carry out attacks with a few clicks of a button [9].

Another reason for its prominence is the explosion of ransomware social engineering toolkits, such as rogue websites and infected e-mail attachments. These tools are more readily available thanks to RaaS, resulting in a growing presence of available ransomware toolkits on the internet [10]. This effect can be seen in the number of ransomware attacks in recent years. Sophos shows a 57% global increase between 2020 and 2021 [12]. This trend is also reflected in multiple studies by renowned cybersecurity organizations CrowdStrike [9], Thales [13], and Verizon [16].

Yet another reason is the COVID-19 pandemic. As the paradigm shifted to include more remote-work scenarios, organizations have faced weaker security control because employees often have poorer network security at home than at their offices and tend to use their own personal devices and local networks [15]. These home networks are mostly unsecured by nature and fail to meet industrial standard security controls, leading to an increase in potential attack vectors and thus attack surface for ransomware [103]. Gartner includes attack surface expansion in its seven top trends in cybersecurity for 2022 [17].

Finally, another reason is due to the introduction of cryptocurrency, which has enabled creation of a viable revenue model and the subsequent explosion in ransomware attacks [2]. While in ransomware's early days, payment methods were limited – largely consisting of a hacker sending a message for money to be wired to a bank account – the authorities could trace such transfers. With the usage of cryptocurrencies, which permits anonymous transfers, the payments became untraceable [105].

The observations so far described make it easy to conclude that ransomware is decisively a rising threat to the continuity of organizations and governments in our present-day and ever-growing digitized society. According to European parliamentarian Bart Groothuis, Europe is in the midst of a "ransomware pandemic," which could affect civil society [18]. The threat of a ransomware attack can come from multiple angles and have major consequences for business continuity.

Some well-known examples of organizations attacked in recent years in the Netherlands include Maastricht University, VDL, the Hof van Twente municipality, and MediaMarkt. All these organizations made news headlines because ransomware attacks took down all or almost all of their IT infrastructure, majorly impacting business continuity. An example of how disabling an attack can be is the Dutch municipality Hof van Twente, which was attacked in 2019 and, as of late 2022, was still busy rebuilding systems [28]. But ransomware is a big problem globally. In 2021, JBL, one of the largest meat processors in the United States and Australia, was attacked by ransomware. Hundreds of slaughterhouses had to temporarily close their doors, and the financial consequences were severe [20]. Other major international examples include the ransomware attacks on Equifax in 2017 and Colonial Pipeline in 2021.

1.4 Goal

The goal of this study report, therefore, is to present a framework that guides organizations through the concrete steps they can take to boost their cyber resilience against ransomware attacks. Because IT experts can help organizations identify the risks combined with the different steps in the ransomware attack chain [26], this study report also draws on interviews offering insights into attack methodologies in the ransomware kill chain. A ransomware kill chain is a concept devised to stop the attack by analyzing the kill chain to then break it [30]. The study report shares suggestions for how organizations can boost cyber resilience through mapping the ransomware kill chain to know where the threats and risks are. To mitigate the greatest risks, experts agree that a good first step is to investigate which vectors an attacker uses. With its primary focus on identifying the most common vectors in a ransomware attack, this study report thus provides input for the initial threat assessment organizations make concerning where in the ransomware kill chain that cybersecurity controls should be implemented.

Since ransomware attacks are a growing problem for society, organizations must increase their cyber resilience. The National Institute of Standards and Technology (hereafter NIST) defines cyber resilience as [112]:

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.

And yet, in IBM's global study on cyber resilient organizations, only 21% of surveyed IT professional responded that their organizations are "mature" [106] in reference to implementation of cyber resiliency security activities. NCTV research on cybersecurity in the Netherlands shows that digital resilience and risk management are still in their infancy. More attention should thus go to boosting resilience to ward off the constant threat of cybersecurity attacks [19]. As Martijn Hoogesteger (Head of Cyber Security at S-RM, a global intelligence and cybersecurity consultancy) writes in a column for the Platform for Information Security (hereafter PVIB) [31]:

What I ask is not how do you defend yourself, but how do you stop the attacks or at least make them harder. It sounds like the same thing, but it requires a different outlook! Focus on how they attack, outside-in thinking. Be pragmatic. Thinking from the perspective of your organization and how you implement some particular control is inside-out. Often that's exactly where you come up against a lot of hurdles.

In short: "outside-in" thinking makes it harder for an attacker to gain initial access.

1.5 Research methods and approach

Our research methods consisted of rigorous review of leading ransomware papers and worldwide trend reports¹ as well as interviews conducted with IT experts in the Netherlands. The present study report yields insights into how organizations can better stay in control as they face the threat of ransomware. Its results should contribute to improved understanding of how organizations can apply an accepted ransomware framework to increase their cyber defenses against ransomware attacks. Multiple IT experts with varying perspectives validated the results, enabling us to create the ransomware framework, which can be used by CISOs, IT auditors, information security consultants, regulators, and others

The study report first describes the impact of ransomware attacks on society. Next, it identifies the most common attack vectors in a ransomware attack and, based on them, compiles a top three. It then looks at which specific cybersecurity controls are needed to combat attack vectors most common in ransomware. Finally, the study report examines the ransomware kill chain, the multiple phases an attacker goes through, and corresponding cybersecurity controls. Since an organization must also maintain control after an attacker intrudes, corresponding cybersecurity controls for the follow-up phase in the ransomware kill chain are also included.

1.6 Scope limitations

Our research examined the years 2021 and 2022 to arrive at the most significant attack vectors, defined as “path[s] or means by which an attacker or hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element” [32]. Selecting the most common attack vectors have kept the scope of the research manageable. Earlier years were also excluded because ransomware attack methods have changed significantly [2]. Another reason for including only the 2021 and 2022 attack vectors is that reputable cybersecurity organizations and government agencies have differing research periods in their reports. They do not specifically focus on 2021 and they include data from 2022. This study report thus focuses on the most current ransomware attack methods at the time of writing in early 2023. It also covers multiple models that highlight the ransomware kill chain while ultimately selecting the kill chain that is most complete and relevant.

¹ For details on our sources associated with the European Agency for Cybersecurity (ENISA), the National Council of Information Sharing and Analysis Centres (ISACs), the Netherlands' National Cyber Security Centre (NCSC), and the UK's National Cyber Security Centre (NCSC), see reference list entry numbers 2, 6, 7, 8, 9, 11, 12, 13, 14, 16, 19, 25, 37, 54, 61, 62, 63, 68, 96, 107, 108, and 109.

2 Ransomware

2.1 What is ransomware?

Ransomware has evolved into a mature cybercrime model in recent decades. The NIST defines ransomware as follows [33]:

Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. Attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public.

Ransomware is thus malware that encrypts files and systems on an IT system using an encryption algorithm. It demands a ransom, often in the form of cryptocurrency, such as bitcoin [34], in order to free the files and systems [26]. The term consists of the words “ransom” and “ware” – the latter of which refers to the software or malware an attacker uses to get ransom from an organization before using data encryption as leverage [8].

2.2 A brief history

The first ransomware attack was detected in 1989 [35], when a user inserted a floppy disk into the computer, a counter started running, and 90 boot-ups later, a message demanded \$189 for a decryption key. By 2005, ransomware was being built more professionally. However, because no options to anonymously demand ransom existed, it remained limited to small attacks on individuals [36]. It was not until 2011 that ransomware became more professional due to the rise of cryptocurrency that allowed cybercriminals to start making more money.

The two most common types of ransomware are locker and cryptor [37], while Kok et al. [40] mention scareware. In this third type of ransomware, pop-up ads intend to manipulate users into buying software or making payments, for example, of a fine for an alleged law violation. But locker ransomware came first, with the earliest attacks observed around 2010-2011. This ransomware locks a computer's access screen so the user can no longer perform basic functions, including accessing the desktop and fully or partially disabling the mouse and the keyboard [38]. Second came cryptor ransomware, which causes files to be encrypted using encryption algorithms. Unlike locker ransomware, cryptor encrypts critical data that the user can see – as basic functions still work – but the user cannot access.

In 2015, there were more cryptor than locker ransomware attacks [41]. Around this period, the focus also shifted from attacking individuals to organizations. A well-known example is WannaCry in 2017 [15], the first major ransomware attack known to the public. It was activated in over 150 countries [45], and several large international organizations fell victim. Another well-known ransomware attack is NotPetya in 2017, barely two months after the WannaCry ransomware attack. NotPetya was characterized not as an official ransomware attack, but rather a wiper that ensures data becomes unrecoverable [50]. Since not all organizations had installed the Windows security patch after WannaCry, NotPetya caused destruction. Its total cost worldwide is estimated at €8 billion [48]. The ransomware attack originated from a Ukrainian software package, and

organizations using it were affected if they did a software update but had not the installed the accompanying security patch [51]. Among those affected was container company Maersk's location in the Port of Rotterdam, with costs estimated at €300 million [52]. Observers noted that Maersk was lucky: a brief power outage in Ghana spared a domain controller backup from infection, which allowed Maersk's IT system to become partially operational again within 10 days [53].

The 2022 European Network and Information Security Agency (hereafter ENISA) report no longer refers to locker or cryptor attacks because a ransomware attack has evolved into a multiple attack model. An attacker can perform all of these actions during a ransomware attack instead of just using a locker and, per action, nine different assets can be attacked. Through this lens, ransomware attacks can be analyzed more specifically (see Appendix 1).

A ransomware attack also differs from a cybersecurity attack in that the former is more focused on disruption of business processes to obtain ransom, whereas a cybersecurity attack is focused on stealing intellectual property, credit card data, or business-sensitive data [33]. Ransomware can have a knock-on effect on entire business chains, potentially disrupting industries or society as a whole.

For a more detailed account of ransomware's history, see Appendix 2.

2.3 Ransomware's evolution

Figure 4 presents an overview of ransomware's evolution. By the end of 2019, ransomware 2.0 came to be. Ransomware 2.0 organizations incorporated data exfiltration in their strategies and ensured that even a good backup strategy would not mitigate attack techniques developed in the wake of ransomware 1.0. As of early 2023, ransomware 3.0 is flourishing, enhanced by more attack techniques added to exert more pressure on organizations. Examples include denial-of-service (DDoS) attacks, selling stolen customer data, and business email compromise scams [55]. The swift evolution of ransomware means that, in addition to having a good backup strategy, organizations must implement more security controls.

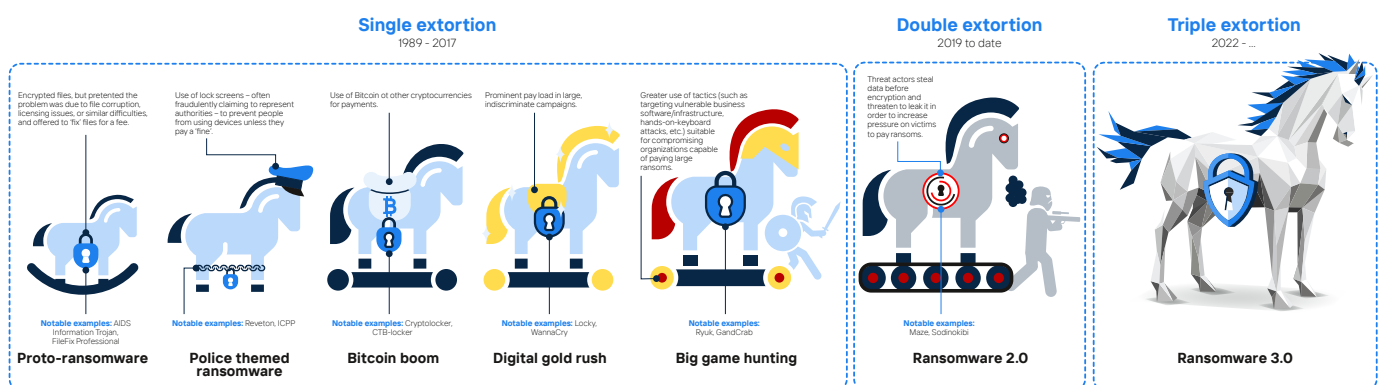


Figure 1: The evolution of ransomware [56]

Ransomware-as-a-Service (RaaS)

In the past years, more ransomware tooling has become available, leading to a large increase in the number of ransomware attacks. RaaS is a service model wherein money is earned through the lending of software made for ransomware attacks [57]. This allows people without much technical expertise to perform ransomware attacks in a few clicks of a button. The hostage software consists of a platform or control panel that integrates all aspects of a ransomware attack [11]. The provider of the ransomware platform or control panel, often a ransomware organization, negotiates to get some of the ransom, which O’Kane et al. find can be as high as 70% [58].

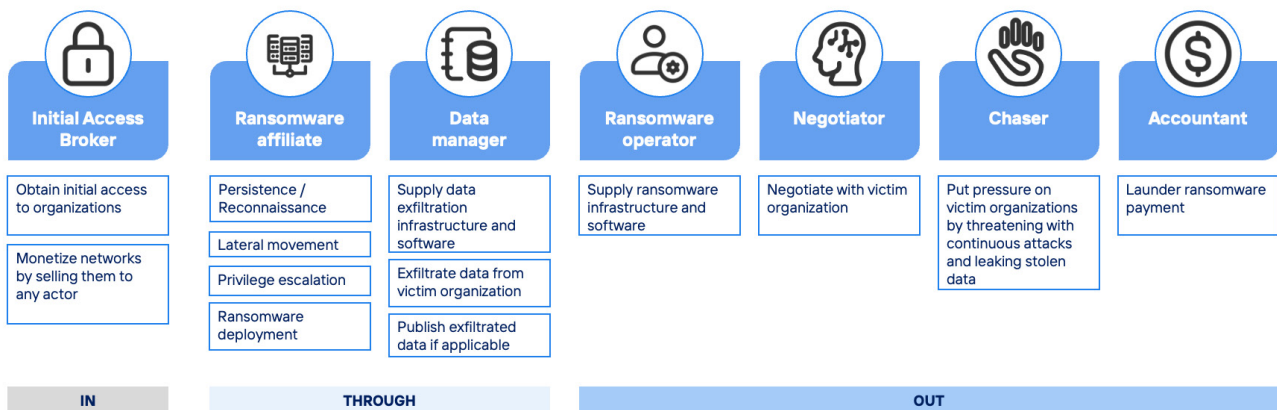


Figure 2: Model of ransomware roles [57]

Ransomware families

The modus operandi of ransomware organizations – often referred to as “families” – varies and depends on the RaaS offering. The literature identifies several ransomware families as ranking among the top three in 2021-2022. According to the Federal Bureau of Investigation (hereafter FBI), the three most common ransomware families in 2021 were Conti, Lockbit 2.0, and REvil [60], which also aligns with the NCSC’s ransomware white paper [8]. ENISA (2021b) and Sophos (2021) find that Conti and REvil were the two most common ransomware families, holding a 25-30% market share. Conti, Lockbit 2.0, and REvil all use the RaaS ecosystem, which aligns with findings by Zscaler [61] and Group-IB [62] that about eight out of 11 ransomware families use the RaaS ecosystem.

Conti is currently the most well-known ransomware family, with the Conti Leaks revealing that the family has likely obtained \$2 billion in cryptocurrency via ransomware attacks. This allowed the Conti family to continue to invest in their attack methods [19]. The family’s modus operandi is to create hostage software and deliver it to other cybercriminals. According to cybersecurity organization Northwave, ransomware families often serve as the ransomware operators within the RaaS ecosystem [57]. The cybercriminals responsible for the attacks include initial access brokers and affiliates. An affiliate then gains access to the attacked organization’s systems to install the ransomware on IT infrastructure. A ransomware family, often serving as the ransomware operator, can then use one of the other specialists to command as much ransom as possible. A ransomware family can additionally perform the roles of help desk, data manager, and negotiator [8]. Ransomware families can suddenly disappear, as occurred with the Conti family once internal disagreements led to their modus operandi becoming public (via the Conti Leaks). Usually, these ransomware families reappear under a different name with the same, albeit improved, attack techniques [7].

Extortion methods

Attack motives to deploy ransomware vary. These can be financial or meant to disrupt organizations, if not entire industries. Since 2019, there is an increase in the number of attack techniques used during an attack, which led to demanding higher ransom [48]. Ransomware attacks increasingly include double or even triple extortion [19]. According to ENISA, the use of more than one extortion technique rose significantly in 2021 [54]. One study shows a 117% increase between 2021 and 2020, mainly in the healthcare sector [61]. The rise is due to many more ransomware families, such as Conti, having started using this technique [63]. The three extortion methods are [8]:

- Single extortion (ransomware 1.0): when a victim's files are encrypted, and the decryption key may or may not be offered upon payment.
- Double extortion (ransomware 2.0): when in addition to encryption, there are threats to disclose stolen, often sensitive, data through data exfiltration. According to ENISA [54], 10 terabytes of data is stolen monthly, with 58.2% of what is stolen being related to GDPR data.
- Triple extortion (ransomware 3.0): when in addition to the above methods, customers, partners, and third parties may be extorted to pay ransom. It has become increasingly common for attackers to perform a secondary attack, such as a DDoS attack, to exert even more pressure on the organization [63].

According to specialized ransomware organization Coveware, 70% of ransomware attacks included data exfiltration tactics in the last quarter of 2020 [64]. By the first quarter of 2022, this had risen to 84% [74]. This is confirmed by Verizon [16], finding a clear trend of ransomware corresponding over time with data breaches. An additional risk is a GDPR violation fine for cybersecurity negligence when personal data is leaked due to poor IT system security.

2.4 Damage and statistics

Estimates of ransomware attacks and costs vary widely due to the complexity of making an accurate estimate. Multiple sources provide a sound indication of the impact of ransomware on various factors. From a study by Capgemini, it appears that in the first six months of 2021, there were 304.7 million ransomware attacks worldwide. This is a 150% increase from 2020 [67]. Other research finds that in the first four months of 2021, "the NCSC handled the same number of ransomware incidents as for the whole of 2020 – which itself was a number more than three times greater than in 2019" [68]. This aligns with Verizon's research in 2021 [14] and 2022 [16], with ransomware accounting for a growing share of data breaches; overall, the share of ransomware grew from 12% in 2020 to 25% in 2021. Figures from ENISA ransomware incident survey also shows more than a doubling [54].

Research from 30 countries found that the incident cost of a ransomware attack also rose sharply in 2021. In 2020, the incident cost was \$761,106; in 2021, it rose to \$1.86 million [12]. For both years, the ransom constitutes only 15% of the total ransomware attack damage to an organization [69]. Coveware provides quarterly statistics concerning ransomware attacks (Figure 3)².

2 For more details regarding the quarterly reports of Coveware see reference list entry numbers: 70, 71, 72, 73, 74, 75, 76 and 110.

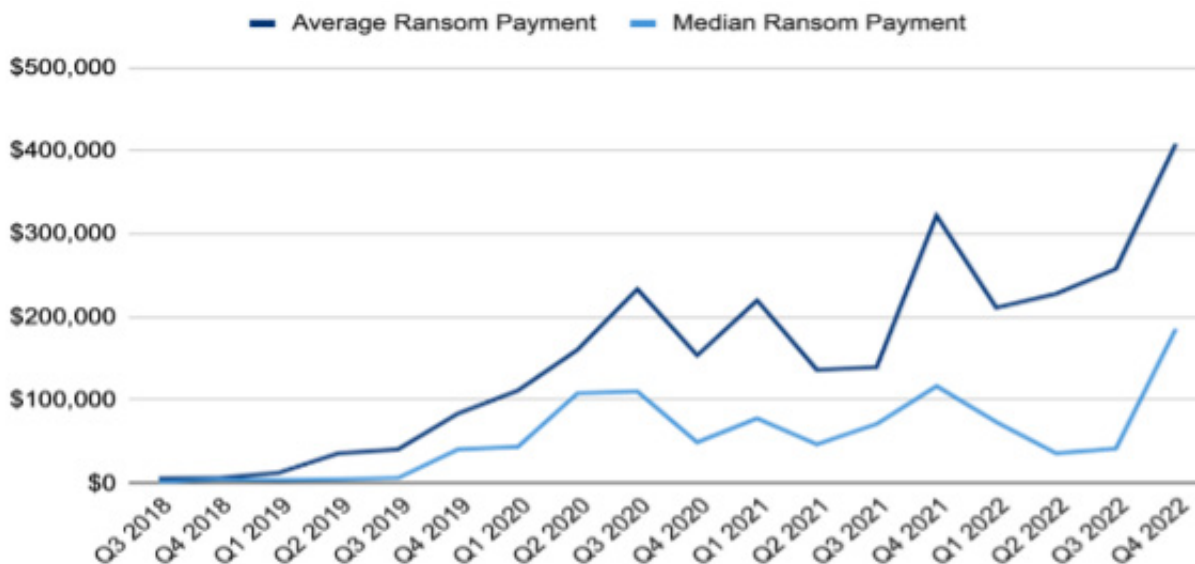


Figure 3: Coveware ransomware quarterly ransomware payments [110]

Average ransoms have been tracked quarterly by Coveware (see Figure 3). Fluctuation is due to more RaaS groupings being added or disbanded and more attacks on smaller organizations instead of multinationals (in the form of “big-game hunting”). The highest ransom demand in 2021 was by REvil, at an estimated \$70 million [54]. The Palo Alto Networks (Unit 42) find that the most attacked sectors in 2021 were professional and legal services, followed by construction, retail, and healthcare [63]. One of the reasons these sectors are popular targets is the high level of automation in their IT infrastructure. When a ransomware attack takes down IT infrastructure, it immediately has a major impact on productivity, and an attacker can leverage this method to take advantage [63].

Group-IB [62] found that in 2021, organizations in North America experienced the most ransomware attacks (52%), followed by Europe and the UK (28%). This is consistent with Palo Alto Networks (Unit 42) research [63]. Within Europe, countries most affected were the UK and France (17%), followed by Italy and Germany (15%). The Netherlands shared sixth place with Switzerland (4%) [62]. This shows that particular countries are more likely to experience a ransomware attack on an organization. However, because everything is connected to the internet, any organization can be attacked and fall victim to a ransomware attack [54].

2.5 Ransomware kill chain

“The ugly truth is – the bad guys are just better at attacking than organizations are at defending, and the former will always have the advantage over the latter. The only way organizations can truly defend themselves against Ransomware is by preventing the infection from even entering in the first place.”

JOSE MIGUEL ESPARZA, HEAD OF THREAT INTELLIGENCE OUTPOST24 [77]

The kill chain is used to analyze an adversary’s end-to-end attack steps and divide those steps into distinct conceptual phases to perform a successful attack. By analyzing the link between the phases, points in the attack pattern can be identified and the organization can apply targeted controls to defend itself for each phase, thereby breaking the chain that produces the attack. If one of these steps is interrupted, the organization might be able to prevent the attack altogether or at least limit the damage insofar as possible.

Defense group Lockheed Martin [78] has further developed this concept in the context of cyberattacks as the Cyber Kill Chain. This kill chain can help organizations learn how adversaries gain access and block their future entry [79]. It allows organizations to not only detect, but also prevent attacks and determine their cyber resilience maturity level. Still, experts agree that detection remains crucial because even if an organization can prevent 90% of ransomware attacks, a 10% chance remains that ransomware will be deployed [101]. An organization can apply cyber threat intelligence along the cyber kill chain to understand what to look for, such as malware families and specific tactics, techniques, and procedures (TTPs) [101]. Once an attack is analyzed, organizations can map potential controls against each of these attack steps. In sum, a kill chain analysis can help organizations defend themselves against complex cyberattacks [80].

NCSC kill chain

There are several ransomware kill chain models. The NCTV, in collaboration with the Dutch NCSC, created a ransomware kill chain that is a modified variant of Lockheed Martin’s Cyber Kill Chain [2]. The NCTV’s ransomware kill chain consists of five steps:

1. Obtain initial access to the target’s network by using known attack methods. The access can later be sold by the initial access broker to the ransomware affiliate.
2. Consolidate position in the network by installing additional malware.
3. Siphon off information to increase pressure and maximize the ransom.
4. Deploy the ransomware by encrypting files and blocking access.
5. Negotiate ransom and obtain the decryption key.



Figure 4: NCTV ransomware kill chain [2]

Unified Kill Chain

The kill chain of the NCTV shows at a high level the steps that ransomware attackers take. A more detailed model on the tactics of ransomware attackers is in Figure 5. The Unified Kill Chain was developed by cybersecurity researcher Paul Pols and derived from two other well-known attack models, Lockheed Martin’s Cyber Kill Chain and MITRE ATT&CK. The Unified Kill Chain model highlights 18 steps at the tactical level for a successful attack, but not every attack step occurs in every attack. The Unified Kill Chain describes three phases (In, Through, Out) to achieve the goal, including the different attack tactics [80].



Figure 5: The Unified Kill Chain [80]

Northwave kill chain

Dutch cybersecurity organization Northwave also created a ransomware kill chain model. The Northwave kill chain’s three distinct phases are derived from the Unified Kill Chain [81]. Northwave extracted the most common ransomware attacks from the Unified Kill Chain model’s 18 steps for a successful attack (Figure 6).

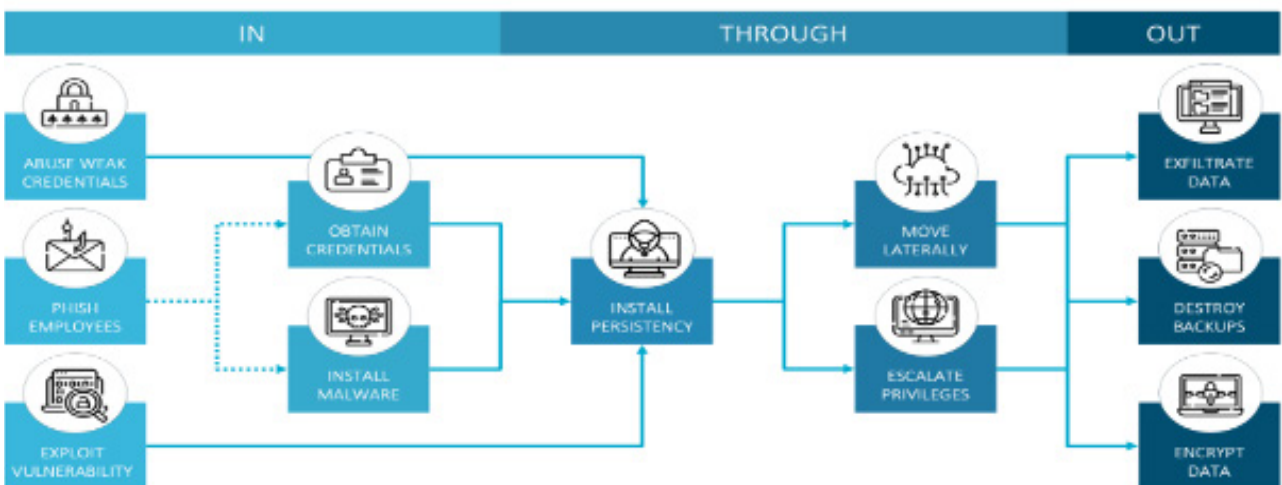


Figure 6: Northwave ransomware kill chain [81]

In the Northwave kill chain's phase 1 (In), an attacker or initial access broker can attempt to gain access into the organization's network in a number of ways, such as through the remote desktop protocol (hereafter RDP). One way of doing this can be via weak passwords, which can be easily hacked by buying them on the dark web or by brute-force attacks, inter alia. Other attack methods to penetrate the network are configuration errors or vulnerabilities in the system or phishing. Phishing can take the form of emailing compressed files that install malware or emailing a rogue link to obtain login credentials. The purpose of the IN phase is to gain access to an organization's network and then perform other actions.

In phase 2 (Through), an attacker has successfully penetrated, and backdoors can be built into the IT infrastructure to remain unseen for even an extended period of time. In this phase, an attacker will try to gain the highest possible privileges (privileged access) in the network. From there, an attacker can perform more actions in the network. Another attack method is lateral movement, which entails exploring the network for sensitive information, its crown jewels. The purpose of the Through phase is to gain more control over an organization's network.

In stage 3 (Out), the final stage, an attacker attempts to extract large amounts of data from the systems (data exfiltration), delete backups, or apply data encryption. This step is about putting as much pressure as possible on an organization to command more ransom. This phase aims to cause organizational disruption by heightening pressure and maximizing ransom.

Based on these three ransomware kill chain models, we see that a ransomware attack begins with gaining initial access to an organization's IT systems. An attacker can do this in multiple ways, including using multiple attack vectors. To reiterate, attackers are better prepared than organizations. Organizations therefore need to preemptively defend themselves against ransomware attacks by mitigating the most commonly used methodologies in the first place [77].

Kill chains and attack vectors

Coveware tracks the most common attack vectors per quarter. As in Northwave's ransomware kill chain [81], Coveware's survey identifies the top three ransomware attack vectors as: RDP compromise (including through weak passwords), phishing via email or otherwise, and the use of software vulnerabilities. In 2021, RDP and e-mail phishing, at roughly equal percentages, were the most common attack vectors. Verizon [16] and Group-IB [62] also identified these three vectors as the most common. ENISA [11] notes that in the past years, RDP attacks were most common, which aligns with Coveware's results (Figure 7). RDP and phishing are the most popular because these methods allow attackers to easily gain access to organizations' IT system and then deploy other tooling. These ransomware routes include email phishing and spear phishing attacks, RDP attacks via weak passwords and brute-force attacks, and web application attacks via software vulnerabilities [16].

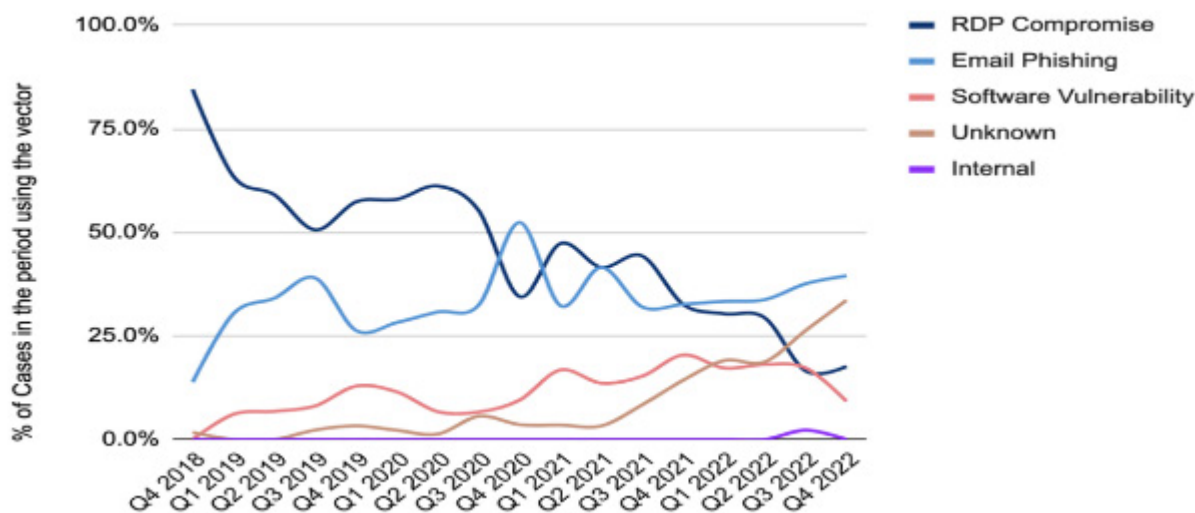


Figure 7: Initial attack ransomware attack vectors [110]

Digital supply chain & other attacks

The first quarter of 2022 showed a decrease in email phishing and RDP but an increase in other attack vectors (categorized as “unknown” or “internal”). The NCTV also noted a decrease in RDP and phishing, by email or otherwise, and the use of software vulnerabilities [2]. This is due to a growth in attacks through the software supply chain. Called a digital supply chain attack, this growing trend is an indirect attack on an organization through its software or other suppliers. In such an attack, if a supplier is hacked, companies using its software also become at risk [82]. Some well-known examples of companies that were attacked in this way are SolarWinds [83] and Kaseya [84][85].

The trend is consistent with Bommel and Augustine’s study [82], showing how an attacker finds a weakness in a vendor’s IT security, such as a zero-day vulnerability, and then installs malware to create a backdoor in the system; this enables a ransomware attack on the target itself or a large group of organizations simultaneously. ENISA also found a high growth in attacks via vendors, and reported that digital supply chain attacks quadrupled from 2020 to 2021 [86]. Gartner included digital supply chain attacks in its top seven cybersecurity risks for 2022. According to Gartner, 45% of global organizations will experience a digital supply chain attack by 2025; this is a threefold increase from 2021, so the risk of digital supply chain attacks should be a high priority in IT security [17]. TNO and the Dutch NCSC included digital supply chain attacks in their 2019-2022 research programming, recognizing that supply chains are becoming more critical because of all the organizational interdependencies [87].

Another emerging trend is recruiting “insiders” – people within the targeted organization to carry out a ransomware attack [11]. Coveware’s quarterly report [74] [76] revealed that insiders are now more often involved in ransomware attacks, which aligns with a report by cybersecurity intelligence organization Tenable [87]. Unlike digital supply chain attacks, recruiting insiders has not yet had major impact, so it is excluded from this study’s scope.

2.6 Existing security frameworks

“I’ve worked for some firms where before auditors come in, they do a big cleanup. It’s fantastic for the next three months, but then it slowly deteriorates. You need to make frameworks a part of daily life.”

ANONYMOUS US-BASED LEADER [89]

Implementing a cybersecurity framework can increase cyber resilience provided an organization’s cybersecurity maturity level also suffices. Maturity level impacts how effectively controls can be implemented [90]. The less mature an organization is, the more likely attackers can access the network, resulting in data being encrypted or stolen through data exfiltration. At a minimum, organizations should implement basic controls to minimize the likelihood and impact of a ransomware attack. As Matthijs Jaspers of the Netherlands’ Cybercrime National Police has stated: “Insufficiently implementing basic controls against ransomware lets it flourish” [23].

The challenge is to implement cybersecurity controls in a targeted and efficient manner that increases organizational cyber resilience [91]. Applied expertise and experience can reduce the likelihood and impact of a ransomware attack. An internationally accepted cybersecurity framework can be used to select the controls applicable to the identified and most common attack vectors in the ransomware kill chain. Such a framework also helps implement and maintain cybersecurity controls already in place, while guiding organizations to purposefully mitigate risks that may arise from possible gaps in resilience. Well-known cybersecurity frameworks are known for covering the entire chain of how an organization must defend against a wide variety of cybersecurity risks [92].

Most common frameworks

From the literature, several cybersecurity frameworks have emerged as being among the most used. This study report examines internationally accepted cybersecurity frameworks and draws from a large international survey with cybersecurity experts conducted by research organization ThoughtLab. To the question asking about the most appropriate and relevant cybersecurity framework to adopt to increase cyber resilience, the following answers were most commonly cited [89]:

1. ISO 27001 (48% of respondents)
2. Centre for Internet Security (hereafter CIS) (45% of respondents)
3. NIST-500-53 (40% of respondents)
4. NIST Cyber Security Framework (hereafter NIST-CSF) (32% of respondents).

A note about the two abovementioned NIST frameworks: NIST-500-53's focus area is broader in scope than the NIST-CSF and more focused on government [93]. The NIST-CSF framework addresses a higher level than the more detailed NIST-500-53, making the former more readable for management professionals without technical expertise [94]. Because the NIST-500-53 includes more than just cybersecurity controls [95], the framework is less relevant to this study than the NIST-CSF. This study report thus compares the abovementioned frameworks except NIST-500-53 as well as an additional recently published cybersecurity framework: NIST-CSF Ransomware. Drawing from these four frameworks, we examine the most relevant controls for increasing organizations' cyber resilience against ransomware. For detailed descriptions of the cybersecurity frameworks, see Appendix 3.

The frameworks compared

The four cybersecurity frameworks' most salient features are summarized in Table 1. They reflect the most important factors to consider when deciding which cybersecurity framework best suits an organization. Comparing the frameworks, we find that CIS can make the strongest contribution to creating a ransomware framework for IT experts to put directly into practice. Moreover, the CIS framework is more focused on implementing technical and operational cybersecurity controls than ISO 27001 and NIST-CSF. The CIS Controls are also more detailed in their descriptions than NIST-CSF and NIST-CSF Ransomware. As Table 1 shows, the CIS Controls cybersecurity framework focuses on the specific technical security and operational controls that the ransomware framework demands. This study report therefore adapts and builds on the CIS Controls framework, which NCSC board director Gary McAlum has also attested to, saying: "From a strategic view of what a strong security program should accomplish, the CIS Critical Controls are a great starting point" [89]. Unlike the NIST-CSF Ransomware framework, however, the CIS Controls framework is not currently focused on ransomware. To create greater, better applicable insights for organizations, moreover, the newly created NOREA Ransomware Framework includes ransomware-specific control information.

Cybersecurity framework	Focus	Description controls	Publication year	Add-ons	Certification
ISO 27001	Information security management system	Generic	2022	ISO 27002	Yes
NIST-CSF	Risk analysis & risk management controls	Generic	2018	Security groups	No
CIS Controls	Technical security & operational controls	Specific	2021	Security groups & implementation groups	No
INIST-CSF Ransomware	Risk analysis & risk management controls (ransomware)	Generic	2022*	Security groups Ransomware information	Yes

Table 1: Comparison of cybersecurity frameworks [102]

3 Ransomware in control

In chapter 2, we defined ransomware and provided a brief history. We explained how ransomware has evolved over the past few years – including how its methods have grown from single, to double, and currently triple extortion – to become a sophisticated business model executed by ransomware families. We also noted the scale of damage it has caused. Section 2.5 introduced the well-known kill chain models, visualizing the attack phases through which ransomware moves within an organization. This was followed by section 2.6, which described the most commonly used cybersecurity frameworks and compared their utility for organizations.

In this chapter, we begin with an introduction of the NOREA ransomware kill chain. Section 3.2 then goes on to describe four main mitigation strategies for managing the risks associated with the kill chain's three phases. In section 3.3, we offer guidance on how organizations seeking to protect themselves can start with the prevention controls. Section 3.4 presents the NOREA Ransomware Framework itself. Finally, section 3.5 concludes the chapter with thoughts on how to maintain and keep improving the framework.

3.1 NOREA ransomware kill chain

Because existing kill chains do not sufficiently reflect these latest developments, in this chapter we present the NOREA ransomware kill chain. We created this model (Figure 8) on the basis of the Northwave model though added the three main extortion methods that are currently applied in the Out phase. We chose to use the Northwave kill chain for its simplicity and because it is helpfully derived from the Unified Kill Chain. Furthermore, in our research we verified that these are the most common attack vectors used [11][16][62][86][110]. Above all, our aim is to offer an up-to-date depiction of ransomware attacks today so organizations can successfully prepare themselves, taking the kill chain as starting point for their prevention programs.

In creating the NOREA ransomware kill chain, we incorporated the MITRE ATT&CK tactics into our model. Short for Adversarial Tactics, Techniques, and Common Knowledge, MITRE ATT&CK is self-described as a “globally accessible knowledge base of adversary tactics and techniques based on real-world observations” [104]. MITRE ATT&CK identifies 14 global attack tactics. As these are frequently used by the cybersecurity community, we found it valuable to provide universal reference points by linking to this knowledge base.

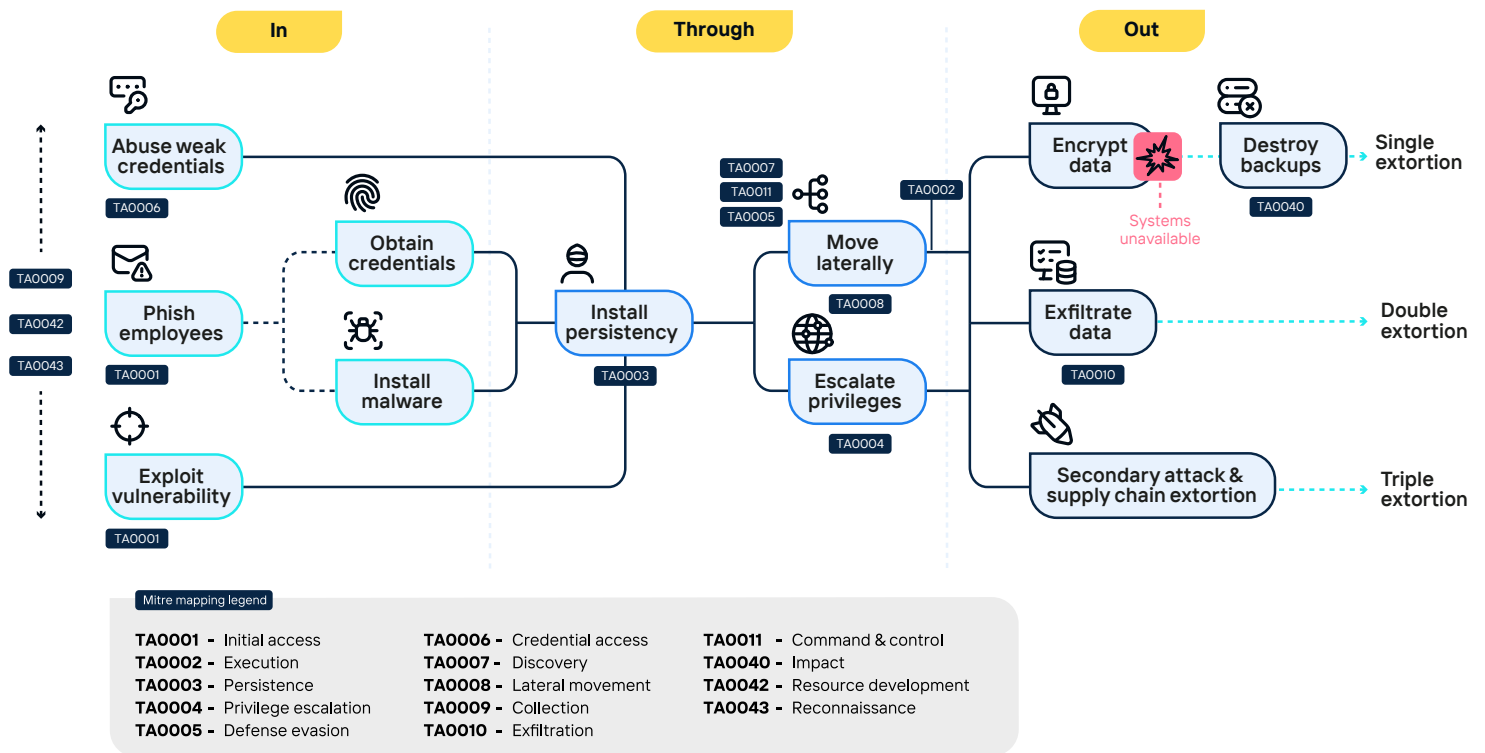


Figure 8: NOREA ransomware kill chain

3.2 Mitigation strategies

Figure 8 shows the three main kill chain phases – In, Through, Out – through which a ransomware attack spreads in an organization over time. These phases can be considered the risk domains that organizations must properly manage and prove they have control over, especially if they are obliged to under regulation. Drawing on information from our interviews, literature review, and analysis of multiple recent ransomware attacks, we developed four main mitigation strategies for properly managing the risks associated with these three kill chain phases.

Kill chain phase	Risk description	Mitigation strategy	Mitigation strategy description
In	Gain initial access into the organization's network and systems and install malware	Prevent	Preventive controls primarily focused on preventing a ransomware attacker from gaining initial access into the organization and deploying malware
Through	Escalate the initially gained access rights to administrator access rights and achieve broad lateral movement across the organization's networks	Contain	Preventive controls primarily focused on prohibiting the possibility to escalate the compromised user account to gain administrator rights and prevent lateral movement through the organization's networks Corrective controls focused on isolating and eradicating identified malware
In & Through	See above	Detect & Response	Detective controls primarily focused on detecting and alerting for malicious activity, malware, breaches, and attacks preferably as soon as possible in the ransomware kill chain

Kill chain phase	Risk description	Mitigation strategy	Mitigation strategy description
Out	Deploy the ransomware broadly in the organization's systems and render data useless (encryption), steal the data, and/or disclose the data followed by sending the ransom note	Rebuild	Corrective controls primarily focused on rebuilding the compromised environment to ensure that no traces of the used malware, ransomware, or potential backdoors are in the newly built environment NB: If an attack has reached this phase, Contain is deemed an insufficient strategy and controls are focused on rebuilding a new environment.

Table 2: Ransomware mitigation strategies

3.3 How to start

Based on our research, we propose two possible approaches for organizations to determine how and where to start with the control framework. Focused on prevention, the pragmatic approach is appropriate for organizations preferring a more general best-practices sequence of control implementation that they can begin right away. Focused on organizational context, the advanced approach is appropriate for organizations with the capacity and capability to conduct a threat assessment based on their own context-specific circumstances and, according to the kill chain mapping, to select only controls that are relevant for them.

3.3.1 The pragmatic approach: Prevention first

Approaches endorsed by IT experts, national cyber defense organizations, and International Sharing and Analysis Centers (ISACs), among other authoritative sources, all recommend that organizations seeking to protect themselves from ransomware start with prevention controls³. As stated by the head of Threat Intelligence Outpost²⁴: “The only way organizations can truly defend themselves against Ransomware is by preventing the infection from even entering in the first place” [77]. Or as Dave Woutersen, an incident handler and security specialist at the Dutch NCSC, has stated: “It’s better to avoid finding yourself with your back against the wall by undertaking all the preparations necessary to keep the miserableness out” [23]. This is in line with ISACA states: “If you’re not going to spend money on preventive control, you’re going to be spending it on incident response” [24]. From the kill chain outlined in section 3.2, we can conclude that the majority of ransomware attacks currently occurs via three main strategies: abusing weak credentials, employee phishing, and exploiting known vulnerabilities. Security measures to prevent these attacks have long been part of basic security hygiene and control frameworks; in 2022, the Dutch NCSC published a ransomware guideline with basic cybersecurity measures [25] as they believe that implementing basic, mostly preventive, controls has the biggest impact. In Figure 9, this mitigation strategy is shaded green as there is no negative impact for the organization in this phase.

³ For details on our sources associated with these organizations, see reference list entry numbers 6, 7, 11, 19, 23, 25, 37, 54, and 68.

Once main prevention controls are in place, focus should be on ensuring an organization has measures to contain infections that may still get past the prevention controls. The goal of these controls is to contain and eradicate the infection, ensuring lateral movement is stopped and organizational impact is as low as possible. Another crucial mitigation strategy concerns detection and response. Controls in this domain focus on detecting a ransomware attack as soon as possible and, once identified, to trigger a robust incident response process. In Figure 9, this mitigation strategy is shaded orange as there is negative impact on the organization.

Last comes rebuilding. If an infection has spread too far in an organization, containment and eradication are no longer a recommended strategy. Analyses of several ransomware attacks have shown that once attackers gain too much access into an organization, it becomes very difficult, if even possible, to guarantee the integrity of the environment again. In this case, a complete rebuild of the environment is the only solution. Rebuilding within an acceptable timeframe requires the organization to make serious architectural choices and often takes long to achieve. Focus should therefore, at least initially, be on the first three strategies, followed by rebuilding. In Figure 9, this mitigation strategy is shaded red as the integrity of the organization may be completely compromised.

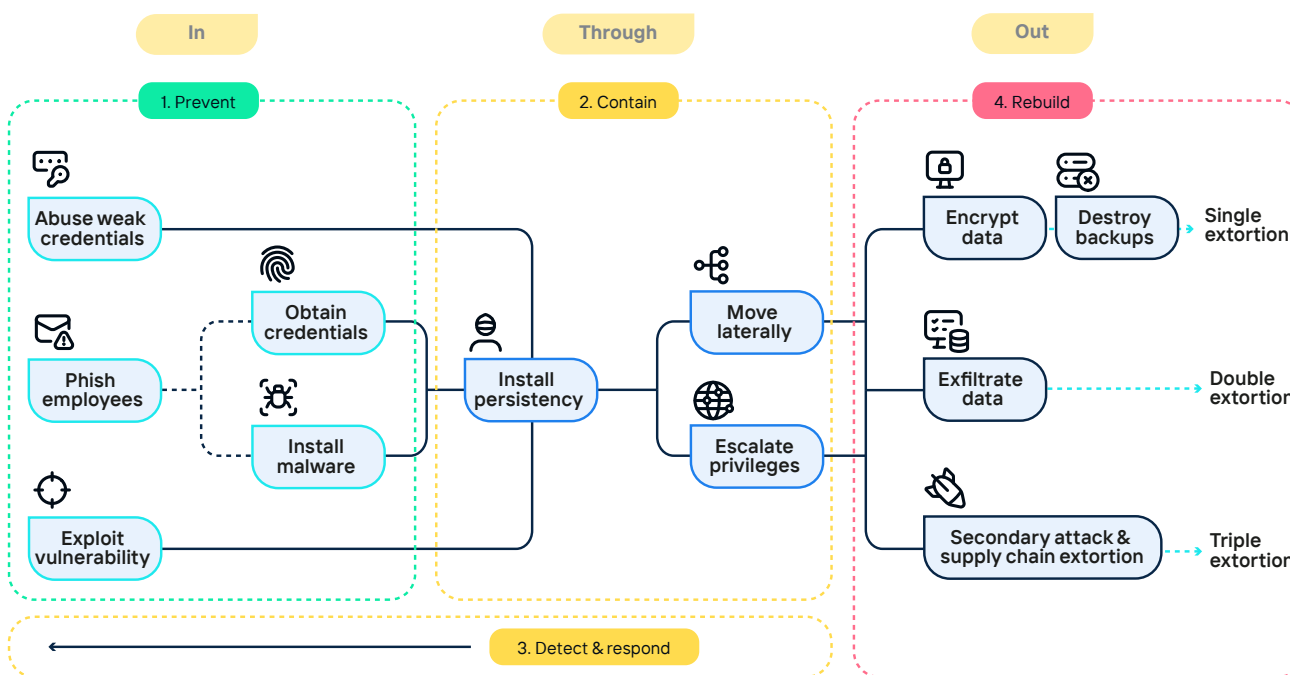


Figure 9: Norea Kill chain including mitigation strategies in sequence

3.3.2 The advanced approach: Threat assessment

Organizations that have the capacity to perform a threat assessment can do so to identify the specific ransomware threats for their specific context. This is a more efficient approach as it focuses directly on the weak spots in the organization, followed by identifying those specific controls from the framework that map to the identified threats. There are many threat assessment approaches available. We offer one example, based on a model from AWS, whose steps we have tailored to ransomware [111].

1. Identify assets: identify the systems in scope for the threat assessment to protect against ransomware.
2. Identify actors: identify the actors who frequently attack similar industries. Attackers can be classified as script kiddies, hacktivist, insider threats, organized crime, or state actors.
3. Select a model of threat factors: in this case, the NOREA ransomware kill chain can be used to identify the threat factors.
4. Brainstorm with a well-versed group of relevant experts to identify a list of threats and risks.
5. Per threat and risk, identify the mitigation controls from the framework, as based on the kill chain mapping.
6. Perform a gap assessment to determine the current implementation level of the selected mitigation controls.

3.3.3 Suggestion for further prioritization for both approaches

The CIS v8 Framework has helpfully introduced three implementation groups (IG) for further prioritization of implementation sequence. IG1 controls are essential for organizations' basic digital hygiene, IG2 controls are useful for more complex organizations, and IG3 controls concern organizations that employ their own cybersecurity experts since they often perform important functions within society. We encourage organizations to make use of the IG prioritization if further refinement of prioritization is needed by taking the following steps:

1. Start with implementing the IG1 controls following the sequence of the Prevent, Contain, Detect & Response, and Rebuild mitigation strategy.
2. Implement the IG2 controls following the same mitigation strategy sequence.
3. Implement the IG3 controls following the same mitigation strategy sequence.

3.4 NOREA Ransomware Framework

Given the complexity of a ransomware attack and the fact that no single control can fully protect against ransomware, we saw an increasingly urgent need in the market for a specific ransomware framework.

As mentioned in chapter 2, we selected CIS v8 to serve as the basis for the framework introduced in this section because it is currently the most elaborate and complete starting point. Based on available guidance, largely from international governmental cyber defense organizations and Sharing and Analysis Centers (ISACs) as well as supplemented by interviews with experts, we made the following additions to the framework:

- Selection of which CIS controls are relevant to protect against ransomware
- Mapping the controls to the 12 specific attack steps of the kill chain within these main phases (column 4)
- Supplementing the selected controls where needed with specific ransomware control activities that are required, as based on all internationally available guidelines and interviews with experts (column 5)
- Mapping the controls to the three main phases of a ransomware attack (column 6)
- Mapping the controls to the four mitigation strategies we developed (columns 7-10)

In total, of the 153 CIS v8 controls, 89 (58%) were selected for the NOREA Ransomware Framework, of which Table 3 provides an overview.

Domains CIS	CIS controls	Ransomware controls	Prevent controls	Contain controls	Detect & Response controls	Rebuild controls
1 - Inventory and control of enterprise assets	5	2	2	0	1	1
2 - Inventory and control of software assets	7	5	5	0	1	1
3 - Data protection	14	1	1	0	0	0
4 - Secure configuration of enterprise assets and software	12	8	2	5	0	1
5 - Account management	6	3	3	1	0	0
6 - Access control management	8	7	7	7	0	0
7 - Continuous vulnerability management	7	7	7	0	0	0
8 - Audit log management	12	4	0	0	4	0
9 - Email and web browser protections	7	6	6	0	0	0
10 - Malware defenses	7	7	7	0	0	0
11 - Data recovery	5	5	0	0	0	5
12 - Network infrastructure management	8	4	1	3	0	2
13 - Network monitoring and defense	11	4	2	1	3	0
14 - Security awareness and skills training	9	6	6	0	1	0
15 - Service provider management	7	4	3	2	2	3
16 - Application software security	14	5	5	0	0	0
17 - Incident response management	9	8	0	1	8	0
18 - Penetration testing	5	3	3	0	0	0
TOTAL	153	89	60	20	20	13

Table 3: Overview of ransomware framework controls

In figure 10, the CIS domains are plotted on the kill chain to illustrate the required control domains that need to be addressed for each of the three kill chain phases.

3.4.1 Major point of attention: Rebuild capability

Figure 10 shows that the CIS domains do not provide sufficient attention for a complete rebuild of the IT environment, nor do any other control frameworks. We have therefore added the most specific ransomware control activities (column 5) to the domains in scope for the rebuild mitigation strategy. Examples of attention points include:

- Implement infrastructure as code (IaC) best practices, at least for critical applications and associated supporting applications and services, to drastically increase the time for rebuild activities. IaC entails the use of appropriate technology and a way of working in line with the DevOps model. Interactive configuration management tools enable infrastructure components (such as networks, virtual machines, and load balancers) and applications to be defined and deployed automatically rather than manually. This greatly enhances speed, consistency, and quality.
- Ensure that backups are performed not only for application data, but also for server snapshots and images, IaC scripts and orchestration tooling data, active directory, and other components critical for rebuilding an application stack.
- Attend to applying a more robust backup strategy against ransomware, such as to achieve immutability of the backup data. Consider, for example, a 3:2:1 strategy as recommended by the Dutch NCSC [25]. Other possible strategies include applying strict access control to backup applications and data such as by using a separate network, authentication domain, and active directory, thereby ensuring that lateral movement to these systems is not possible.
- Ensure that data recovery test scenarios contain the rebuild of a complete application stack to ensure the maturity of the rebuild capability.
- Treat backup management more holistically rather than approach each application or database as an isolated instance for which backups need to be created. In practice, applications often facilitate and are part of many business processes, thus also being part of a chain of applications that make changes to the data. In the backup management process, this added complexity must be accounted for, as it can influence the way, frequency, and point in time that the backup is made.

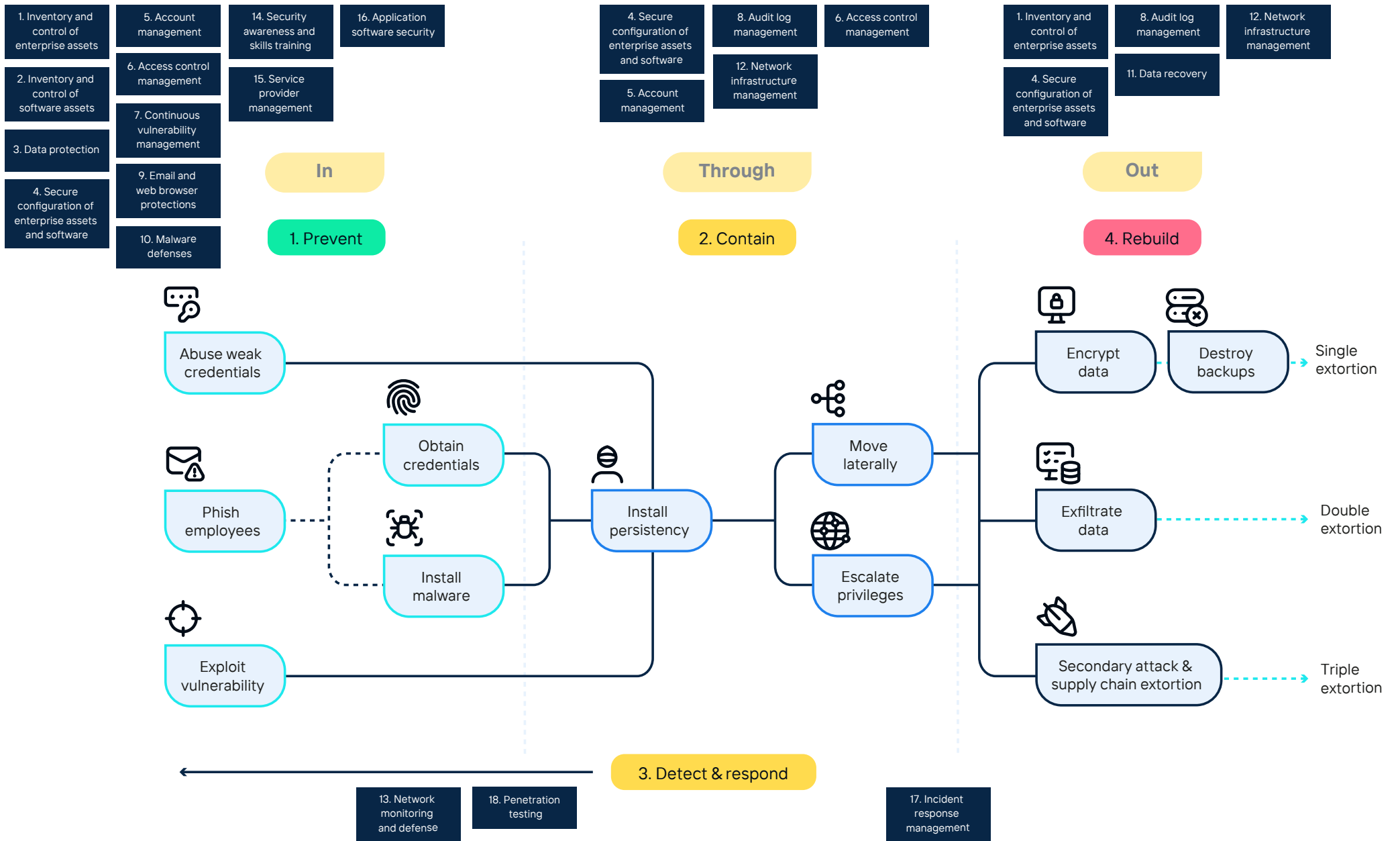


Figure 10: Control domains plotted on the NOREA kill chain

3.4.2 Framework maintenance

The NOREA Ransomware Framework presented below is groundbreaking because it is the first of its kind to be created and freely disseminated. However, we see it as just one step in the ongoing journey to combat this global cyber threat. The control framework addresses the current state of ransomware and world affairs as best as possible. Yet, we acknowledge that no control framework can ever be considered complete or finished. Technology keeps evolving. Alas, cyberattack tactics and techniques do too.

Because our aim is to maintain and continuously enhance this framework, we are publishing it as an open source tool. We invite security experts, IT professionals, and anyone else interested in or affected by ransomware to share experiences, ideas, and strategies for how organizations can better prevent attacks and protect themselves.

While a condensed table of our framework is embedded in this document, the full version has been made available via GitHub. We formatted the file in Excel because it is user-friendly and easy to edit. Take a look, download the file, and contribute to keeping it relevant and rigorous. We welcome your comments and feedback.

Link (also accessible to non-GitHub account holders)



CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
Inventory and Control of Enterprise Assets		Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.							
1,1	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	Exploit vulnerability	Ensure to include RDP solutions in the asset inventory.	IN	X			X
1,2	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	Phish employees Exploit vulnerability	See also 13.5	IN	X		X	

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
Inventory and Control of Software Assets		Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.							
2,1	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Exploit vulnerability		IN	X			X
2,2	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Exploit vulnerability		IN	X		X	
2,5	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	Exploit vulnerability Install persistency	Ensure that only authorized software (applications, libraries, code, scripts) is allowed to be executed. Potentially this can be done through Microsoft Software Restriction Policy or AppLocker. Ensure that unsigned macro's are blocked from execution.	IN THROUGH	X			
2,6	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.	Exploit vulnerability Install persistency	In cases where Windows operating systems are used Windows Defender Application Control can be used to achieve further control on the executing of undesired scripts or software.	IN THROUGH	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
2,7	Allowlist Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	Exploit vulnerability Install persistence	Ensure to restrict usage of PowerShell, using Group Policy, to specific users, locations or paths on a case-by-case basis. Consider putting PowerShell in constrained language mode to further prevent misuse.	IN THROUGH	X			
Data Protection		Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.							
3,3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Abuse weak credentials		IN	X			
Secure Configuration of Enterprise Assets and Software		Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).							
4,1	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Install malware Install persistence Move laterally Escalate privileges	Ensure specific attention is paid to domain controllers. Important configurations are: <ul style="list-style-type: none"> Limiting the installation of additional/unnecessary software Removal of unnecessary software Disable unnecessary services Restrict internet connectivity (e.g. through outbound firewall proxy) Related to control 16.7 on hardening.	IN THROUGH	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
4,2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Exploit vulnerability Install persistency Move laterally	Ensure that the network devices (such as firewalls, VPN, Load balancers) are kept strictly updated. Ensure that firewall rules are documented and regularly reviewed.	IN THROUGH OUT		X		
4,4	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	Move laterally Exfiltrate data	Ensure that firewalls are restricting port access on the network. Ensure implementing Deny by Default on firewalls.	THROUGH OUT		X		
4.5	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Move laterally Exfiltrate data	Ensure that firewalls are restricting access on the network (e.g. through whitelisting). Where necessary block remote IT management tools such as Teamviewer. Ensure implementing Deny by Default on firewalls.	THROUGH OUT		X		
4,6	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	Encrypt data Destroy backups	Implementing & safeguarding IaC and orchestration configurations & documentation for at least critical systems to enable (rapid) rebuild of complete application stacks during the response phase. See also control 11.1. Ensure that the availability and capability is present to rebuild a new infrastructure and application environment.	OUT				X

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
4,9	Configure Trusted DNS Servers on Enterprise Assets	Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.	Move laterally Encrypt data Exfiltrate data	Include the configuration to alert on anomalous DNS tunneling in a network. Ensure that DNSSEC is configured on the DNS servers to define which DNS servers can send responses back.	THROUGH OUT		X		
4,11	Enforce Remote Wipe Capability on Portable End-User Devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.	Move laterally Exfiltrate data		THROUGH OUT		X		
4,12	Separate Enterprise Workspaces on Mobile End-User Devices	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.	Phish employees Exploit vulnerability		IN	X			
Account Management		Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.							
5,2	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	Abuse weak credentials Phish employees Obtain credentials	Ensure to implement more extensive password requirements in a password policy, such as: account lockout policy, disabling re-used of passwords across different services, change passwords at least every 60 days, use of password managers, include password complexity, etc.	IN	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
5,3	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	Abuse weak credentials Obtain credentials		IN	X			
5,4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	Abuse weak credentials Move laterally Escalate privileges	<p>Only allow network support personnel administrative access to endpoints, domain controllers, workstations, and network resources (least privilege). Revoke administrative access of all other/ non-relevant parties/persons.</p> <p>Make sure to limit the use of domain administrator accounts to only perform maintenance on the domain.</p> <p>Ensure that in cases that services need administrative privileges to run, that these rights are provided as Local System as this allows applications to have high privileges locally but can't be used to move laterally.</p>	IN THROUGH	X	X		

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
Access Control Management		Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.							
6,1	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	Abuse weak credentials Move laterally Escalate privileges	Ensure granting access to employees and services is done based on a zero-trust model and level of access is based on the least-privilege principle. Ensure that real-time overviews of access rights per person/role are available including reporting on toxic combinations. Review of these overviews is part of control 6.8.	IN THROUGH	X	X		
6,2	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	Abuse weak credentials Move laterally Escalate privileges		IN THROUGH	X	X		
6,3	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	Abuse weak credentials Move laterally	Require MFA for all employees for all services (not only externally-exposed services such as virtual desktop services, RDP and remote IT management tools). Exceptions need to be documented and approved, with additional mitigation controls. Avoid call & SMS-based MFA methods.	IN THROUGH	X	X		
6,4	Require MFA for Remote Network Access	Require MFA for remote network access.	Abuse weak credentials Move laterally	Exceptions need to be documented and approved.	IN THROUGH	X	X		

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
6,5	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	Abuse weak credentials Move laterally Escalate privileges	Require MFA for all admin accounts. Exceptions need to be documented and approved.	IN THROUGH	X	X		
6,7	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.	Abuse weak credentials Move laterally Escalate privileges	Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.	IN THROUGH	X	X		
6,8	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.	Abuse weak credentials Move laterally Escalate privileges	Perform access control reviews based on a frequency that determined by the associated risk or criticality, but at least on at least quarterly basis and ideally automated. Particularly Remote Monitoring and Management accounts that are publicly accessible—this includes audits of third-party access given to MSPs.	IN THROUGH	X	X		

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
Continuous Vulnerability Management		Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.							
7,1	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Exploit vulnerability		IN	X			
7,2	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	Exploit vulnerability		IN	X			
7,3	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Exploit vulnerability Escalate privileges	Ensure proper enlisting for patch feeds for all used operating systems within the organization. Ensure that all patches are prioritized based on potential vulnerability threat and implemented according to this priority. Make use of central insight to monitor proper rollout of all patches (e.g. through WSUS or SCCM). In case of vulnerable legacy systems that are out of support for patching or cannot be updated, ensure these systems are isolated in the network and do not have access to the internet.	IN	X			
7,4	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Exploit vulnerability Escalate privileges	Ensure proper enlisting for patch feeds for all used software within the organization. Ensure that all patches are prioritized based on potential vulnerability threat and implemented according to this priority.	IN	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
7,5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.	Exploit vulnerability		IN	X			
7,6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.	Exploit vulnerability		IN	X			
7,7	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	Exploit vulnerability		IN	X			
Audit Log Management		Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.							
8,6	Collect DNS Query Audit Logs	Collect DNS query audit logs on enterprise assets, where appropriate and supported.	Install malware Install persistency Move laterally Escalate privileges	Ensure that next to DNS logging also file system access is logged to enable identification of data exfiltration events. Ensure proper retention of DNS query log, as it is also crucial for forensics. See 8.10.	IN THROUGH			X	
8,7	Collect URL Request Audit Logs	Collect URL request audit logs on enterprise assets, where appropriate and supported.	Install malware Install persistency Move laterally Escalate privileges		IN THROUGH			X	

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
8,8	Collect Command-Line Audit Logs	Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.	Install malware Install persistency Move laterally Escalate privileges		IN THROUGH			X	
8,10	Retain Audit Logs	Retain audit logs across enterprise assets for a minimum of 90 days.	Install malware Install persistency Move laterally Escalate privileges	Restrict access to log files and store them in a separate network segment. Evaluate based on the companies risk profile if 90 days is sufficient.	IN THROUGH			X	
Email and Web Browser Protections		Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.							
9,1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	Phish employees Exploit vulnerability	Only use browser and email client plugins that are needed for daily operations. Also, disable all unnecessary browser and email client plugins.	IN	X			
9,2	Use DNS Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.	Exploit vulnerability		IN	X			
9,3	Maintain and Enforce Network-Based URL Filters	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.	Obtain credentials		IN	X			
9,4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.	Exploit vulnerability		IN	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
9,5	Implement DMARC	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.	Phish employees Obtain credentials	Ensure that the DMARC policy must at the very least be set to quarantine status. This will move all incoming emails to the SPAM folder when they fail the DMARC test to make users aware of the (potentially) malicious and harmful contents in the SPAM-marked emails.	IN	X			
9,7	Deploy and Maintain Email Server Anti-Malware Protections	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	Obtain credentials Install malware	Ensure that filters are implemented at the email gateway to filter out emails with known malicious indicators and block suspicious Internet Protocol (IP) addresses at the firewall.	IN	X			
Malware Defenses		Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.							
10,1	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.	Install malware	<p>Ensure that the anti-malware solution (e.g. End Point Security) is supplemented by EDR (Endpoint Detection and Response) capabilities for all assets (including endpoint devices and servers) on which anti-virus is installed.</p> <p>See also control 2.6 on the use of Windows Defender Application Control.</p> <p>Ensure that there is a list of legacy systems that do not support anti-malware and EDR solutions and that other mitigation measures (such as isolation) are implemented for these systems.</p>	IN	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
10,2	Configure Automatic Anti-Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.	Install malware	Anti-malware solutions have Global Trend Intelligence (GTI) functionalities where the hashes of suspicious files are send to the global lab database to be validated if they are malware (based on e.g. new IoC's). This is a real-time functionality, whereas signature file update occurs every 24 hours (or later).	IN	X			
10,3	Disable Autorun and Auto-play for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.	Install malware		IN	X			
10,4	Configure Automatic Anti-Malware Scanning of Removable Media	Configure anti-malware software to automatically scan removable media.	Install malware		IN	X			
10,5	Enable Anti-Exploitation Features	Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.	Install malware		IN	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
10,6	Centrally Manage Anti-Malware Software	Centrally manage anti-malware software.	Install malware	<p>Ensure that anti-virus and anti-malware solutions are properly configured to ensure that the right checks and functionalities are enabled, such as directly blocking of malicious software instead of alerting or putting in 'observer' mode.</p> <p>Ensure that tamper protection of anti-malware/virus scanning tools is enabled to ensure attackers cannot disable the products.</p>	IN	X			
10,7	Use Behavior-Based Anti-Malware Software	Use behavior-based anti-malware software.	Install malware	See also control 10.1.	IN	X			
Data Recovery		Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.							
11,1	Establish and Maintain a Data Recovery Process	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Encrypt data	Ensure that in establishing the data recovery process the proper scope is included. The determination of the scope should take into account the scenario that the organization will be in need of rebuilding the complete network and applications environment. Typically the scope for the backup management process will be extended with, for example, application (golden)images/snapshots, account (AD) structure, IaC and orchestration configurations and documentation.	OUT				X

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
11,2	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	Encrypt data	<p>Ensure a backup policy is in place that includes:</p> <ul style="list-style-type: none"> ▪ RPO and RTO objectives to properly configure backup frequency and type of backups. ▪ For critical systems ensure a RPO of seconds and an RTO of minutes (maximum one hour). See control 1.1 and 2.1 for overview of (critical) assets to ensure completeness. ▪ Ensure the backups include the IaC data as well as mentioned in control 4.6. 	OUT				X
11,3	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Encrypt data Exfiltrate data	<p>Ensure that access to backups is secured by using for example a different authentication domain, network and active directory.</p>	OUT				X
11,4	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.	Encrypt data Exfiltrate data	<p>Ensure a 3:2:1 backup implementation is applied, at least for business critical applications and data (3 copies, on 2 different media types, and 1 offline/immutable).</p> <p>Ensure that the back-up application is configured in such a way that the data cannot be overwritten by a person or service, called write once read many (WORM) to achieve immutability.</p> <p>Ensure that the NTP server time settings are restricted and monitored.</p>	OUT				X

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
11,5	Test Data Recovery	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.	Encrypt data	<p>Ensure that test scenario's include the rebuild of complete (working) application stacks and not just focused on backup/ data restore.</p> <p>Evaluate based on the organizations risk profile what test frequency is sufficient or if testing needs to be automated and tested for example on a daily basis.</p>	OUT				X
Network Infrastructure Management		Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.							
12,2	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.	Move laterally Exfiltrate data	<p>Ensure proper attention is paid to network segmentation that fits the organizations risk profile. Typical network segmentation is implemented by segmenting O, T, A and P environments supplemented by further segmentation based on data classification (e.g. putting sensitive or classified information in a different network segment).</p>	THROUGH OUT		X		X
12,4	Establish and Maintain Architecture Diagram(s)	Establish and maintain architecture diagram(s) and/ or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Move laterally Exfiltrate data	<p>Ensure that the network diagram include depictions of covered major networks, any specific IP addressing schemes, and the general network topology (including network connections, interdependencies, and access granted to third parties or MSPs).</p>	THROUGH OUT		X		X

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
12,7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.	Abuse weak credentials Exploit vulnerability	If RDP is used, place it behind a firewall and ensure it must be accessed through a proper VPN. Alternatively, periodically review whether RDP is needed to be used. Periodically review whether port 3389 (enables users to access remote computers) is not externally accessible (to the public) via the internet. This can be done by performing (automatic) vulnerability scans. If not, consider closing port 3389 due to its vulnerabilities. Log RDP login attempts and enforce account lockouts after a specified number of attempts.	IN	X			
12,8	Establish and Maintain Dedicated Computing Resources for All Administrative Work	Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.	Move laterally		THROUGH		X		

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
Network Monitoring and Defense		Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.							
13,1	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.	Abuse weak credentials Exploit vulnerability Install malware Move laterally Escalate privileges Encrypt data Exfiltrate data	<p>Properly assess which key alerts related to ransomware need to be implemented on both the internal and external network traffic, for example:</p> <ul style="list-style-type: none"> ▪ alert on generic malicious activity in logfiles, including known IOC's (e.g. based on third-party IOC subscription) ▪ alert on executable files that attempt to connect to the internet (unauthorized) ▪ alert when large amounts of data are exfiltrated without approval ▪ alert when anti-virus and anti-malware solution report malicious scripts in the windows event logs ▪ alert on the deletion of anti-virus and anti-malware software on active servers ▪ alert on suspicious activity with the domain administrator account. <p>Ensure that proper analysis has been performed on what crucial source logfiles are needed to implement the proper alerts (e.g. PowerShell Command Execution logging).</p> <p>Ensure that the respective team performs proper threat intelligence management (insight in latest APT's, IOC's and IOA's) to continuously learn and update the applicable log and alerting processes (e.g. read threat intelligence reports of well-known cybersecurity firms)</p> <p>Ensure that the chosen technology allows for threat hunting and the ability to recreate the threat actors actions.</p>	IN THROUGH OUT	X		X	

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
13,4	Perform Traffic Filtering Between Network Segments	Perform traffic filtering between network segments, where appropriate.	Move laterally		THROUGH		X	X	
13,5	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.	Abuse weak credentials Phish employees Obtain Credentials Install malware Exploit vulnerability	Implement an end-user device compliance policy where end-user devices that do not meet company set (patch) policy are treated as unauthorized assets and removed or denied access from the network.	IN	X			
13,6	Collect Network Traffic Flow Logs	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.	Move laterally	In addition to 13.1 think of following suspicious activities to alert on: <ul style="list-style-type: none"> TOR traffic Connections to known C2 servers Traffic related to know exploit kits Traffic to suspicious/criminal activity related websites <p>In case of an attack, ensure that monitoring is performed for the Indicators of Compromise (IoC's) used.</p>	THROUGH			X	
Security Awareness and Skills Training		Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.							
14,1	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	Abuse weak credentials Phish employees Exploit vulnerability		IN	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
14,2	Train Workforce Members to Recognize Social Engineering Attacks	Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.	Abuse weak credentials Phish employees Obtain credentials Exploit vulnerability	It is highly recommended to execute phishing awareness campaigns multiple times per year. Include in the training program also practical information on how to recognize a ransomware infection and how to react.	IN	X			
14,3	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	Abuse weak credentials Phish employees Obtain credentials Exploit vulnerability	Include in the training that private passwords are not allowed to be re-used for company access. Ensure that users are properly educated on not accepting unexpected two-factor authentication (2FA).	IN	X			
14,6	Train Workforce Members on Recognizing and Reporting Security Incidents	Train workforce members to be able to recognize a potential incident and be able to report such an incident.	Abuse weak credentials Phish employees Exploit vulnerability Secondary Attack	Provide the option for personnel to easily report suspicious emails.	IN OUT	X		X	
14,7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	Abuse weak credentials Phish employees Exploit vulnerability		IN	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
14,8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.	Abuse weak credentials Phish employees Exploit vulnerability		IN	X			
Service Provider Management		Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.							
15,1	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	Abuse weak credentials Phish employees Exploit vulnerability Secondary Attack	Ensure that service providers are properly classified to know which providers manage critical applications and data.	IN OUT				X
15,2	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.	Abuse weak credentials Phish employees Exploit vulnerability		IN	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
15,4	Ensure Service Provider Contracts Include Security Requirements	Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.	Abuse weak credentials Phish employees Exploit vulnerability Obtain credentials Install malware Install persistency Move laterally Escalate privileges Exfiltrate data Destroy backups Encrypt data Secondary Attack	Ensure that per service provider it is documented which provider has access to the companies network and what type of access (e.g., VPN, RDP, patching). Based on this, ensure proper security measures are agreed to prevent ransomware spread from the service provider. See also domains 12 & 13.	IN THROUGH OUT	X	X	X	X
15,5	Assess Service Providers	Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.	Abuse weak credentials Phish employees Exploit vulnerability Obtain credentials Install malware Install persistency Move laterally Escalate privileges Exfiltrate data Destroy backups Encrypt data Secondary Attack		IN THROUGH OUT	X	X	X	X

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
Application Software Security		Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.							
16,2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.	Exploit vulnerability		IN	X			
16,5	Use Up-to-Date and Trusted Third-Party Software Components	Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.	Exploit vulnerability		IN	X			
16,7	Use Standard Hardening Configuration Templates for Application Infrastructure	Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.	Exploit vulnerability		IN	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
16,9	Train Developers in Application Security Concepts and Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.	Exploit vulnerability		IN	X			
16,12	Implement Code-Level Security Checks	Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.	Exploit vulnerability		IN	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
Incident Response Management		Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.							
17,1	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	All	<p>Ensure that the selected key person has the right mandate to take potentially drastic decisions in case of an attack (e.g. close off networks or in a worst case scenario pay the ransom) and that the mandate is approved by the board.</p> <p>Ensure that in the process attention it paid that the designated personnel is available 24x7 for contacting in case of an (ransomware) incident.</p> <p>Ensure that proper contact details are available for contacting the designated personnel outside business hours.</p> <p>Properly evaluate the need to preselect an experienced ransomware negotiation firm as this process is challenging and required knowledge and experience.</p> <p>If you don't have a permanent organization that manages security incidents, it is recommended using the ICS (Incident Command System) as a temporary organizational structure to handle the crisis.</p> <p>Refer also to NIST SP800-184 (Guide for Cybersecurity Event Recovery).</p>	IN THROUGH OUT			X	

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
17,2	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	All	<p>Make agreements on and create a procedure to contact regulators, legal counsel and the cyber insurance company (if applicable) so that they are immediately notified when a ransomware attack occurs. Take account of regulatory timelines that might be applicable (e.g. in case of GDPR).</p> <p>Make agreements on and create a procedure on the step to take in case of a ransomware attack, such as contact specific law enforcement agencies, what digital evidence to collect and secure, what other relevant parties are required to be notified etc.</p>	IN THROUGH OUT			X	
17,3	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	All		IN THROUGH OUT			X	

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
17,4	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	All	<p>Ensure the inclusion/adaptation towards a ransomware response plan and/or ransomware playbook that includes at least the following activities:</p> <ul style="list-style-type: none"> ▪ containment steps after identification of an infection such as disabling systems from the network and how to perform this properly. ▪ disabling all or all infected user accounts, potentially followed by resetting these accounts. ▪ Reset of authentication methods used such as passwords for administrator and other system and service accounts. ▪ Disable write/edit rights on files ▪ Validate if MFA is still enabled on all required accounts/services. ▪ Block suspicious network activity. <p>Ensure the response plan includes a strategy on how to respond to a ransom note. Responding to the ransom note is important to gather information that might be crucial for the response. Note: contacting the attacker does not mean that we imply to pay the ransom. The advice from the government is to not pay any ransom.</p> <p>Ensure that the communication plan is reviewed by legal and compliance departments to ensure that (public) communication does not breach applicable regulation.</p>	IN THROUGH OUT			X	

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
17,5	Assign Key Roles and Responsibilities	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	All	Ensure that key roles and responsibilities are available for (ransomware) forensic activities as well. The organization should have arranged for the ability and technology to perform forensics activities on the environment in case of an attack to determine for example the impact, timelines, containment, eradication, assistance with (regulatory) reporting	IN THROUGH OUT			X	
17,6	Define Mechanisms for Communicating During Incident Response	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	All		IN THROUGH OUT			X	
17,7	Conduct Routine Incident Response Exercises	Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.	All	Ensure that the incident response exercises include ransomware scenario's. Based on the applicable industry, there might be additional requirements from regulators (e.g. DNB). See also 11.5: Ensure that test scenario's include the rebuild of complete application stacks.	IN THROUGH OUT			X	
17,8	Conduct Post-Incident Reviews	Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.	All	Based on the applicable industry, there might be additional requirements from regulators (e.g. DNB) on sharing the reviews with them as well.	IN THROUGH OUT			X	

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
Penetration Testing		Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.							
18,1	Establish and Maintain a Penetration Testing Program	Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.	Abuse weak credentials Phish employees Exploit vulnerability Obtain credentials Install malware Install persistency Move laterally Escalate privileges Exfiltrate data Destroy backups Encrypt data Secondary Attack		IN THROUGH OUT	X			

CIS Safeguard	CIS Title	CIS Description	NOREA kill chain step	Special ransomware attention points	Ransomware phase	1.Prevent	2.Contain	3.Detect & Response	4.Rebuild
18,2	Perform Periodic External Penetration Tests	Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.	Abuse weak credentials Phish employees Exploit vulnerability Obtain credentials Install malware Install persistency Move laterally Escalate privileges Exfiltrate data Destroy backups Encrypt data Secondary Attack	Include in the reconnaissance phase information on the darkweb related to the organization and the organization's key personnel. Information could relate to disclosure of a successful ransomware attack, information on planning an attack, disclosure of stolen information of the organization including user account information.	IN THROUGH OUT	X			
18,3	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.	Abuse weak credentials Phish employees Exploit vulnerability Obtain credentials Install malware Install persistency Move laterally Escalate privileges Exfiltrate data Destroy backups Encrypt data Secondary Attack		IN THROUGH OUT	X			

4 Conclusion

The need for digital resilience has never been more urgent. Due to the demands of rapid digitalization, all major business processes rely on software and enterprise technology has become indispensable for daily operations. As such, the impact of security incidents on organizations is dramatically evolving; an incident that may have once been an inconvenience can now jeopardize business continuity or even threaten an organization's existence. Responding to ransomware also requires a broad combination of measures; an effective backup strategy, zero trust architecture, or a highly segmented network is not enough. What's more, ransomware is the first security threat that demands organizations be prepared to rebuild their IT landscape completely; prior to ransomware, a recovery or clean-up strategy could suffice. Achieving a successful rebuild capability takes tremendous investments, including new (resilient) architecture choices, new ways of working, and an adaptive mindset to enable fast decision-making. In short, ransomware forces both victims and would-be victims to pay very high prices.

Mapping controls on a framework and responding to potential threats with security and mitigation measures can go a long way. However, organizations still need to strategize digital resilience in view of their own risk appetite, threat assessment, and available capacities and capabilities. In a world rife with ransomware, organizational leaders are thus faced with considerable questions. Has the organization planned what to do if an attack renders its entire IT landscape unavailable? Has such a scenario been exercised? What if the integrity of the data itself is affected? Is the backup data secure and immutable enough? Besides database backups, are there also secure backups and documentation to rebuild application stacks from the ground? Is the organization's recovery time objective (RTO) adjusted in anticipation of a ransomware attack, which, experts agree, is likely to happen? Are employees aware enough to identify suspicious activity and do they know how to report such activity?

In ransomware we face the most impactful cyber threat yet. Its complexity lies not just in its potential destruction, but the herculean amount of work required to thwart it. For clear guidance, however, we can now turn to a professionally validated and universally applicable framework: the NOREA Ransomware Framework. In selecting the most relevant controls to protect and recover from an attack, this new framework holds the potential of helping organizations build even greater digital resilience.

References

- [1] Palmer, D. (2022, 28 June). *Ransomware is the biggest global cyber threat. And the attacks are still evolving*. ZDNet. Accessed on 1 July 2022. <https://www.zdnet.com/article/ransomware-attacks-are-the-biggest-global-cyber-threat-and-still-evolving-warns-cybersecurity-chief>
- [2] NCTV. (2021, June). Cybersecuritybeeld Nederland CSBN 2021. <https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021>
- [3] Gartner. (2021). 2022 Audit Plan Hot Spots. In Gartner. <https://emtemp.gcom.cloud/ngw/globalassets/en/risk-audit/documents/2022-audit-plan-hot-spots.pdf>
- [4] Accountant.nl. (2022, 20 January). ING: belangrijker rol bij cybersecurity voor IT-dienstverleners. Accessed on 22 March 2022, <https://www.accountant.nl/nieuws/2022/1/ing-belangrijker-rol-bij-cybersecurity-voor-it-dienstverleners>
- [5] Van der Woude, M. (2021, 18 August). Ict-beveiligers: ransomware gaat richting nationale crisis -. [Securitymanagement.nl](https://www.securitymanagement.nl/ict-beveiligers-ransomware-gaat-richting-nationale-crisis). Accessed on 23 March 2022. <https://www.securitymanagement.nl/ict-beveiligers-ransomware-gaat-richting-nationale-crisis>
- [6] ISACA. (2022). Ransomware Readiness Audit Program. https://store.isaca.org/s/store?utm_source=other&utm_medium=other&utm_campaign=blog_both_content_blogs_ransomware-audit-program_q123_ransomware-audit-program&utm_content=ransomware-audit-program_ransomware-audit-program&cid=blog_3002169&Appeal=blog#/store/browse/detail/a2S4w000005uz6vEAA
- [7] NCSC. (2021, 29 January). The rise of ransomware. [Ncsc.gov.uk](https://www.ncsc.gov.uk/blog-post/rise-of-ransomware). Accessed on 11 June 2022. <https://www.ncsc.gov.uk/blog-post/rise-of-ransomware>
- [8] Cyberveilig Nederland. (2021, August). Whitepaper Ransomware. https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf
- [9] CrowdStrike. (2022, February). The CrowdStrike 2022 Global Threat Report. <https://go.crowdstrike.com/global-threat-report-2022-thank-you.html>
- [10] Sharmeen, S., Ahmed, Y. A., Huda, S., Kocer, B. S., & Hassan, M. M. (2020). Avoiding Future Digital Extortion Through Robust Protection Against Ransomware Threats Using Deep Learning Based Adaptive Approaches. *IEEE Access*, 8, 24522–24534. <https://doi.org/10.1109/access.2020.2970466>
- [11] ENISA. (2021, October). ENISA Threat Landscape 2021. <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>
- [12] Sophos. (2022, April). Sophos-state-of-ransomware-2022. <https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxnhfhgj9bxbgj9/sophos-state-of-ransomware-2022-wp.pdf>
- [13] Thales. (2022, February). 2022 Thales Data Threat Report. https://cpl.thalesgroup.com/sites/default/files/content/research_reports_white_papers/field_document/2022-03/2022-data-threat-report-global-edition.pdf
- [14] Verizon. (2021, May). 2021 Data Breach Investigations Report. <https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf>
- [15] C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, 111, 102490. <https://doi.org/10.1016/j.cose.2021.102490>
- [16] Verizon. (2022, May). 2022 Data Breach Investigations Report. <https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf>
- [17] Moore, S. (2022, 3 April). Gartner Top Security and Risk Trends in 2022. Gartner. Accessed on 11 June 2022, <https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022>

- [18] La Verge, M. (2022, 25 February). Europese cyberwetten: dit gaan ze voor je bedrijf betekenen. KVK. Accessed on 28 June 2022, <https://www.kvk.nl/advies-en-informatie/veiligzakendoen/cybersecurity/europese-cyberwetten-dit-gaan-ze-voor-je-bedrijf-betekenen>
- [19] NCTV. (2022, July). Cybersecuritybeeld Nederland CSBN 2022. <https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022>
- [20] Steeman, P. (2021, 26 October). Gebukt onder cyberdreiging. Accountant.nl. Accessed on 25 March 2022, <https://www.accountant.nl/magazines/accountant-2021-nr.-5/gebukt-onder-cyberdreiging>
- [23] NCSC/Ministerie Justitie en Veiligheid. (2021, 16 December). “Om je te weren tegen ransomware moet je de keten snappen” - NCSC Magazine. NCSC. Accessed on 25 March 2022, <https://magazines.ncsc.nl/ncscmagazine/2021/02/om-je-te-weren-tegen-ransomware-moet-je-de-keten-snappen>
- [24] ISACA. (2021). To Pay or Not to Pay: Proven Steps for Ransomware Readiness. <https://www.isaca.org/resources/proven-steps-for-ransomware-readiness>
- [25] NCSC. (2021, June). Handreiking Cybersecuritymaatregelen. <https://www.ncsc.nl/onderwerpen/basismaatregelen/documenten/publicaties/2021/juni/28/handreiking-cybersecuritymaatregelen>
- [26] Opark, K. (2021, 11 November). Ransomware en de rol van een IT-Auditor. IT-auditor.nl. Accessed on 25 March 2022, <https://www.deitauditor.nl/business-en-it/ransomware-en-de-rol-van-een-it-auditor>
- [28] Borgerink, R. (2022, 29 November). Gehackt Hof van Twente eist in rechtbank 4 miljoen euro van systeembeheerder. RTV Oost. Accessed on 5 December 2022, <https://www.rtvoost.nl/nieuws/2167567/gehackt-hof-van-twente-eist-in-rechtbank-4-miljoen-euro-van-systeembeheerder>
- [29] Orange Cyberdefense. (2022). Security Navigator 2023. Accessed on 5 December 2022, <https://www.orange cyberdefense.com/global/security-navigator>
- [30] Orchilles, J. (2022, 24 March). Purple Teaming and Threat-Informed Detection Engineering. SANS Institute. Accessed on 4 August 2022, <https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team>
- [31] Hoogesteger, M. (2022, 17 June). Column - Omdenken met ransomware - PvIB. Platform voor InformatieBeveiliging (PvIB). Accessed on 29 June 2022, <https://www.pvib.nl/actueel/blogs/omdenken-met-ransomware>
- [32] Shacklett, M. E. (2021, 13 April). Attack Vector. SearchSecurity. Accessed on 3 August 2022, <https://www.techtarget.com/searchsecurity/definition/attack-vector>
- [33] Barker, W. C., Fisher, W., Scarfone, K., & Souppaya, M. (2022). Ransomware Risk Management: A Cybersecurity Framework Profile. NIST. <https://doi.org/10.6028/nist.ir.8374>
- [34] Kara, I., & Aydos, M. (2020). Cyber Fraud: Detection and Analysis of the Crypto-Ransomware. 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 0764–0769. <https://doi.org/10.1109/uemcon51285.2020.9298128>

- [35] Tailor, J. P., & Patel, A. D. (2017). A comprehensive survey: ransomware attacks prevention, monitoring and damage control. *A comprehensive survey: ransomware attacks prevention, monitoring and damage control*, 4(15), 116–121.
- [36] Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1), 10–21. <https://digitalcommons.kennesaw.edu/facpubs/4276>
- [37] NCSC. (2020, 9 July). Factsheet Ransomware. Factsheet | Nationaal Cyber Security Centrum. Accessed on 5 July 2022, <https://www.ncsc.nl/documenten/factsheets/2020/juni/30/factsheet-ransomware>
- [38] Kaspersky. (2016, June). KSN Report: Ransomware in 2014–2016. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190822/KSN_Report_Ransomware_2014-2016_final_ENG.pdf
- [39] Keijzer, N. (2020, June). The new generation of ransomware: an in depth study of Ransomware-as-a-Service (Masterthesis). University of Twente. <http://essay.utwente.nl/81595>
- [40] Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm. *Computers*, 8(4), 79. <https://doi.org/10.3390/computers8040079>
- [41] Kaspersky. (2021, 28 June). De opkomst van ransomware: de meest in het oog springende voorbeelden. www.kaspersky.nl. Accessed on 5 July 2022, <https://www.kaspersky.nl/resource-center/threats/ransomware-threats-an-in-depth-guide>
- [42] Harford, I. (2021, 8 October). 4 types of ransomware and a timeline of attack examples. SearchSecurity. 8 July 2022, <https://www.techtarget.com/searchsecurity/feature/4-types-of-ransomware-and-a-timeline-of-attack-examples>
- [43] Constantin, L. (2016, 28 March). This nasty ransomware overwrites your PC's master boot record. PCWorld. Accessed on 7 July 2022, <https://www.pcworld.com/article/420185/petya-ransomware-overwrites-mbrs-locking-users-out-of-their-computers.html>
- [44] Security.nl. (2016, 13 May). MBR-ransomware installeert tweede ransomware als back-up. Accessed on 7 July 2022, <https://www.security.nl/posting/470721#posting471004>
- [45] Chen, Q., & Bridges, R. A. (2017). Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware. 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA). <https://doi.org/10.1109/icmla.2017.0-119>
- [46] Harford, I. (2021, 8 October). The history and evolution of ransomware. SearchSecurity. Accessed on 8 July 2022, <https://www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware>
- [47] Kaspersky. (2021, 13 January). Wat is WannaCry-ransomware? Accessed on 8 July 2022, <https://www.kaspersky.nl/resource-center/threats/ransomware-wannacry>
- [48] Grustniy, L. (2021, 31 May). The ransomware saga. Kaspersky. Accessed on 8 July 2022, <https://www.kaspersky.com/blog/history-of-ransomware/39203>
- [49] Eenbergen, C. (2017, 28 June). Nieuwe ransomware Petya gaat WannaCry overtreffen. Techzine.nl. Accessed on 8 July 2022, <https://www.techzine.nl/nieuws/analytics/108883/nieuwe-ransomware-petya-gaat-wannacry-overtreffen>
- [50] Cimpanu, C. (2017, 29 June). Surprise! NotPetya Is a Cyber-Weapon. It's Not Ransomware. BleepingComputer. Accessed on 8 July 2022, <https://www.bleepingcomputer.com/news/security/surprise-notpetya-is-a-cyber-weapon-its-not-ransomware>
- [51] NCTV. (2018, June). Cybersecuritybeeld Nederland CSBN 2018. <https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2018/06/13/cybersecuritybeeld-nederland-2018>

- [52] Lalkens, P. (2018, 26 January). Maersk moest complete IT-systeem vernieuwen na cyberaanval. FD.nl. Accessed on 25 March 2022, <https://fd.nl/ondernemen/1239239/maersk-moest-complete-it-systeem-vernieuwen-na-cyberaanval-kyc2casOPrCc>
- [53] Lalkens, P. (2018, 2 September). Server in Ghana redde Maersk na beruchte cyberaanval. FD.nl. Accessed on 22 March 2022, <https://fd.nl/ondernemen/1267803/server-in-ghana-redde-maersk-na-beruchte-cyberaanval-kyc2casOPrCc>
- [54] ENISA. (2022, July). ENISA Threat Landscape for Ransomware Attacks. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks>
- [55] Grimes, R. (2022, 27 October). Ransomware 3.0: It Is About To Get Much Worse. Knowbe4. Accessed on 18 November 2022, <https://blog.knowbe4.com/ransomware-3.0-it-is-about-to-get-much-worse>
- [56] Attack Landscape Update H1 2021. (2021). F-Secure. Accessed on 19 November 2022, <https://blog-assets.f-secure.com/wp-content/uploads/2021/03/30120359/attack-landscape-update-h1-2021.pdf>
- [57] Baker, K. (2022, 14 February). Ransomware as a Service (RaaS) Explained | CrowdStrike. CrowdStrike.Com. Accessed on 11 July 2022, <https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas>
- [58] O’Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. IET Networks, 7(5), 321–327. <https://doi.org/10.1049/iet-net.2017.0207>
- [59] Keijzer, N. (2022, 2 March). Inside the world of ransomware part 2/3: Different roles within a ransomware attack. Northwave. Accessed on 25 March 2022, <https://northwave-security.com/inside-the-world-of-ransomware-part-2-3-different-roles-within-a-ransomware-attack>
- [60] FBI. (2021, March). FBI Internet Crime Report 2021. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
- [61] Zscaler. (2022, June). The 2022 ThreatLabz State of Ransomware Report. <https://www.zscaler.com/blogs/security-research/2022-threatlabz-state-ransomware-report>
- [62] Group-IB. (2022, May). Ransomware Uncovered 2021–2022. [https://www.group-ib.com/resources/threat-research/ransomware-2022.html?utm_medium=ppc&utm_source=adwords&utm_campaign=\[JI\]%20Brand%20-%20worldwide](https://www.group-ib.com/resources/threat-research/ransomware-2022.html?utm_medium=ppc&utm_source=adwords&utm_campaign=[JI]%20Brand%20-%20worldwide)
- [63] Palo Alto Networks (Unit 42). (2022, March). Ransomware Threat Report. <https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html>
- [64] Siegel, B. (2021, February 1). Ransomware Payments Decline in Q4 2020. Coveware: Ransomware Recovery First Responders. Accessed on 14 August 2022, <https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020>
- [65] Capgemini. (2022, June). Trends in Cyber Security 2022. <https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2022/05/Trends-in-Cybersecurity-2022-an-accelerated-digital-transformation.pdf>
- [66] NCSC. (2021, 17 November). NCSC Annual Review 2021. Ncsc.Gov.Uk. Accessed on 13 July 2022, <https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/ransomware-threat-methodology>
- [67] Toulas, B. (2022, 28 April). Ransom payment is roughly 15% of the total cost of ransomware attacks. BleepingComputer. Accessed on 13 July 2022, <https://www.bleepingcomputer.com/news/security/ransom-payment-is-roughly-15-percent-of-the-total-cost-of-ransomware-attacks>
- [68] Siegel, B. (2021, 26 April). Ransomware Attack Vectors shift as New Software Vulnerability Exploits Abound. Coveware: Ransomware Recovery First Responders. Accessed on 11 July 2022, <https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound#costs>

- [71] Siegel, B. (2021, 23 July). Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority. Coveware: Ransomware Recovery First Responders. Accessed on 11 July 2022, <https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority>
- [72] Siegel, B. (2021, 21 October). Ransomware attackers down shift to “Mid-Game” hunting in Q3. Coveware: Ransomware Recovery First Responders. Accessed on 11 July 2022, <https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts>
- [73] Siegel, B. (2022, 24 January). Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority. Coveware: Ransomware Recovery First Responders. Accessed on 11 July 2022, <https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority>
- [74] Siegel, B. (2022, 4 April). Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021. Coveware: Ransomware Recovery First Responders. Accessed on 11 July 2022, <https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021>
- [75] Siegel, B. (2022, 28 July). Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022. Coveware: Ransomware Recovery First Responders. Accessed on 1 August 2022, <https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022>
- [76] Siegel, B. (2022, October 26). Uber Verdict Raises New Risks for Ransom Payments. Coveware: Ransomware Recovery First Responders. <https://www.coveware.com/blog/2022/10/26/q3-2022-quarterly-report>
- [77] Esparza, J. M. (2020, 26 November). How to mitigate Ransomware attacks | Outpost 24 blog. Outpost24. Accessed on 2 August 2022, <https://outpost24.com/blog/How-to-mitigate-Ransomware-attacks>
- [78] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1(1), 80.
- [79] Lockheed Martin. (2015). Gaining the advantage: Applying Cyber Kill Chain® Methodology to Network Defense. Lockheed Martin. Accessed on 7 January 2023, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
- [80] Pols, P. (2017). The Unified Kill Chain. Accessed on 19 November 2022, <https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf>
- [81] Keijzer, N. (2021, 2 November). Inside the world of ransomware, Part 1/3: dissecting the attack. Northwave. Accessed on 25 March 2022, <https://northwave-security.com/en/inside-the-world-of-ransomware-dissecting-the-attack>
- [82] Augustinus, R. & van Bommel, S. (2021, 24 December). Ketenafhankelijkheden. IT-auditor.nl. <https://www.deitauditor.nl/business-en-it/ketenafhankelijkheden>
- [83] Hueck, H., & Van Gils, S. (2020, 14 December). Russische staatshackers vielen bedrijven binnen via update in software SolarWinds. FD.nl. Accessed on 22 March 2022, <https://fd.nl/economie-politiek/1367588/russische-staatshackers-vielen-bedrijven-binnen-via-update-in-software-solarwinds-kyc2casOPrCc>
- [84] Van Gils, S. (2021, 11 July). “Kaseya loste eerdere beveiligingsproblemen niet goed op”. FD.nl. Accessed on 14 May 2022, <https://fd.nl/futures/1394421/kaseya-loste-eerdere-beveiligingsproblemen-niet-goed-op-one2caCUE9IR>

- [85] Den Brinker, G., & Van Gils, S. (2021, 4 July). Honderden Nederlandse bedrijven geraakt door megahack. FD.nl. Accessed on 22 March 2022, <https://fd.nl/ondernemen/1390703/grote-russische-hack-treft-ook-nederlandse-bedrijven-lyc2casOPrCc>
- [86] ENISA. (2021, July). ENISA threat landscape for supply chain attacks. <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>
- [87] NCSC. (2021, May). ICT-supply chain risicomanagement. <https://www.ncsc.nl/onderzoek/onderzoekresultaten/grote-verschillen-in-benadering-risico%E2%80%99s-ict-supply-chains-bij-nederlandse-organisaties>
- [89] ThoughtLab. (2022, May). Cybersecurity Solutions for a Riskier World. https://thoughtlabgroup.com/wp-content/uploads/2022/05/Cybersecurity-Solutions-for-a-Riskier-World-eBook_FINAL-2-1.pdf
- [90] Boehm, J., Hall, F., Isenberg, R. & Michel, M. (2022, 3 March). Ransomware prevention: How organizations can fight back. McKinsey & Company. Accessed on 19 September 2022, <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/ransomware-prevention-how-organizations-can-fight-back>
- [91] Cyber Security Raad. (2021, April). Advies Rapport Integrale Aanpak Cyberweerbaarheid.
- [92] Ryerse, J. (2020, 9 oktober). The importance of a cybersecurity framework. 2020-10-01 | Security Magazine. Accessed on 18 September 2022, <https://www.securitymagazine.com/articles/93509-the-importance-of-a-cybersecurity-framework>
- [93] Houten, P., Spruit, M., & Wolters, K. (2019). Informatiebeveiliging onder controle (4th edition). Pearson Benelux B.V.
- [94] Praetorian. (2015, 2 March). NIST Cybersecurity Framework vs. NIST Special Publication 800–53. Accessed on 3 August 2022, <https://www.praetorian.com/blog/nist-cybersecurity-framework-vs-nist-special-publication-800-53>
- [95] Force, J. T. (2020). Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication (SP) 800–53 Rev. 5. <https://doi.org/10.6028/nist.sp.800-53r5>
- [96] NIST. (2018, April). Framework for Improving Critical Infrastructure Cybersecurity. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- [97] CIS. (2021, 24 July). About us – CIS®. Accessed on 12 August 2022. <https://www.cisecurity.org/about-us>
- [98] CIS. (2021, April). CIS Community Defense Model (Version 2.0). <https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0>
- [99] Jartelius, M. (2021, 21 May). What’s new and changed in CIS CSC version 8 – IG1 | Outpost 24 blog. Outpost24.Com. Accessed on 12 August 2022, <https://outpost24.com/blog/what-s-new-and-changed-in-CIS-CSC-version-8%E2%80%93IG1>
- [100] Maranon, A., Pell, S. (2021). Countering the Ransomware threat: A whole-of-Governmental Effort. <https://www.lawfareblog.com/countering-ransomware-threat-whole-government-effort>
- [101] Harford, I. (2022, 1 June). How ransomware kill chains help detect attacks. Security. <https://www.techtarget.com/searchsecurity/feature/How-ransomware-kill-chains-help-detect-attacks>
- [102] Kirvan, P. (2021, 21 December). Top 10 IT security frameworks and standards explained. Security. <https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one>
- [103] Pranggono, B., Arabo, A. COVID-19 pandemic cybersecurity issues. Internet Technology Letters 4(2). e247. <https://onlinelibrary.wiley.com/doi/full/10.1002/itl2.247>

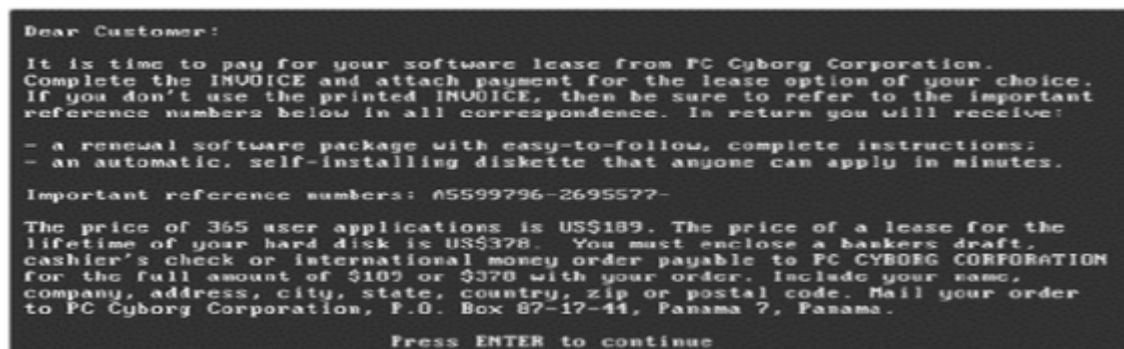
- [104] MITRE. (2022). Tactics - Enterprise | MITRE ATT&CK®. [attack.mitre.org](https://attack.mitre.org/tactics/enterprise). Accessed on 24 September 2022, <https://attack.mitre.org/tactics/enterprise>
- [105] Splunk. (2022). The Essential Guide to Ransomware. Accessed on 29 January 2023. https://www.splunk.com/content/dam/splunk2/en_us/gated/white-paper/splunk-essential-guide-to-ransomware-ss-106.pdf
- [106] IBM. (2021, July). Cyber Resilient Organization Study 2021. Accessed on 29 January 2023, <https://www.ibm.com/resources/guides/cyber-resilient-organization-study>
- [107] Nationaal Cyber Security Centrum. (2022, 14 October). Incidentresponsplan Ransomware. Publicatie | Nationaal Cyber Security Centrum. <https://www.ncsc.nl/documenten/publicaties/2022/juni/3/incidentresponsplan-ransomware>
- [108] CISA. (2020). Ransomware Guide. Accessed on 17 December 2022, https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf
- [109] CISA. (2022, September). Ransomware Guide. Accessed on 17 December 2022. <https://www.cisa.gov/stopransomware/ransomware-guide>
- [110] Siegel, B. (2023, 20 January). Improved Security and Backups Result in Record Low Number of Ransomware Payments. Coveware: Ransomware Recovery First Responders. Accessed on 29 January 2023. <https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments>
- [111] Boyd, D. (2021, 11 January). How to approach threat modeling. AWS Security Blog. Accessed on 30 January 2023. <https://aws.amazon.com/blogs/security/how-to-approach-threat-modeling>
- [112] Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing Cyber-Resilient Systems. NIST. <https://doi.org/10.6028/NIST.SP.800-160v2r1>

Appendix 1. ENISA attack model

		Actions			
		Lock	Encrypt	Delete	Steal
Assets					
Files		✗	✓	✓	✓
Memory		✗	✓	✓	✓
Folders		✗	✓	✓	✓
Database Content		✗	✓	✓	✓
MFT		✓	✓	✓	✗
MBR		✓	✓	✓	✗
Cloud		✗	✓	✓	✓
CMS		✗	✓	✓	✗
Screen		✓	✓	✓	✗

Appendix 2. A more detailed history of ransomware

The first ransomware attack was detected in 1989 [35]. The ransomware attack spread when a user inserted a floppy disk into the computer and a counter started running. After the computer had been booted up 90 times, all file names were encrypted and a message appeared stating that the user could reopen the files with a decryption key acquired by paying a fee of \$189 (Figure A2).



```
Dear Customer:
It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:
- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: 65599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue
```

Figure A2: PC Cyborg ransomware message [35].

By 2005, ransomware was being built more professionally. However, because no options to anonymously demand ransom existed, it remained limited to small attacks on individuals [36]. It was not until 2011 that ransomware became more professional due to the rise of cryptocurrency that allowed cybercriminals to start making more money. The two most common types of ransomware are locker and cryptor [37]. Kaspersky suggests that in 2015-2016, 40% of ransomware attacks employed encryption [38]. This implies that the remaining 60% were locker ransomware or other types. However, as Keijzer points out, there is no evidence in the literature validating these percentages or that year [39], nor is there for 2022.

Kok et al. [40] mentions a third type called scareware, whereby pop-up ads intend to manipulate users into buying software or making payments, for example, of a fine for an alleged law violation. This ransomware attack is therefore not immediately harmful to the user, but through its social-engineering tactic, still tries to get ransom. Locker and cryptor ransomware are the most common, so are discussed further in the study report.

Locker ransomware came first, with the earliest attacks observed around 2010-2011. This ransomware locks a computer's access screen so the user can no longer perform basic functions, including accessing the desktop and fully or partially disabling the mouse and the keyboard [38]. The first known locker ransomware attack was the variant WinLock in 2007-2012 [36]. It came via a malicious website and instructed victims to purchase a premium SMS code (costing around \$10) to then receive an unlock code [43]. Another well-known example is Petya in 2016 [15]. Petya rendered an entire hard drive inaccessible by overwriting the master boot record (hereafter MBR) [43]. The MBR contains the hard drive's library, through which the system finds files. As a result, the master file table (hereafter MFT) is encrypted and the operating system can no longer boot up [44].

Second came cryptor ransomware, which causes files to be encrypted using encryption algorithms. Unlike locker ransomware, cryptor encrypts critical data that the user can see – as basic functions still work – but the user cannot access. In a complex attack, besides encrypting data on a local IT system, all backups, hard drives, and data on the cloud can also be attacked [37]. For organizations lacking proper backups, the consequences can be disastrous because the data cannot be recovered. In 2015, there were more cryptor than locker ransomware attacks [41]. Around this period, the focus also shifted from attacking individuals to organizations. A well-known example is WannaCry in 2017 [15], the first major ransomware attack known to the public. It was activated in over 150 countries [45], and several large international organizations fell victim. WannaCry is a replicating cryptoworm that was able to spread in part because of the NSA's leaked attack tool EternalBlue [46], which exploited a zero-day vulnerability in the Windows operating system. Microsoft had released a critical security patch to address the vulnerability, but not all organizations had done the patching [47]. According to Kaspersky, WannaCry led to over \$4 billion in damage worldwide, including costs due to the WannaCry decryption key being defective [48].

Another well-known ransomware attack is NotPetya in 2017, barely two months after the WannaCry ransomware attack. According to researchers, NotPetya is an intermediate variant of Petya and WannaCry. Some of the malware code matches, but enhancements have also made the malware code more sophisticated [42]. As with Petya, NotPetya encrypts the MBR and the MFT to allow entrance using the same, albeit modified, vulnerability as WannaCry [48]. According to researchers, the goal was not ransom, but rather to disrupt multiple chains. Hence, the name NotPetya. The malware has no technical way – in the form of a kill switch [49] – to enable decryption even after payment. As such, NotPetya was characterized not as an official ransomware attack, but rather a wiper that ensures data becomes unrecoverable [50]. Since not all organizations had installed the Windows security patch after WannaCry, NotPetya caused destruction. Its total cost worldwide is estimated at €8 billion [48]. The ransomware attack originated from a Ukrainian software package, and organizations using it were affected because they did a software update but had not installed the accompanying security patch [51]. Among those affected was container company Maersk's location in the Port of Rotterdam, with costs estimated at €300 million [52]. Observers noted that Maersk was lucky: a brief power outage in Ghana spared a domain controller backup from infection, which allowed Maersk's IT system to become partially operational again within 10 days [53].

ENISA's LEDS model for classification

The 2022 European Network and Information Security Agency (hereafter ENISA) report no longer refers to locker or cryptor attacks because a ransomware attack has evolved into a multiple attack model. ENISA does not classify the type of ransomware attack, but rather the actions performed as per the LEDS model – an acronym for lock, encrypt, delete, and steal – and attacked assets [54]. An attacker can perform all of these actions during a ransomware attack instead of just using a locker. Per action, nine different assets can be attacked, such as documents or the MBR. Through this lens, ransomware attacks can be analyzed more specifically (Appendix 1). A ransomware attack also differs from a cybersecurity attack. A ransomware attack is more focused on disruption of business processes to obtain ransom, whereas a cybersecurity attack is focused on stealing intellectual property, credit card data, or business-sensitive data [33]. Ransomware can have a knock-on effect on entire business chains, potentially disrupting industries or society as a whole.

Appendix 3. Overview of cybersecurity frameworks

ISO 27001

ISO 27001 covers standards that describe requirements for how an organization can best set up an information security management system (hereafter ISMS). It comes from the ISO 27000 family that focuses on standards related to information security. Connected to ISO 27001 is ISO 27002, which provides a more in-depth look at how these cybersecurity controls can be implemented to meet the standards of ISO 27001. ISO 27001 addresses what an organization must implement based on risk assessments. It consists of 14 security categories and 114 controls, cybersecurity and otherwise. Each security category consists of an objective including the basic set of controls and activities [93]. Based on this set of standards, an information security baseline is created that applies to the entire organization. An advantage of the ISO 27001 is the certification mechanism, which allows an organization to an ISMS has been implemented. The latest version of ISO 27001 was published in 2022.

NIST-CSF

NIST has several publications in its Special Publication 800 series focused on governance and operations for implementing an information security framework within an organization. NIST 500-53 is its best-known publication and that from which NIST-CSF evolved. NIST-CSF focuses on protecting organizations' critical infrastructures; it contains a cybersecurity framework consisting of five steps: identify, protect, detect, respond, and recover. A total of 23 categories are broken down by step, including 108 cybersecurity controls [93]. The NIST frameworks are intended as a guideline for organizations to increase their cyber resilience, though unlike ISO 27001, they offer no certification capabilities. The latest version of NIST-CSF is v1.1 published in 2018 [96].

NIST-CSF Ransomware

In addition to the NIST-CSF, NIST released a new publication with a cybersecurity framework on ransomware based on NIST-CSF. The NIST-CSF Ransomware framework selected cybersecurity controls that help reduce the likelihood and impact of a ransomware attack. Its purpose is to help organizations identify and prioritize risks to improve their cyber defenses against ransomware attacks [33]. The framework includes 69 cybersecurity controls derived from the NIST-CSF. An addition to the framework is the overarching explanation of the relationship between a certain control and ransomware. The latest version of the NIST-CSF Ransomware is published in 2022, based on the NIST-CSF version of 2018.

CIS Controls

The nonprofit organization CIS aims to help organizations increase their cyber resilience. Its cybersecurity publication shares best practices for securing IT systems and data. In addition, CIS is known for its hardening baselines on configurations of IT systems [97]. CIS published a cybersecurity framework consisting of 153 cybersecurity controls divided into 18 categories and including NIST-CSF security functions. CIS also added implementation groups to indicate focus areas in three distinct phases for each cybersecurity control. The first implementation group (IG1) covers all basic cybersecurity controls that even small- to medium-sized organizations should implement. The second (IG2) covers larger organizations that are more operationally complex and have a higher risk of IT system failure. The third (IG3) concerns organizations that employ their own cybersecurity experts, as these organizations often perform important functions within society. The 153 cybersecurity controls are divided into these three implementation

groups, whereby the IG3 cybersecurity controls cover the whole CIS framework. CIS research on ransomware defense shows that this CIS Controls v8 provides protection against 10 out of 14 attack techniques of the MITRE ATT&CK framework, with the IG3 safeguards defending against 92% of attack techniques and IG1 safeguards alone defending against 78% [98]. The latest version of the CIS Controls is v8, published in 2021 [99].

Appendix 4. NOREA Ransomware framework attack steps

Kill chain phase **In**

Attack step	Attack step description	MITRE ATT&CK tactic reference
Abuse weak credentials	Gaining initial access by e.g. abusing remote desktop services within the network; based on stolen credentials, brute force attacks, or configuration errors	TA0006
Exploit vulnerabilities	Gaining initial access by using vulnerabilities in software or elsewhere	TA0001
Phishing	Gaining initial access by sending compressed files containing malware or a link in emails to obtain credentials	TA0001 TA0009 TA0042 TA0043

Kill chain phase **Through**

Attack step	Attack step description	MITRE ATT&CK tactic reference
Install persistency	Maintaining access to the network, often via what are referred to as “backdoors”	TA0003
Move laterally	Increasing access to other network parts	TA0002 TA0005 TA0007 TA0008 TA0011
Escalate privileges	Gaining higher privileges in the network	TA0004

Kill chain phase **Out**

Attack step	Attack step description	MITRE ATT&CK tactic reference
Exfiltrate data	Getting information, sensitive or otherwise, out of the system as leverage	TA0010
Destroy backups	Deleting backups as leverage	TA0040
Encrypt data	Providing encrypted assets as leverage	TA0040
Secondary attack & supply chain extortion	Exerting even more pressure on the organization by performing DDoS attacks or extorting third parties	NA