Threat Intelligence Report 2025

An In-Depth Analysis of
the Cyber Threat Landscape

TRUESEC

A message from Anna Averud, CEO of Truesec Group

This year's report highlights the most significant trends and insights you need to be aware of to navigate cyber risks effectively. Our goal is to share valuable information and data to help you understand the current threats and protect your business more efficiently. It's critical to stay ahead of these changes to prevent breaches. We aim to help you navigate a constantly evolving threat landscape.

As your trusted cyber partner, we are committed to working alongside your organization to safeguard your operations and help you navigate an increasingly complex threat landscape. We aim to provide you with the knowledge and tools to build robust and resilient organizations in an ever-uncertain world. We hope this report will serve as a solid foundation for your strategic decisions in the coming year by offering new perspectives and actionable insights.

I want to take this opportunity to thank my colleagues for their hard work in preparing this report and to express our appreciation for the time spent reviewing it.

Thank you for your continued partnership and trust in Truesec.

About Truesec:

Truesec is an international cybersecurity company that offers market-leading managed security services, incident response, and expert professional services. Truesec operates the largest Security Operations Center (SOC) in the Nordics. Our CSIRT have conducted more than 100,000 hours of incident response.

The company's goal is to prevent breach and minimize impact. Since 2005, Truesec has delivered advanced security solutions to clients in both the private and public sectors worldwide. Today, the company comprises over 330 cyber specialists with deep expertise and a leading role in cybersecurity in the Nordics.

For more information, visit Truesec.com

Content

TRUESEC

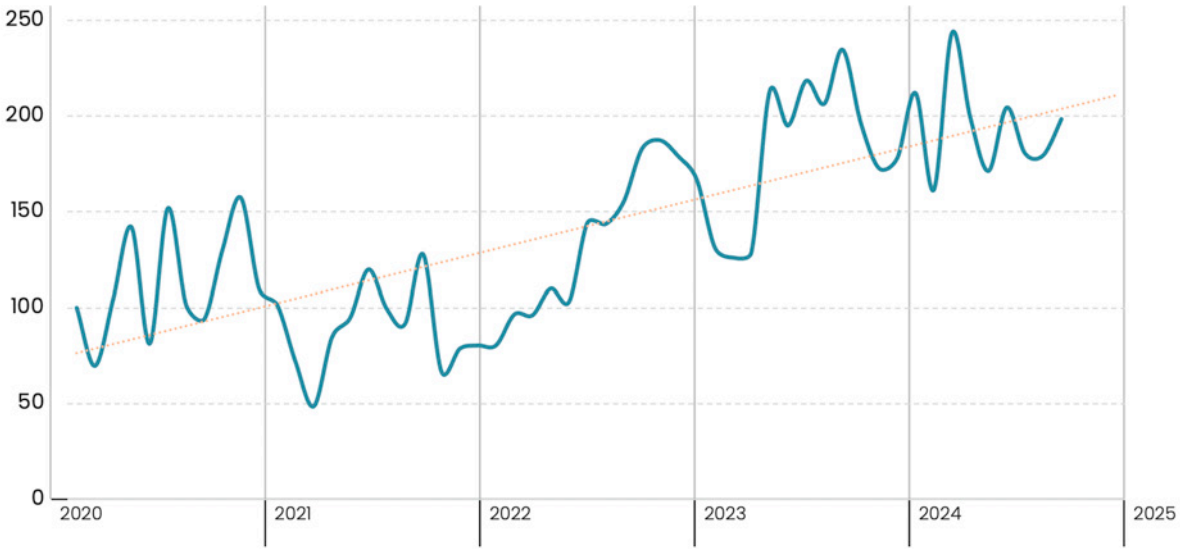
Developments in the Threat Landscape

Positive effects following cybersecurity investments

The year 2024 was a milestone for cybersecurity in the Nordics as we are starting to see the positive effects of large enterprises investing in increased cybersecurity. The threat of ransomware and other forms of cybercrime remains as dangerous as before, but our metrics now appear to show that organizations that do invest in meeting the challenge markedly will reduce the risks.

While this is a positive sign, it's important to observe that there are no indications that the threats are abating. Our SOC has disarmed a similar amount of intrusion attempts in 2024 as in the previous year. The increase in cyber intrusion attempts we have observed since the Russian invasion of Ukraine shows that geopolitical events continue to shape cybercrime too.

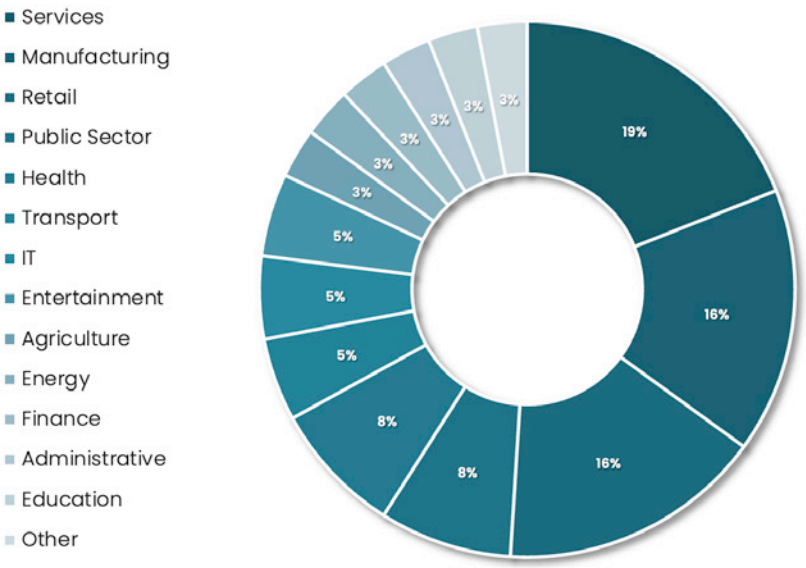
Trend of intrusion attempts disarmed in Truesec Security Operations Center



As many organizations improve their cybersecurity, cybercriminals become more opportunistic. Ransomware groups still have a good understanding of which industries are most likely to cave in to their demands, but they primarily attack where they manage to get a foothold. “Don’t be low-hanging fruit” is even more relevant today.

Truesec has also observed that opportunistic cybercriminals are shifting to ransomware attacks on smaller enterprises. The traditional business model, so-called big-game-hunting, was to target large organizations capable of paying large sums of ransom.

Truesec ransomware incident engagement per industry sector in 2024



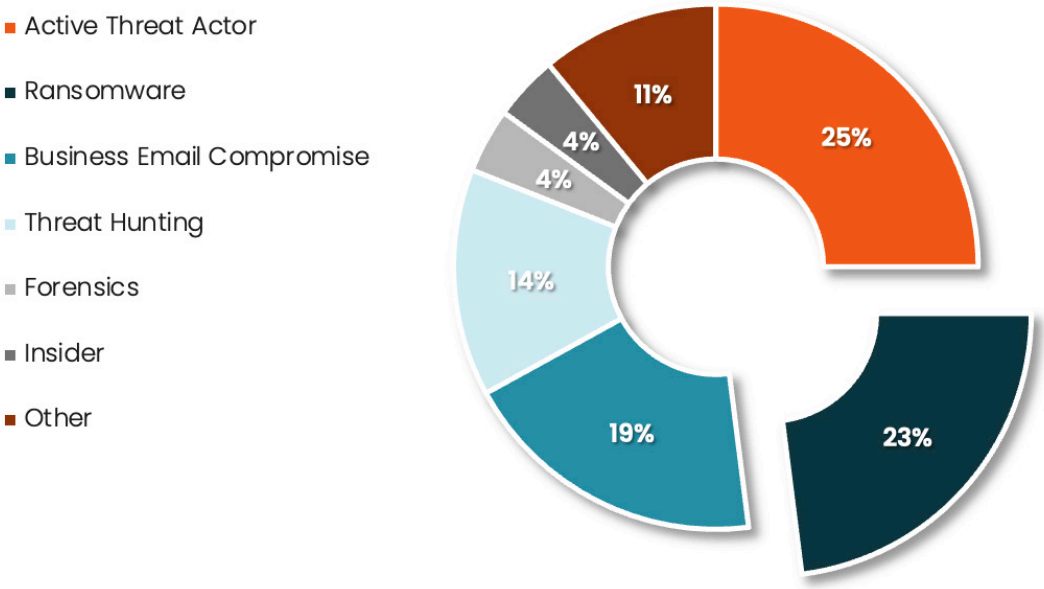
Attacks on small and medium-sized businesses (SMB) generate less revenue, but if they are less protected, the attack is swifter and likelier to succeed. It's also possible that there are more unreported ransomware attacks against smaller organizations that don't show up in our statistics.

While SMBs seldom have the same resources as the large corporations, they typically face a less complex threat landscape, since cybercriminals don't want to invest too much time and resources in an attack that will not generate a massive payoff. This year Truesec devotes a part of this report specifically for advice for how SMBs can improve their cyber-security based on the current threat landscape.

2024 also saw an ongoing campaign of international law enforcement striking at important infrastructure used for ransomware and other cybercrime. The two largest so-called ransomware-as-a-service groups, BlackCat and Lockbit, have both had their infrastructure hacked and capabilities degraded. Some ransomware affiliates now appear to forego the RaaS portals and act alone. The criminal ecosystem is resilient, however, and new ransomware-as-a-service groups have emerged in their place, like RansomHub and Cicada3301.

The geopolitical tensions in the world continue to influence the cyber threat landscape. Government directed cyber sabotage and hacktivism is used to amplify information operations to intimidate and influence the population of Western nations. Much of what passes as "hacktivism" is in fact government sponsored hybrid war.

Breakdown of types of Truesec cyber incident engagements in 2024



Another worrying trend that Truesec highlighted last year, is that as Western sanctions start to harm nations like Iran and North Korea, government controlled cyber actors are turning to cybercrime to finance their activities. North Korea's military intelligence has financed its operations with cybercrime for years, but this year more evidence appeared indicating that cyber espionage groups from Iran are now collaborating with Russian ransomware criminals. Whether adversaries use cybercrime to finance their activities or simply allow it to continue as a bargaining chip, cybercrime will continue to be linked to the geopolitical landscape.

Other forms of cybercrime still flourish. As predicted last year, some cybercriminals are now beginning to use AI to enhance their social engineering. Cybercriminals are using LLM and chatbots to generate texts for phishing mail. More sophisticated cybercriminals use deep-fake technology to mimic real people in online meetings to conduct fraud. Truesec has observed a rise in cyber enabled fraud, so-called business email compromise (BEC) where cybercriminals hack corporate mail accounts and use this access to send email with fraudulent payment information. Here we have also seen examples of Chinese cybercriminals now operating out of Africa.

As technical cyber defenses continue to improve, many threat actors will instead focus on social engineering and fraud to gain access to networks. IT personnel and software developers are becoming the focus of many such attacks, since they typically have accounts with much higher privilege than regular users.

Open source code sharing sites like Github are constantly filled with fake projects and forked code bundles that include malware. Even fake job interviews can be used to lure software developers to download malware, allowing criminals to take over the corporate network they are on. Securing your organization's software supply chain is a vital part of cybersecurity.

Our data indicates that large Nordic enterprises appear to have learned their lesson, and investing in cybersecurity has allowed them to break the trend of increasing ransomware attacks - this is a positive trend but hardly a cause for relaxation. As threats continue to evolve, it's important to stay up to date with the latest threats and prepare to meet them.

Breaching the Network

Initial attack vectors: Ransomware and Extortion

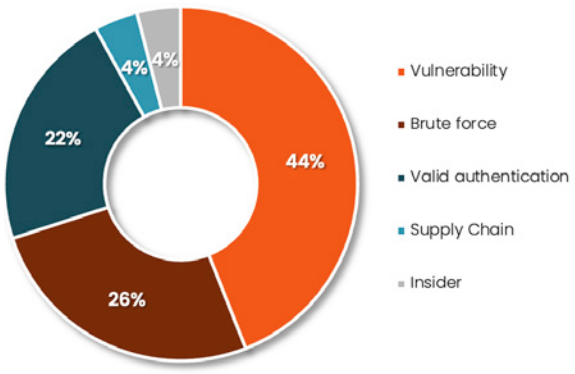
Ransomware incidents usually begin with one of two initial attack vectors that are also to some extent tied to different business models used by the cybercriminals. More than 40% of all ransomware incidents begin with cybercriminals exploiting vulnerabilities in external facing security applications, such as VPN solutions and firewalls, that allow remote code execution.

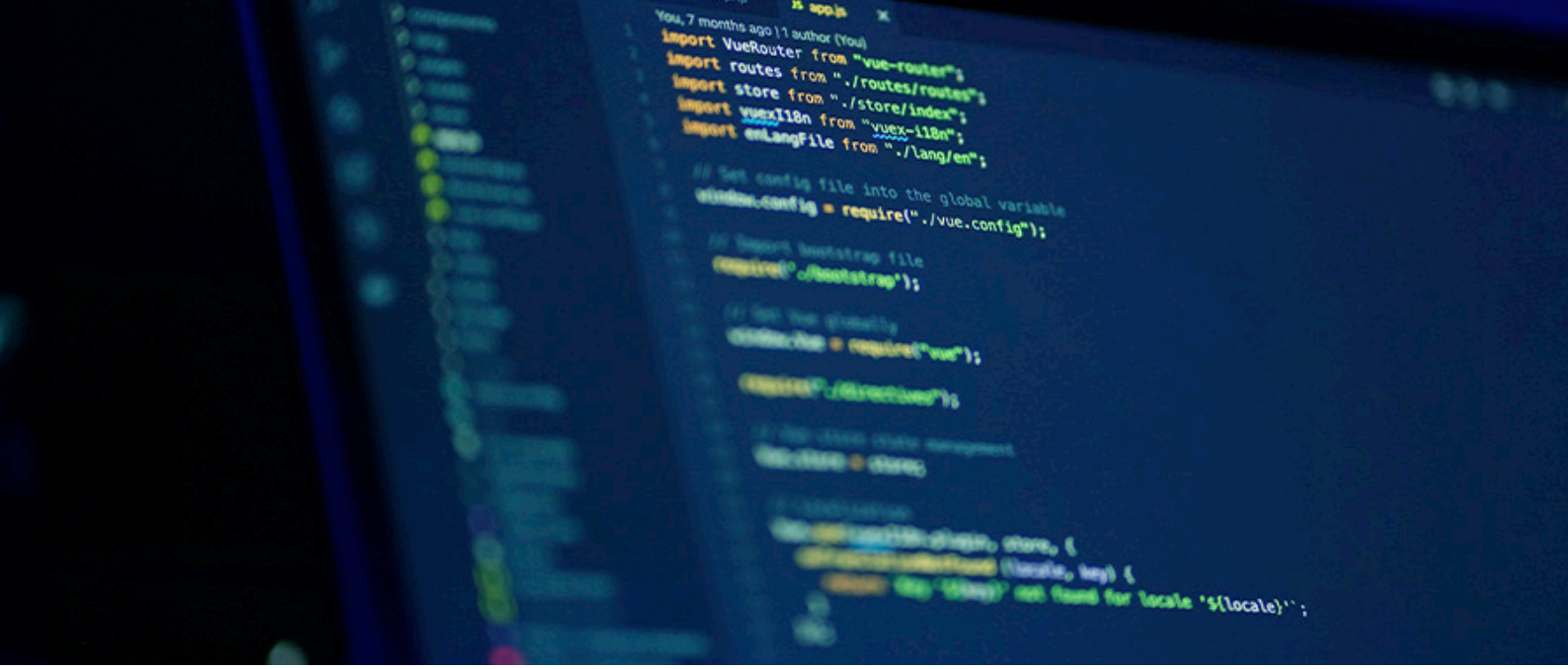
Most of the other ransomware incidents begin with some form of identity-based attack. Identity-based attacks range from using stolen credentials obtained by information-stealing malware to simple brute force password-guessing. They all involve obtaining credentials and then just logging in to the victim's account.

Information stealing malware can be installed on victim machines using a range of different methods, including phishing mail, compromised web sites, and infected code packages on code sharing sites.

While supply chain attacks are a legitimate worry, especially for larger organizations, they still constitute a minority of all ransomware attacks. Over 90% of the ransomware incidents that Truesec handled in 2024 could have been avoided by blocking incoming password guessing, strictly enforcing multi-factor authentication (MFA) and active vulnerability management.

Initial Attack Vector in successful ransomware attacks





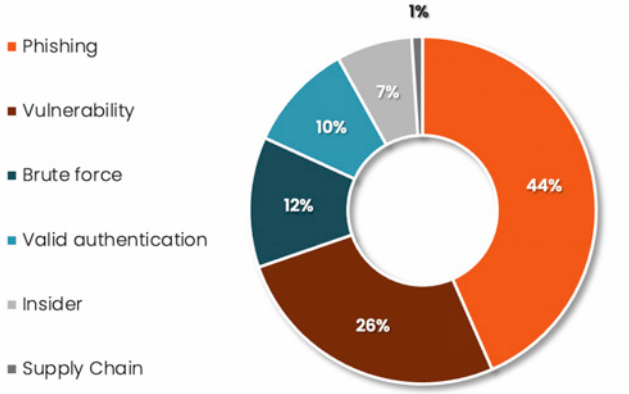
Business Email Compromise

Business Email Compromise (BEC) and other forms of cyber fraud are aimed at email accounts and almost always begin with a phishing email. The phishing email contains a link to a fake login page that steals credentials, session cookies or other tokens, that allows the criminals to take over a mail account and exploit it.

It is worth noting that while BEC criminals generally are less skilled hackers than ransomware criminals, it is seldom that ransomware criminals use token stealing phishing mail to gain access to networks.

The reason is not known but may include a business model where access is often obtained by a so-called initial access broker (IAB) that sells access to ransomware criminals, which can mean that ransomware criminals will not use the access until days or weeks after the initial breach. Stolen session cookies have a short duration, and BEC criminals usually exploit a successful phishing within hours of a victim having fallen for the phishing mail. An information stealing trojan can provide updated account information as long as it remains undetected.

Initial Attack Vectors across all Truesec incident engagements



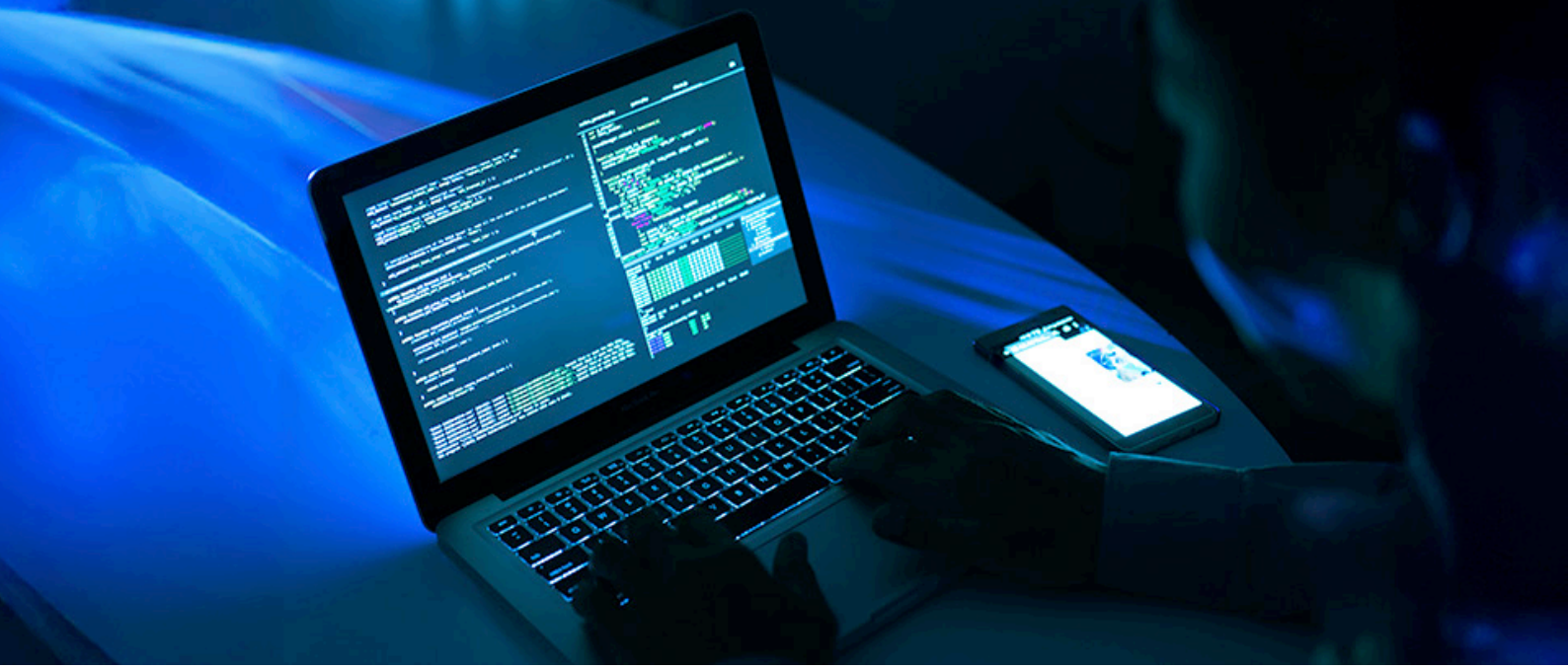
The Future of Cyber Extortion

Whenever an organization is dependent on an IT system for availability or confidentiality, this can be exploited by cybercriminals for extortion and should consequently be adequately protected.

Historically, cyber-enabled extortion has had many faces: ever since ransomware became a billion-dollar criminal industry, cyber extortion has become the top worry for most organizations. Most industries today rely on IT systems for their day-to-day operations, and if criminals deny them the use of their IT environment, production can grind to a halt, with immediate loss of revenue for every hour during the ongoing incident.

Cyber extortion is more than just ransomware, however. Sometimes even threats of a crude distributed denial-of-service (DDoS) attack that can disrupt web applications that online business relies on, such as customer portals, can be used for extortion.

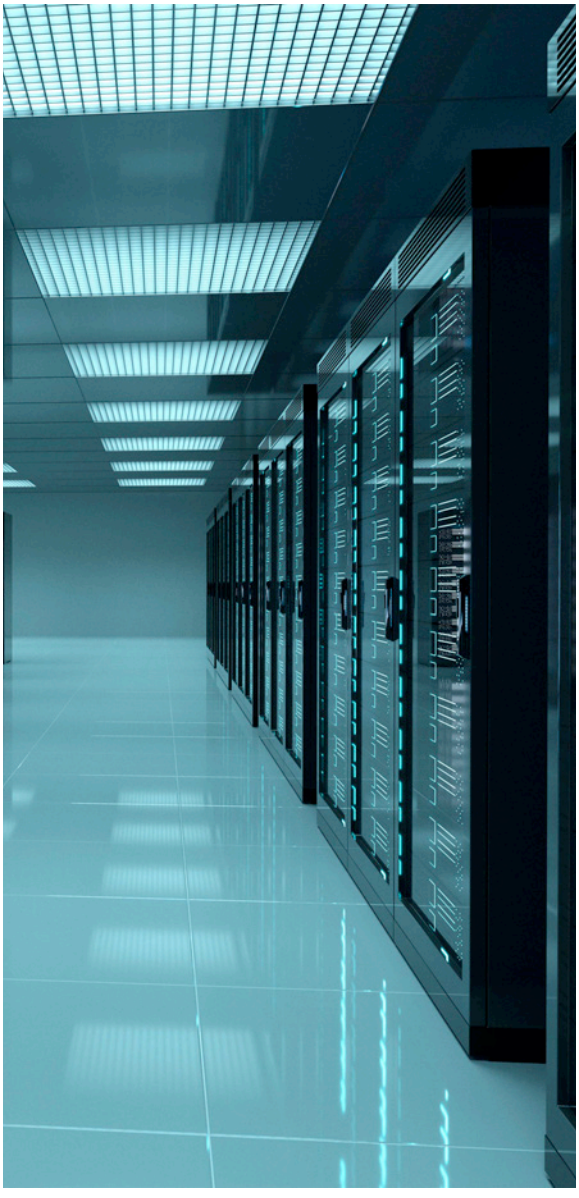
Another common form of cyber extortion is to steal confidential data and threaten to release it to the public, something which can potentially lead to loss of customer confidence, lawsuits or exposure to being in breach of data privacy legislation.



Many cybercriminals have a keen understanding of which type of victims are most vulnerable to various forms of cyber extortion. Organizations that depend on customer confidence in handling sensitive personal information, such as legal firms or private health-care institutions, are prime targets for data leak extortion, while organizations depending on customer confidence in stable access to online services, such as online shopping and financial institutions, can be targeted with DDoS extortion.

While cybercriminals are often opportunistic, it's very important to understand that ALL organizations with an online presence can be subject to intrusion attempts with the purpose of a limited or full-scale cyber extortion.

The cybercriminal ecosystem is ever changing and in active development and while ransomware is still trending, the future battle between defenders and attackers is very likely to include an extortion component.



Protect Your Data

When organizations turn digital, their knowledge is their competitive edge. This also turns their intellectual property into the most desirable target for threat actors, which means that such information has to be protected from possible theft.

Innovation and knowledge are keys to success for most modern businesses. For many corporations today, a significant portion of their value lies in unique knowledge and intellectual property that is stored digitally. Stealing this data can provide competitors with information that allows them to copy their production methods without having to invest in the research and development, allowing them to undercut prices.

Cyber espionage, trying to gain an advantage by obtaining confidential information, has been a part of the digital world for a long time. Initially such data theft was mostly the domain of state intelligence agencies that spy on national secrets, but today it is also conducted to support business.

Data theft can also allow a company to game their competitors' bids and win tenders or to gain privileged information that can be used in litigation battles. In principle, all exclusive knowledge that can be monetized and is stored digitally can become the target of data theft.

In addition to the large national spy agencies, there is now a growing industry of private contractors that offer to conduct cyberattacks and steal confidential corporate information that can be leveraged by competitors. Many such private cyber espionage actors also have deals with their governments that allow them to operate with relative freedom, even if they are exposed.

This means that organizations don't need to possess the capacity to conduct data theft themselves to hack their competitors, they can just rent it. As the rules-based international order is now under strain, such data theft is expected to continue to grow in the future.

Modern Forms of Cyber Sabotage

With almost all modern government and business being reliant on IT technology today, they can be disrupted by targeting their digital support through cyberattacks. Destructive cyberattacks and other acts of cyber sabotage are a form of violence. The aim is to disrupt, harm or intimidate a perceived opponent, at least in the eyes of the actor's supporters.

Cyber sabotage is almost always political in nature. Even when some hacktivists conduct cyber sabotage as a form of performance to solicit money from their online fans, they are relying on their audience's political preferences to get their support.

The ultimate form of violence is war, and the worst form of destructive cyberattacks is usually associated with cyber warfare units. Destructive cyber warfare attacks aim to degrade or destroy IT systems that support the adversaries' war effort, either by directly affecting their ability to wage war, or indirectly by hurting civilian morale.

However, cyber warfare is just the most extreme form of cyber sabotage. Other forms of cyber sabotage include sabotage such as "hacktivism" that is more akin to digital terrorism, than outright acts of war. Even simple forms of cyber sabotage, such as distributed denial-of-service attacks and web defacement, are technically a form of cyber terrorism as its primary aim is to frighten and intimidate adversaries, while projecting an image of strength to your own side.

Acts of cyber sabotage are now an integral part of modern conflicts. As governments in Europe are repeatedly warning that the threat of conventional war in Europe is rising, this means that conflicts in the cyber domain will also likely continue to increase, resulting in more cyber sabotage.

Combating Cybercrime Together

Global joint operations

In 2024, Interpol, Europol, FBI, and private sector organizations have made significant strides in combating cybercrime. These efforts reflect a coordinated global response to the evolving threat of cybercrime, aiming to protect individuals and businesses worldwide. The operations of law enforcement during 2024 focused mainly on attacking the infrastructure of the cybercriminal ecosystem, rather than going after specific threat actors. The operations had a real impact on the cybercriminal ecosystem, leading to several changes in the threat actors' modus operandi and abilities to collaborate.

Europol's Internet Organized Crime Threat Assessment (IOCTA) of 2024 highlighted several significant joint operations aimed at combating cybercrime.

Operation Cronos

In this joint venture with law enforcement agencies from 10 different countries, Europol disrupted the operations of the LockBit group. 34 servers were taken down and more than 200 cryptocurrency accounts were frozen. Two LockBit actors were arrested in Poland and Ukraine. From the data analyzed in the takedown, several decryption tools were made public on the No More Ransom portal.

Operation Dark Hunt

This operation targeted dark web marketplaces involved in the sale of illegal goods and services. It led to the arrest of multiple suspects across Europe and the seizure of significant amounts of cryptocurrency.

Operation Nova

Focused on dismantling the operations of groups using LockerGoga, MegaCortex, HIVE and the Dharma ransomware. This operation resulted in the arrest of several high-profile ransomware operators and the seizure of their infrastructure.

Operation Synergia II

Conducted by Interpol from April to August 2024, this operation achieved significant results in the fight against cybercrime. Over 22,000 malicious IP addresses and servers linked to phishing, ransomware, and information stealers were dismantled. The operation led to the arrest of 41 individuals, with 65 others still under investigation. Authorities seized 59 servers and 43 electronic devices, including laptops, mobile phones, and hard disks. The operation involved law enforcement agencies from 95 member countries, highlighting the importance of international cooperation. These efforts have significantly disrupted cybercriminal activities and prevented potential harm to countless individuals and businesses worldwide.

One notable arrest during Operation Synergia II involved a cybercriminal in Estonia. This individual was linked to a network responsible for distributing phishing emails and deploying information stealers. During the operation, Estonian authorities seized over 80GB of server data, which included sensitive information used in various cyberattacks. This arrest highlights the importance of international cooperation in tracking and apprehending cybercriminals, as well as the effectiveness of coordinated efforts in disrupting malicious activities.

Operation Endgame

The FBI, in collaboration with international law enforcement agencies, conducted this operation that had a significant impact on global cybercrime rates in 2024. It dismantled the infrastructure of several major malware groups, including IcedID, Smokeloader, Pikabot, and Bumblebee. This disruption significantly reduced the operational capabilities of these groups. Following the operation, there was a noticeable decline in the number of cyberattacks, particularly those involving ransomware and information stealers. Authorities seized significant amounts of illegal proceeds, which disrupted the financial operations of cybercriminal networks. This included freezing assets and confiscating cryptocurrency used in criminal transactions.

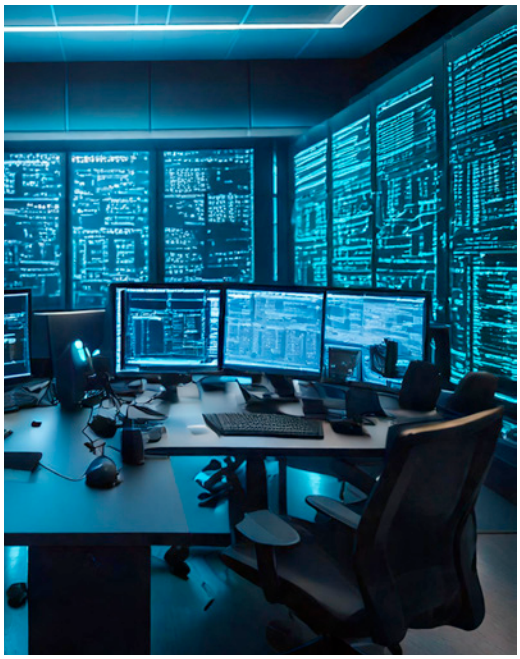
The Nordic countries have also conducted several successful joint operations to combat cybercrime in the region.

Operation Nordic Shield

This operation targeted a sophisticated phishing network that had been defrauding individuals and businesses across the Nordic region. The coordinated effort led to the arrest of 15 suspects and the seizure of numerous electronic devices used in the scams.

Operation Arctic Fox

Focused on dismantling a ransomware group that had been targeting critical infrastructure, this operation involved law enforcement agencies from Denmark, Finland, Norway, and Sweden. It resulted in the arrest of key members of the group and the disruption of their operations.



The Swedish Cybercrime Center (SC3), together with the regional centers, within the Swedish Police Authority, has throughout the year of 2024 participated in several international operations. Swedish Police played a significant role in Operation Cronos, disrupting the world's largest ransomware operation Lockbit, as well as the DDoS operation performed by Anonymous Sudan, resulting in both arrests and the seize of criminal infrastructure and financial resources.

Sweden continues to have a liaison officer within Europol's Joint Cybercrime Action Taskforce J-CAT, making international cooperation easy and efficient. International cooperation is increasing with the realization that no country can fight international cybercrime on their own.

On a national level, the admin, and several moderators, of the largest Swedish darkweb drugsite has been prosecuted and sentenced to imprisonment for many years. Swedish police have supported Finnish police in taking down a similar darkweb drugsite in Finland with digital infrastructure in Sweden.

Swedish police continue to increase the ability to intervene in the digital arena, to secure evidence and increase cooperation with private actors in the cyber security sector.

A crucial part of law enforcement and the ability to prosecute cyber criminals is the will of the victims of cybercrime to report the incidents to the police. Every bit of data is a step towards an international operation, seizure of criminal infrastructure and imprisonment of perpetrators.

Steffen Oxenvad
Investigation leader SC3
The Swedish Police Authority

Dissecting the Cicada

The Cicada3301 appears to be a traditional ransomware-as-a-service group that offers a platform for double extortion, with both a ransomware and a data leak site, to its affiliates. The first published leak on the group's data leak site is dated June 25, 2024. Four days later, on June 29, the group published an invitation to potential affiliates to join their ransomware-as-a-service platform on the cybercrime forum Ramp.

The Cicada3301 group uses ransomware written in Rust for both Windows and Linux/ESXi hosts. The focus here will be on the ESXi ransomware, but there are artifacts in the code that suggest that the Windows ransomware is the same ransomware, just with a different compilation.

While more and more ransomware groups are adding ESXi ransomware to their arsenal, only a few groups are known to have used ESXi ransomware written in Rust. One of them is the now defunct Black Cat/ALPHV ransomware-as-a-service group. Analysis of the code has also shown several similarities in the code with the ALPHV ransomware.

The Cicada3301 ransomware has several interesting similarities to the ALPHV ransomware.

- Both are written in Rust
- Both use ChaCha20 for encryption
- Both use almost identical commands to shutdown VM and remove snapshots
- Both use –ui command parameters to provide a graphic output on encryption
- Both use the same convention for naming files, but changing "RECOVER-"ransomware extension"-FILES.txt" to "RECOVER-"ransomware extension"-DATA.txt"
- How the key parameter is used to decrypt the ransomware note

Below is an example of code from Cicada3301 that's almost identical to ALPHV

```
                    try { // try from 001leac4 to 001leae1 has its CatchHandler @ 001lf8c1
                    LAB_001leac4                                                    XREF[1]:     00211524(*)
001leac4    LEA     RCX, [s_|_--no_vm_ssnohup_esxcli_--forma_001f4880+261]  ; = "|  --no_vm_ssnohup esxcli --formatter=csv
                                                                            ; --format-param=fields==\"WorldID,DisplayName\" vm process list | grep -viE
                                                                            ; \",(),\" | awk -F \"\\\"*,\\\"*\" '{system(\"esxcli vm process kill
                                                                            ; --type=force --world-id=\"$1)}' > /dev/null 2>&1; for i in `vim-cmd
                                                                            ; vmsvc/getallvms| awk '{print$1}'`;do vim-cmd vmsvc/snapshot.removeall $i &
                                                                            ; done > /dev/null 2>&1; --uiesxcli --formatter=csv…
```

Analysis of the Threat Actor

The initial attack vector was the threat actor using valid credentials, likely brute-forced against a NetSupport Manager appliance. The IP address 91.92.249.203, used by the threat actor, has been tied to a botnet known as "Brutus" that, in turn, has been linked to a broad campaign of password guessing various VPN solutions. This botnet has been active since at least March 2024, when the first article about it was published, but possibly longer. This indicates that likely the operators behind the Brutus botnet have at least a transactional relationship with the ransomware group behind Cicada3301.

The group could also have teamed up with the malware developer behind ALPHV. This individual appears to have worked for several different ransomware groups in the past. Regardless of whether Cicada3301 is a rebrand of ALPHV, or they have a ransomware written by the same developer as ALPHV, or if they have simply copied parts of ALPHV to make their own ransomware, the timeline suggests that the demise of BlackCat and the emergence of first the Brutus botnet and then the Cicada3301 ransomware operation may possibly be all connected. More investigation is needed before we can say anything for certain, however.

Technical Details

At the start of the ransomware main function, there are several references to parameters that should be passed as an argument to binary, using clap::args, that hold different functionalities that can be used in combination as well.

The binary has a built-in help function with explanations of the different parameters and how they should be used.

The ransomware parameters

Below are parameters discovered in the ransomware binary:

ui prints the result of the encryption to the screen, showing which files have been encrypted.

no_vm_ss encrypts files without shutting down the virtual machines that are running on ESXi. Also deletes snapshots.

key inputs the decryption key. It must be provided, otherwise the binary will fail and show "Key is invalid" on the screen.

check_key_and_get_rec_text checks length of the key. If the length is less than 0x2c the binary will terminate directly.

File encryption

The first function is to extract another public PGP key, stored in the data section. This key is used to encrypt the symmetric key that is generated for file encryption.

It then creates the file that will store the ransomware message in the folder of the encrypted files. It will be named "RECOVER-'ending of encrypted file'-DATA.txt"

Then it checks the size of the file. If it is greater than 0x6400000 it will encrypt the file in parts, and if it is smaller, the whole file will be encrypted.

The files will then be encrypted with a symmetric key generated by OsRng using ChaCha20. After the encryption is done it encrypts the ChaCha20 key with the provided RSA key and finally writes the extension to the encrypted file. The file extension is also added to the end of the encrypted file together with the RSA encrypted ChaCha20 key.

Inside the encryption function there is also a list of file extensions where most of them are related to either documents or pictures. This indicates that the ransomware has been used to encrypt Windows systems before being ported to ransomware ESXi hosts.

Scan to read the full analysis on our blog:

A Major Concern for Small and Medium Businesses

Cyber criminals targeting organizations with smaller cybersecurity investments

In the Nordic region, small and medium-sized businesses (SMBs) make up a significant portion of the business landscape. Approximately 99% of all companies in the Nordics are considered SMBs. This high percentage underscores the vital role that SMBs play in the economy, contributing to innovation, employment, and economic growth.

SMBs in Sweden contribute significantly to the economy. They generate approximately 51.4% of the value added to the Swedish GDP. This further highlights the crucial role SMBs play in driving economic growth and employment in the country.

In the contemporary digital landscape, cybersecurity has become a paramount concern for organizations of all sizes. However, SMBs often find themselves at a significant disadvantage. Cyber criminals strategically prioritize attacking organizations that have smaller investments in cybersecurity, leading to them becoming an easier target for the criminals. Understanding why this is the case, and the potential consequences, is crucial for these businesses to protect themselves effectively.

The Danger of Smaller Investments in Cybersecurity

Many small business owners mistakenly believe they are too small to be targeted, leading to complacency in implementing necessary security measures. Despite their size, small businesses often hold valuable data, such as customer information and payment details, which can be lucrative for attackers. The fact that many SMBs are also part of the supply chain of larger organizations may lead to them becoming collateral damage in the hunt for larger prey. Small and medium busineses typically operate with limited financial resources, which often translates to smaller budgets allocated for cybersecurity. This limitation can manifest in various forms, such as outdated software, inadequate security technologies, lack of regular security audits, and insufficient employee training programs. Cyber criminals are acutely aware of these vulnerabilities and exploit them with precision.

The inadequate investment in IT and cybersecurity makes SMBs vulnerable for several reasons:

Lack of Advanced Cybersecurity Solutions: Smaller investments often result in basic or inefficient security measures, making it easier for cybercriminals to breach systems undetected.

Limited IT Staff: SMBs may not have dedicated IT security personnel, leading to slower response times and less effective incident management.

Unpatched Systems: Regular updates and patches are essential for security, but these may be neglected due to resource constraints, leaving systems vulnerable. Vulnerable IT systems is the most common intrusion attack vector represented in our ransomware incident response engagements.

Inadequate Employee Training: Without sufficient training, employees might fall prey to phishing schemes and other social engineering tactics.

Consequences of Cyberattacks on SMBs

The repercussions of a cyberattack on a small or medium-sized business can be devastating and far-reaching. The immediate financial impact can be crippling. Costs associated with data recovery, legal fees, fines, and compensation to affected customers can quickly escalate. For many SMBs, these expenses can threaten their very existence.

Trust is a critical asset for any business. A breach can severely damage a company's reputation, leading to loss of customers and revenue. Rebuilding trust and a positive brand image can take years and substantial effort.

Business operations often get disrupted, leading to downtime and loss of productivity. This disruption not only affects the company's immediate ability to generate revenue but also its long-term operational efficiency.

Even small businesses are subject to regulations that require them to protect customer data. Failure to do so can result in hefty fines and legal actions. Additionally, compliance with legal requirements can become more stringent post-attack, adding to the company's burden.

Mitigating the Risks

Investing in cybersecurity is crucial to protect against potential threats and ensure business continuity. For small businesses, it's generally recommended to allocate 4% of their total revenue to IT. Within this IT budget, 5-20% should be dedicated specifically to cybersecurity. This range can vary based on factors such as the industry, the sensitivity of the data handled, and the specific risks faced by the business. Not making these investments can have severe consequences, all of which come at a higher cost than the suggested investment.

First and foremost, if you don't have the resources to build your own capabilities, consider outsourcing. This is just as valid for cybersecurity as for IT Operations. It's hard, if not impossible, to scale these kinds of specialties in-house for a small organization.

Secondly, ensure that all IT operations follow best practices with a strong emphasis on keeping everything up to date and current, both when it comes to software as well as hardware. Unmanaged, Unknown or Forgotten systems, applications or devices, is still the number one attack vector leading to breaches.

Having strong authentication implemented on ALL systems and solutions, whether they are Internet facing or not, greatly reduces the risk of a breach. Implement authentication mechanisms that are as user-friendly as they are secure, such as Yubico's Yubikeys.

Implement and verify secure backup solutions, where the backup is not reachable from the environment it protects. Ensure that you regularly have full verification tests on the backups into a production-like environment. This will be the last line of defense if an opportunistic threat actor attacks and encrypts the environment.

Since no defense is an absolute safeguard, consider acquiring cyber insurance. The insurance will help with the non-technical consequences of a breach, such as costs of business interruption and 3rd party coverage such as legal costs and liabilities. To make sure that you acquire the right insurance for your organization, always consult with an insurance broker specializing in cyber insurance.

The cyber insurance industry has recently recovered from a few very hard and unprofitable years. Following a large uptake for larger organizations, the insurance industry has now made insurance a real alternative also for smaller organizations. A few years ago, SMBs only cyber insurance option were insurance policies that were very limited in scope and/or insurance limit. In many cases, these policies gave a false sense of security and many organizations found out the hard way that they didn't have the insurance cover they expected. These policies are still out there, especially available from national insurers, but there are now better options available.

Luckily, the process for buying cyber insurance has evolved drastically. From 20+ page applications that were difficult if not impossible to answer in full, SMBs can now buy insurance based only of readings from external scans. This change in process has had a very positive impact on the pricing, with rates dropped about 30% in the last 12 months.

In order to qualify for cyber insurance, there are some technical requirements that each company must implement. These are typically not too difficult to overcome, and they all give meaningful protection. Caveat emptor – some insurance companies still have conditions that can jeopardize cover in case there is an incident.

While the exact requirements vary, some are consistent across most insurers:

1. **MFA must be applied** for all remote access. This requirement is typically not too difficult to live up to, but check the fine print. Also, don't forget to disable access on user name and password only. MFA isn't very useful if it's not required.

2. **Backups** – insurers are increasingly demanding that their clients have backups off site. Typically restoration tests aren't required, but can be. As the saying goes – back ups are nothing, restoration is everything.

3. **Monitoring** – moving away from accepting Anti Virus as a sufficient security mechanism, insurers are rapidly starting to require EDR to be in place. EDR is good and well, but means very little if there's no one to manage the alerts. Make sure that you have someone to monitor your network 24/7, because statistics indicate that the majority of incidents that become insurance claims are initiated on Fridays.

There are additional requirements that various insurers can ask for, such as segmentation between IT and OT, email security requirements, phishing trainings etc. Most requirements are manageable, but always check the requirements before signing up for a policy.

In summary, cyber insurance has become a credible alternative also for SMBs, you just need to ensure that the policy you buy works for your business.

Kristoffer Haleen
Deputy CEO and Head of Cyber
Northern Europe, Howden Sweden

When the Threat goes Silent

How attack trends are shifting in the enterprise environment

In 2024, we noticed a shift in the attacks against enterprise organizations. From having been targeted with disruptive attacks, just like the ones now primarily affecting SMBs, the attackers went silent. Silent but not gone. In general, it revolves around the purpose and goal of the threat actors - where it used to be extortion through the use of ransomware, it now became data theft, espionage or creating a link in a supply chain.

What led to this change? Well, all over the world, investments in cybersecurity solutions for enterprises continue to grow, making the smash and grab attacks become more time consuming and difficult. Also, threat actors are finding it more challenging getting paid by organizations that they have crippled by ransomware. Data has shown that an organization is more willing to pay a threat actor that just stole data without disrupting the business with an encryption attack.

What will this entail for enterprises? The major concern is that most of the cybersecurity solutions that are either in place or under implementation, are built to detect and respond against malicious behaviors. Advanced attackers that don't disrupt the business operations or perform malicious activities will simply go undetected. Additionally, it's always more difficult to allocate budget to counter a threat that's not perceived as imminent.

So, what should Enterprises do?

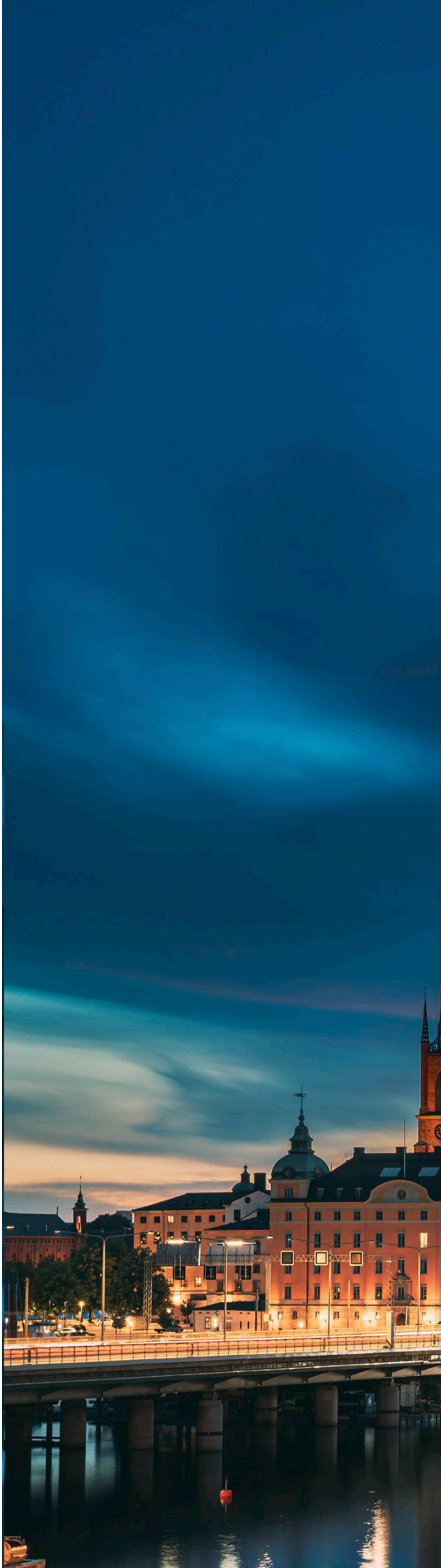
To be able to defend against the silent threats we need to have visibility in all aspects of our IT estates. Now, this fact is true for all sorts of defensive capabilities. But for the silent threat we have to go even further. We need visibility, logging and detection everywhere with deep insights into our own information flows. We need to ensure that we trust no one and no activity is by default marked as benign. It's not a matter of not trusting anything, but rather ensuring that everything is verified, and nothing goes unnoticed.

When considering visibility and detection, you need to have a full suite of detection services monitoring endpoints, identities and networks, including detection on the application layer and in the cloud through logs (SIEM). These tools must be leveraged to their full potential and deployed in tandem; supporting each other, empowered by behavior-oriented detection rules, and continuously realigned to cover emerging threats and new modi. They ensure retained capacity over time, even if attack infrastructure changes and, if done right, will push the asymmetrical game of hide and detect into the favor of the defender.

It is also a matter of protecting your business-critical intellectual property and anything else that might be of interest to a competitor or antagonist. To be able to do this you first and foremost must understand and know what this is. When you have come to terms with what it is that you must protect at all costs, you then need to understand what you are up against. This is where Threat Intelligence comes in. Looking at yourself from both the outside and inside, who are your main concerns and how do they operate? Is your IT estate adequately protected against their Techniques, Tools and Procedures? If not, then you need to urgently implement protection against these gaps in your defense.

Of course, this doesn't mean that Enterprises can stop worrying about ransomware and other opportunistic attacks, they will happen if that door is open to the opportunistic threat actors.

Properly defending against threats from both the outside and inside, especially the silent threat, is equally about best practice, continuous improvement, information security, cybersecurity – as well as IT Operations and Lifecycle Management.



The AI Revolution in Cybersecurity

Opportunities and risks in 2025

Generative AI surged into the mainstream with the release of ChatGPT in late 2023, sparking an explosive wave of technological adoption. Once the domain of innovators and niche technical applications, AI quickly became integrated into everyday professional and consumer experiences. By 2024, generative AI and machine learning have become pivotal in enabling industries, including cybersecurity.

AI as a Threat Amplifier for Cyberattacks

From a threat actor's perspective, AI is revolutionizing the execution of cyberattacks. The primary threat currently lies in its ability to automate and enhance existing attack strategies rather than invent entirely new ones. Tools powered by generative AI simplify traditionally complex tasks such as reverse-engineering security patches, creating malicious code, and generating convincing phishing emails. This reduces the skill threshold for attackers, allowing a broader pool of individuals to conduct sophisticated operations at scale.

One notable evolution, that does leverage AI for a previously impossible attack, is the use of Deepfake technology for targeted social engineering attacks.

These involve AI-generated real-time voice and video representations to impersonate trusted individuals in high-stakes scenarios, such as CEO or CFO fraud. While the number of such cases is currently limited, the financial scope per attack is significant, often exceeding €10 million.

As an accelerator of opportunistic attacks, AI is leveraged to automate phishing campaigns where generative AI produces grammatically and contextually relevant emails, increasing the likelihood of success. This democratization of attack models creates challenges of scale, potentially overwhelming defenders with a higher volume of increasingly sophisticated threats.

AI in Cyber Defense: A Growing Force

On the other hand, AI also empowers defenders. In 2024, its integration into cybersecurity systems focuses primarily on enhancing prediction and detection. Generative AI supports cyber threat intelligence by processing large datasets to identify and quantify risks as well as simplify application interaction. Machine learning, on the other hand, enables the detection of complex anomalous patterns that might indicate breaches.

Modern detection platforms, including those equipped with extended detection and response (XDR) capabilities, increasingly incorporate AI to simplify for users and lowering the competence threshold. By providing actionable insights and simplifying analysis, these tools have the potential to allow cybersecurity teams to respond to threats more quickly and effectively. While current AI implementations remain limited in fully automating responses due to risks of bias and inaccuracies, their potential for the future is obvious.

The Expanding AI Attack Surface
As organizations race to integrate AI into their operations, the associated risks are becoming apparent. From data breaches caused by inadvertently exposing sensitive information to public AI models to vulnerabilities in AI frameworks like the exploited CVE-2023-48022 affecting the Ray AI framework in March 2024, the rapid adoption of AI introduces new cyber risk.

The indiscriminate use of generative AI for business purposes has highlighted the critical need for robust data governance. Organizations that fail to classify sensitive data effectively risk overexposure, especially when integrating AI into customer-facing applications. To mitigate these risks, businesses must adopt structured architectures, assess supply chain vulnerabilities, and implement rigorous data lifecycle management.

The Future of AI in Cybersecurity

The impact of AI on cybersecurity will continue to grow. Analysts predict a compound annual growth rate of 19.1% for AI technologies, with the market size reaching $1.8 trillion by 2030. This expansion brings both opportunities and challenges. On the defensive side, AI's ability to analyze and interpret large datasets promises to improve threat detection and response. However, the sophistication of AI-driven attacks is also expected to increase.

The widespread availability of generative AI tools could transform the unsophisticated and blunt opportunistic attacks of today into tiered, automatically tailored campaigns of much greater sophistication.

Additionally, the decentralization of AI infrastructure may introduce vulnerabilities that are harder to detect and patch, amplifying risks across the supply chain.

Strategic Recommendations for a Resilient Future

To harness the benefits of AI while mitigating its risks, organizations should adopt a proactive approach:

1. **Invest in AI-Augmented Cyber Defense:** Secure machine learning powered detection capabilities in the network layer and prepare to implement coming generations of generative AI enabled detection capabilities.

2. **Secure AI Deployments:** Implement thorough vetting processes for AI applications, focusing on architecture design, supply chain security, and data management.

3. **Adapt to Evolving Threats:** Stay ahead of attackers by continuously evaluating the threat landscape and refining defense strategies.

AI is increasingly transforming cybersecurity into a dynamic, high-stakes battlefield. By leveraging its strengths responsibly and addressing its vulnerabilities, organizations can protect their assets and capitalize on

Cascading Effects of Supply Chain Breaches

When the breach is not your fault, but your problem

In today's interconnected society, supply chain attacks represent a significant challenge for cybersecurity, posing unique risks and complexities for organizations.

When a supply chain is breached, the consequences can cascade throughout the entire network. A single compromised vendor can expose sensitive data, disrupt operations, and damage reputations.

In early 2024, a significant security breach was discovered in the XZ compression utility, a tool widely used in Linux systems. This breach involved a hidden backdoor that allowed unauthorized access to affected systems. The backdoor was found during an investigation into system performance issues. Although the compromised versions were not widely deployed, the potential risk was high due to the tool's extensive use. The attacker had spent years gaining trust within the project before introducing the malicious code. Once discovered, the issue was quickly addressed, with the compromised versions removed and patched. This incident underscores the importance of rigorous security measures and vigilance in managing software supply chains to prevent such vulnerabilities.

The ransomware attack on Tietoevry in January 2024 was an incident highlighting the extensive impact a single compromised provider can have, emphasizing the importance of robust security measures across the entire supply chain. Occurring during the night of January 19-20, the attack managed to breach one of Tietoevry's data centers in Sweden, causing widespread disruptions. The

attack affected several of Tietoevry's customers, including critical government services. This led to operational challenges and data losses for various organizations. Some regional healthcare services were notably impacted, with disruptions affecting patient data and service availability.

The breach had a noticeable impact on Swedish society. Services across multiple industries were disrupted, causing inconvenience and operational delays for numerous entities and individuals. For example, a gardening chain store had to close its stores and halt e-commerce activities. A sports clothing retailer experienced website shutdowns, affecting their online sales. Additionally, a movie theater chain was unable to sell tickets, leading to significant revenue losses.

The attack also affected several Swedish municipalities. For instance, several municipalities experienced disruptions in payroll systems, library services, and high school selection processes. Furthermore, at least 127 Swedish government agencies connected to the personnel management system Primula were affected, raising concerns about the potential exposure of sensitive personal data.

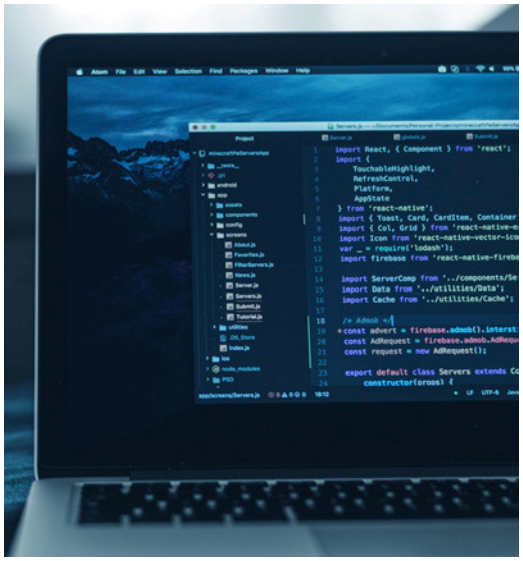
Challenges in Protecting IT-Estates Beyond Your Control

Protecting IT estates that are not directly under your control adds another layer of complexity. Organizations often rely on numerous third-party vendors, each with its own cybersecurity practices and standards. This lack of visibility and control can create blind spots, making it difficult to ensure consistent security measures across the entire supply chain. Additionally, the increasing complexity of supply chains, with multiple tiers of suppliers spread across different geographic locations, expands the attack surface and introduces more potential entry points for cyber threats.

One of the primary challenges is the risk posed by third-party vendors. Vendors with inadequate cybersecurity measures can become weak links, exposing the entire network to potential attacks. Ensuring that all partners adhere to robust security standards is essential but challenging. Limited insight into suppliers' cybersecurity practices can leave organizations vulnerable to hidden threats. Comprehensive supply chain mapping and regular audits are necessary to enhance visibility. Different suppliers may follow varying security protocols, leading to inconsistencies and potential security gaps. Establishing uniform security requirements and ensuring compliance across all partners is critical.

Employees or contractors within the supply chain can pose significant risks if they have malicious intent or are compromised. Implementing strict access controls and monitoring can help mitigate this risk. Ensuring the integrity of data as it moves through the supply chain is vital. Any tampering or corruption can have serious consequences, affecting the reliability and security of the entire operation.

To address these challenges, organizations must adopt a proactive approach to supply chain cybersecurity. This includes conducting thorough due diligence on all third-party vendors, implementing stringent access controls, and regularly assessing the cybersecurity posture of all partners. Additionally, fostering a culture of transparency and collaboration within the supply chain can help identify and mitigate risks more effectively.




112.383
189.623
155.830
117.210
93.073
88.245
122.038
160.658

Why Cybersecurity and Privacy Goes Beyond Compliance

How Goodhart's Law is undermining legal value

In today's digital economy, organizations face an intricate web of regulations related to cybersecurity, data protection, and privacy. The European Union, in particular, has been and continues to be prolific in introducing legislation aimed at safeguarding digital assets and personal data. Amid this regulatory surge, many legal and privacy professionals have trapped themselves in a compliance-centric mindset, emphasizing documentation over actual security measures.

This phenomenon, the author argues, is a manifestation of Goodhart's Law:

"When a measure becomes a target, it ceases to be a good measure."

By prioritizing compliance metrics – such as policy creation and procedural checklists – over material goals to enhance security and data protection, professionals risk undermining their organization's safety as well as their profession's and their own commercial credibility with commercial stakeholders.

Understanding Goodhart's Law in a Legal Context

Originally articulated in the field of economics, Goodhart's Law highlights how metrics lose their effectiveness when they become targets in and of themselves. In other words, when individuals or organizations fixate on specific measurements to gauge success, those measurements can distort behavior, leading to skewed or even counterproductive outcomes.

Within cybersecurity and data protection, Goodhart's Law manifests when compliance requirements become the primary focus rather

than the means to increase maturity in security and data protection. Legal and privacy professionals may concentrate on producing exhaustive documentation to demonstrate adherence to regulations like the General Data Protection Regulation ("GDPR"), the coming directive for a high common level of cybersecurity across the Union ("NIS 2 Directive"), or the upcoming Digital Operational Resilience Act ("DORA"). But the question is how this creates a valuable change within the organization to increase its resilience against adverse events and to protect its data?

While documentation is essential, an overemphasis on it can lead to neglecting the actual implementation of practical security and data protection measures. This creates a false sense of security and leaves organizations vulnerable.

Keep the Goal the Goal

Clients and stakeholders increasingly recognize that mere compliance does not equate to security or data protection. When legal and privacy professionals prioritize paperwork over protection, they risk losing the trust of commercial stakeholders who seek to minimize overhead costs and drive revenue as well as the trust of both the market and the legislators and supervisory authorities who expect their data to be genuinely safeguarded.

Even if supervisory authorities' enforcement has been disappointingly lax under the GDPR, there are discussions in Brussels regarding a stricter enforcement culture as well as increased demands on supervisory authorities under other legislation that is produced under the EU's Digital Agenda. There is, at the same time, a growing risk for organizations

to lose business or face significant financial and reputational damage due to, e.g., data breaches or cyber incidents, increased supply chain risk management obligations on customers forcing them to implement extensive vendor vetting procedures and audit schemes, and due diligence processes related to procurement of cyber insurance products or mergers and acquisitions.

Legal and privacy professionals who prioritize compliance metrics over practical security measures can mislead management into wrongly expecting returns proportional to invested resources, while also risking a diminishment of the organization's value to customers, insurers, and potential buyers if actual changes are not enacted. A compliance-first approach can therefore create a rigid environment where innovation is stifled by opaque and time-consuming internal processes, diverting attention and resources away from commercial goals. By neglecting the practical aspects of security and data protection, legal and privacy professionals may inadvertently hinder the development of proactive strategies that could provide competitive advantages.

Moving Beyond Compliance: Strategies for Legal and Privacy Professionals

To avoid the pitfall of Goodhart's Law, legal and privacy professionals must adopt a more holistic approach to put action first, documentation last. By reordering ways of working, actions can again become the target and documentation the measure. This would not only help frame fundamentally important issues in language appropriate to secure sufficient funding and resources from management in the short term, but also to foster commercial credibility and therefore likelihood to be included early in setting and steering strategic goals in the long term. Including security and data protection as integral parts of the commercial strategy can over time lead to fewer interruptions to innovation and development, reduced risk of litigation, robuster ways of working, and, ultimately, a competitive advantage.

Reframe the Role of Compliance
Regulatory requirements are a map, not necessarily the map – they are in other words a starting point setting out the landscape for how organizations need to operate to meet a baseline deemed relevant by the legislator. However, the legislator does not know your organization and its particular circumstances. The translation of a baseline to a specific roadmap is therefore the obligation of legal and privacy professionals. Shift the attention from ticking boxes to assisting the

organization achieve tangible meaningful outcomes to protect both the organization and its stakeholders.

In practice, this means identifying regulatory obligations and using these as the starting point for engaging with experts across different functions to identify and design initiatives that address the organization's particular circumstances and challenges. For security and data protection, this means cross-departmental collaboration between, e.g., legal, internal IT, (information/protective) security, and/or other relevant functions. To reuse the example above with policy creation as the target rather than a measure, this can mean that a cross-functional team would design and implement fundamental principles and baseline requirements to inform and govern an organization's processing of personal data and then document these measures in a privacy policy. The policy would act to transparently communicate why, how, and when the organization processes personal data. It would, in other words, only serve as a means to deliver information, rather than being an end goal in and of itself.

Embracing a Balanced Approach

The complex cyber threat environment and the rapid growth of legislation require legal and privacy professionals to expand their focus beyond compliance documentation. By understanding and avoiding the pitfalls of Goodhart's Law, they can contribute more effectively to their organizations.

1. **Shift Mindset:** View compliance as part of a broader security and data protection strategy aimed at protecting the organization, and security and data protection strategies as part of the very fabric out of which the commercial strategy is built.

2. **Engage Practically:** Collaborate across functions to implement actionable measures to create the necessary changes.

3. **Enhance Credibility:** Build trust with stakeholders by demonstrating a commitment to genuine security and data protection, not just regulatory adherence.

By adopting these strategies, legal and privacy professionals can drive real value creation, enhance their commercial credibility, and contribute to building safer, more secure organizations.

Outlook 2025

Geopolitics shape the cyber threat landscape

The West is facing many obstacles and challenges in the upcoming years. In a time where we need to be more united than ever, we are more divided than we have been in 80 years. The EU is based on a legalistic approach to international relations, in a world where the rules-based order imposed after WW2 is gradually being eroded. The peace in Europe is threatened both by the overt Russian aggression in Ukraine and by hybrid attacks that include cyber sabotage.

Russia is actively engaged in an information war with nations supporting Ukraine. Just as the West imposes costs on Russia for their aggression against Ukraine through economic sanctions, Russia attempts to impose a cost for the support, by conducting sabotage and cyberattacks against the West. These attacks will likely not cease until either Russia is defeated or its ambition is satisfied.
Politically motivated cyber sabotage groups are also looking to escalate their attacks as the impact of simple distributed denial-of-service attacks appears to be shrinking in the media. Several hacktivist groups will likely experiment with ransomware encryption as a form of cyber sabotage, especially those sponsored by adversarial governments.

The EU will likely continue to struggle to formulate a response to increasing cyber sabotage and other cybersecurity issues. The EU decision making is slow in formulating strategies to impose costs for these attacks.

Attempts to mandate better cybersecurity through regulations risk becoming counterproductive as the EU legislative processes are far slower than the technical developments they attempt to regulate. For many organizations there is a real risk that they will be forced to choose between best practice cybersecurity measures and legal compliance with limited resources.

The new US administration will likely above all else add more uncertainty to the geopolitical landscape. Ideological differences in the approach to regulation and problems with disinformation online may put Europe on a collision course with the USA.

One thing that can be predicted, however, is that the new US administration will likely be far more favorable to cryptocurrency than the outgoing. This will likely end attempts to curtail cyber extortion by regulating cryptocurrency.

If the US administration attempts to promote and normalize the use of cryptocurrency in international transactions, it will put pressure on traditional financial institutions to get in on the market. This will in turn expose them to more cybercrime. Many cybercriminals already target cryptocurrency holders with a wide array of cyberattacks.

The geopolitical rivalry between China and USA is expected to deepen. A looming trade war will also likely involve Europe, as China's ambitions to solve their internal economic contradictions through increased exports will clash with the EU's attempt to preserve its own industrial base. China will likely become even more nakedly aggressive in its attempts to use cyberattacks to win access to key resources and promote their own industry at the cost of European manufacturers. China will also likely use online disinformation campaigns to weaponize legitimate worries over climate issues to harm European resource and manufacturing sectors.

Building resilience and increasing cooperation against these evolving threats will be crucial to maintaining national security and protecting the democratic institutions in Northern Europe.

The geopolitical and security situation in Europe, and particularly in Sweden's vicinity, is complex and worrying. Increased level of cyber attacks from antagonistic states is a matter of when and not if.

Additionally, we have a serious situation within internal security with organized crime and a criminal economy that poses a significant strain on society, including businesses. The main venue for illicit pressure and influence is within the cyber domain. We all need to enhance and improve our security and move from cooperation to collaboration, especially between the public and private sectors. Sharing of lessons learned and best practices is of key concern.

Johan Sjöberg,
Director Security and Defence Policy
Confederation of Swedish Enterprise

A Changing Cybercrime Scene

As our data have shown, it appears that many large enterprises in the Nordics have invested in cybersecurity and now see these investments pay off. This, together with active disruption of the ransomware ecosystem by international law enforcement, is forcing cybercriminals to change their tactics.

Some of the top cyber extortion groups will likely continue to target large enterprises, by investing in more advanced techniques, like zero-days, supply-chain attacks on vulnerable software solutions, and more refined social engineering. The bulk of the cyber extortion groups will however likely turn to attacking smaller organizations with less cybersecurity, using faster, partially automated attacks.

Cybercriminals will also continue to use LLM and AI to refine their social engineering attacks. Chatbots and deepfake technology will be used both for fraud and for breaching networks. Threat actors may also begin to use AI to speed up the process of reversing known vulnerabilities and turning them into workable exploits.

The window available to patch vulnerable systems, already measured in days, may shrink even more in the future. Some actors may even use AI technology to find zero-day vulnerabilities in software in the future.

The sanctions imposed by the West on regimes is putting the economies of countries like Iran, Russia and North Korea under immense pressure. Intelligence organizations could resort to crime and extortion to finance their own activities. The North Korean intelligence is known to have used cybercrime to finance their own activities for years and the same is now happening in Iran. Will Russia be next?

While improvements in cybersecurity in the Nordics have made great strides in recent years, cyber extortion and other forms of cybercrime is far too lucrative to end completely. The competition between criminals and improved defenses will spur adversaries to develop new techniques. When we work together and safeguard one, we strengthen resilience for the rest as well. The threat landscape continues to evolve, *and so will we.*

TRUESEC

Meet the Experts Behind This Report

Marcus Murray
Founder, Truesec

Anna Averud
CEO, Truesec

Daniel Jaurén
Head of Threat Intelligence
Truesec

Mats Hultgren
Director of Operations
Incident Response, Truesec

Levi Bergstedt
Chief Legal Officer, Truesec

Amanda Lövström
Senior Legal Counsel, Truesec

Petter Fahlström
COO, Truesec

Mattias Wåhlén
Threat Intelligence Expert
Truesec

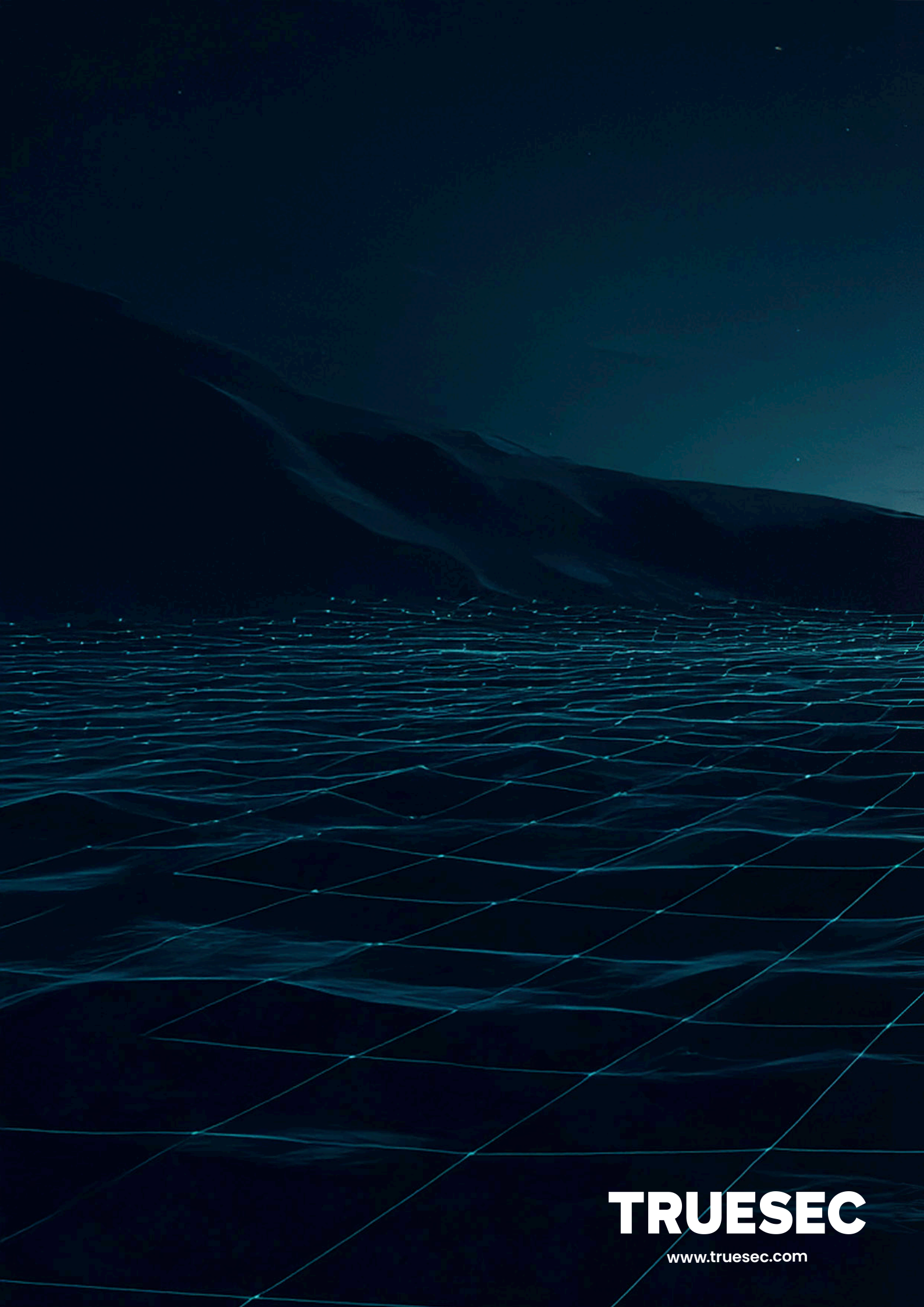
Nicklas Keijser
Senior Threat Analyst, Truesec

TRUESEC

Our Purpose Has Been Clear Since Day One:

Prevent Breach and Minimize Impact.

www.truesec.com


TRUESEC
www.truesec.com