2Secure

RANSOMWARE: A GLOBAL BUSINESS THREAT

Whilst Board agendas have been packed full for the las two years, directors are consistently asking more questions about risk. And one risk at the fore is ransom cyber-attacks and information security breaches. The last two years saw all things online and digital increase in prevalence and exposure. The accelerated need for access, innovation, and advancement has left many companies and government actors around the world susceptible to cyber-attacks. Now, more than ever, protecting yourself against ransom attacks is critical. Cybercrime and cybersecurity breaches are increasing globally, threatening organisations across all countries and industries. The global losses from cybercrime are estimated to hit a record of US $6 trillion for 2021 as the Covid pandemic facilitated new opportunities for hackers to target consumers and businesses. Over the next five years, cyber incidents are expected to grow by 15 percent per year, reaching US $10.5 trillion by 2025. This is due to the propagation of sophisticate tools available to cybercriminals, jurisdictional uncertainty and relaxed attitudes towards cybercrimes in some countries.

Our supply chains and networks are globalised and interconnected, which increases our risk exposure. As cybercrime has no borders, European companies must be prepared to prevent and respond to cyber incidents worldwide, implementing cyber-security risk assessments and having a plan of action to anticipate, prevent and respond to this kind of problems.

Among the different types of cyber threats, ransomware is commonly used by cyber criminals that target a wide range of industries. 2Secure has recorded high-profile ransomware attacks against governments, businesses, universities and hospitals. More than 500 schools and almost 70 government organisations in the US alone were hit by ransomware attacks in 2019. A particularly concerning trend is the targeting of IT and cloud computing sector, where cyber extortionists are infecting larger numbers of victims by gaining access to cloud computing providers. While the largest providers have stringent security measures in place that are currently effective, many smaller providers who operate in specific markets or sectors have proven vulnerable to attacks.

2Secure has observed sharp increases in ransomware demands over the last two years, including large and successful attacks against state-owned companies. This reverses the trend seen in 2018 when there was a decrease in ransomware attacks, with attacks now more sophisticated and resulting in larger financial losses for companies that do not pay. Ransomware criminal groups are using nation state-level tactics in order to do maximum damage to these companies when their ransomware encrypts the victim’s system. A growing number of ransomware actors have also begun to exfiltrate data, rather than simply blocking access to it. They then threaten to release the information if they are not paid, adding the risk of legal costs if data is leaked into the public domain. This creates a high-pressure and complicated negotiation process for crisis management teams.

RANSOMWARE

WHAT IS RANSOMWARE

In recent years, ransomware incidents have become increasingly prevalent among organisations and government entities. Ransomware is a form of malicious software or malware created by cybercriminals where they block access to data or IT systems on an organisation´s device and demand ransom in exchange to restore access. In a ransomware attack, cyber extortionists encrypt an organisation's data and demand a payment for a decryption key.

The global cost of ransomware has increased by 33% in 2020

Backup data can also be compromised in an attack, and it can be hard to determine the extent of the damage and the likelihood of restoring an organisation's systems without a decryption key at the initial stages of an incident.

Perpetrators almost exclusively demand ransoms in the cryptocurrency Bitcoin, and businesses often need time to understand the process of setting up a Bitcoin wallet as well as the business ramifications of spending an extended period without access to their systems.

Ransomware attacks can have critical consequences for both organisations and individuals. The reputational impact of ransomware attacks have also proven challenging for large and small businesses. Ransomware can disturb business processes and leave organisations without the data they need to operate and to deliver services. Cyber criminals have become more sophisticated by threatening victims that they will release stolen data if they refuse to pay and naming and shaming victims in public as secondary forms of extortion.

The monetary cost of ransoms has increased by 33 percent in 2020, with some payments exceeding US $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. These malicious actors also increasingly use tactics, such as removing system backups that make restoration and recovery harder or impossible.

Some examples of how ransomware can gain access to our devices:

- Opening an email with a malicious attachment.
- Clicking an ad that downloads a malicious file.
- Clicking on a malicious link that downloads a file from an external website.
- Visiting a website that is embedded with malware.

The ransomware takes advantage of vulnerabilities in the computer when the user executes a malicious file, not knowing that the file is ransomware. From this computer the ransomware can propagate throughout more computers and networks in the organisation. The ransomware simultaneously encrypts files on all the computers, and then displays messages on their screens demanding payment in exchange for decrypting the files.

CASE: EARLY RANSOMWARE – THE AIDS TROJAN

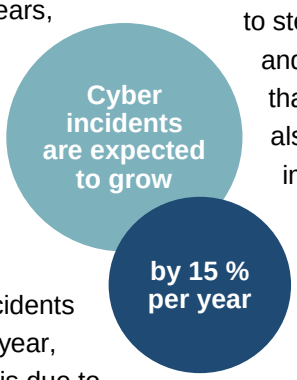
For many of us, ransomware seem like a recent phenomenon. However, one of the first known Ransomware attack was the AIDS Trojan attack, launched in 1989. While most ransomware of today is deployed online, this was not an option in 1989. Instead, Joseph Popp, the inventor of the ransomware and an active AIDS researcher, hijacked a mailing list for people subscribed to the World Health Organisations (WHO) AIDS conference. 20,000 people in 90 nations were sent infected floppy disks, labelled “AIDS Information Introductory Diskette”. The Trojan was disguised as a questionnaire about the AIDS virus and once booted, the Trojan would soon hide directories and encrypt file names on the C: drive, effectively rendering the device unusable. Popp set the ransom at USD189 and asked the victim to send it to a post office in Panama.

The motivations for the attack remain unknown. During his arrest, Popp would claim that he intended to donate the ransoms to AIDS research while it has also been alleged that the WHO had rejected him for a job position and that he was motivated by revenge.

Where Joseph Popp had to organise and fund the distribution of a significant amount of floppy disks, threat actors of today have it much easier in terms of distribution of malicious code relying on social engineering. With 4,6 billion active internet users, many of whom are connected on several devices, criminals can now distribute malicious code and extort ransoms with the threat of financial and sometimes societal havoc. The advent of cryptocurrency has also made it harder to tie payments to an individual, lowering the risk of detection for the criminal. However, many less sophisticated ransomware attacks still rely on tricking an unsuspecting victim into clicking on the wrong thing. Between 95 and 99 percent of cyber-attacks still rely on social engineering. As such, many attacks can be avoided by a well-established security culture and awareness amongst end-users.

WHAT ARE THE RISKS AND TRENDS INTERNATIONALLY?

Even companies that had no intention to embark on digital transformations in 2019 have been forced to undergo significant changes due to new consumer and employee demands. The business environment is different today than it was two years ago, and so is our risk exposure. Over the last two years, cybercrime and cybersecurity breaches are increasing at a rapid rate world widely, threatening organisations across all countries and industries.



The global losses from cybercrime are estimated to hit a record of $6 trillion for 2021. Over the next five years, cyber incidents are expected to grow by 15 percent per year, reaching US $10.5 trillion by 2025. This is due to the propagation of sophisticate tools available to cybercriminals, jurisdictional uncertainty and relaxed attitudes towards cybercrimes in some countries.

STATISTICS

- 95% of cybersecurity breaches are caused by human error.
- 88% of organisations experienced spear phishing attempts in 2019.
- 68% of business leaders feel their cybersecurity risks are increasing.
- On average, only 5% of companies' files are properly protected.
- Data breaches exposed 36 billion records in the first half of 2020.
- 86% of breaches were economically motivated and 10% were interested on espionage.
- 45% of breaches included hacking, 17% involved malware and 22% phishing.
- The top malicious email attachment forms are .doc and .dot which make up 37%, the next highest is .exe at 19.5%.

Cyber-risks in the supply chain network

Businesses sectors that store valuable information like healthcare and finance, together with the governments and public administrations are regularly bigger targets for cybercriminals who want to steal Social Security Numbers, medical records and other personal data. However, the reality is that no industry is safe. Lower-risk industries are also targeted due to the perception that they implement relaxed security measures in their business.

The evolution of supply chain networks has principally been driven by technology. Business of all sizes are moving to the digital space, some forced by Covid outbreak.

While organisations implement cybersecurity measures for themselves, there are several vulnerabilities when contacting and working with manufacturers, suppliers, global partners and other service providers to consider, which may of them are usually smaller businesses with weaker cybersecurity procedures. These are favourable entry points for cybercriminals, very well prepared to breach security at the first chance.

For these reasons, the cybersecurity boundaries between organisations are getting weaker. About 80 percent of reported breaches occur within the supply chain network.

Wherever your organisation appears in the supply chain, if you are connected to any, you are exposed to risk.

Supply chain threats include data leaks, customer data thefts, denial of service, disruption of business, and other malware attacks such as ransomware.

Chief information security officers (CISO) and Chief information officers (CIO) are drowning in a deluge of requests and competing demands and information. The responsibility of CISOs, risk managers, and Boards is increasingly seen to extend beyond their own companies and into third parties and suppliers. Attackers do not distinguish

between your company and your suppliers and attacks like the Sunburst attack highlight that third-party companies provide an attractive opportunity for cyber-criminals.

Mature companies already have conversations with their suppliers and third-parties about their security posture, employee access to sensitive information, background checks, cloud security, and other information security practices. Ransomware is but one of many potential cyber-risks, with growing risks from nation-states, industrial-espionage, data theft, and malicious activity. Regular and transparent communication is needed to ensure an appropriately high level of information security and cyber defences.

Businesses should be including contractual obligations on suppliers and third parties to ensure minimum enterprise cyber security standards are complied with. Companies and government actors need to assess and work with not just their immediate partners, but also their second-tier suppliers, many of whom will be smaller organisations, often with less robust information security protocols in place.

Cybersecurity plans in the supply chain network should consider:

- **Technology**: response and recovery should not be limited to internal technology setups. The adoption of cloud technology, internet of things (IoT) devices and virtual servers opens up new vistas for breaches. To safeguard cybersecurity processes organisations must implement actions like two-factor authentications and biometric access control through all internal as well as third-party systems.
- **People**: all employees and trading partners should be included in the cybersecurity framework. Clear roles and responsibilities for all personnel and third-party entities in protection, detection, and response and recovery measures are crucial. Bring-your-own device (BYOD) policies are the main source of malware and phishing in the supply chain. No personnel-owned device should be allowed to connect to the corporate infrastructure without channelling them through a virtual private network (VPN).
- **Process**: establish cybersecurity processes posture before onboarding any new business or individual in your ecosystem. Regular monitoring to guarantee compliance of processes by all partners is essential to ensuring the capability of the recovery and response plan.

HOW COVID-19 HAS AFFECTED CYBERSECURITY

- Since the pandemic began, the FBI has reported a 300% increase in reported cybercrimes.
- 27% of COVID cyberattacks target banks or healthcare organisations
- Cyber-attacks against banks have increased by 238% in 2020.
- Data breaches in the healthcare industry increased by 58% in 2020.
- In April 2020, Google blocked 18 million malware and phishing emails associated to Coronavirus every day.
- Remote work has increased the average cost of a data breach by $137,000.
- Cloud-based cyber-attacks rose 630% between January and April 2020.
- Remote workers have caused a security breach in 20% of organisations.

CASE: THE WANNACRY ATTACK

One of the most infamous cases of ransomware attacks was that of WannaCry in 2017. WannaCry is a ransomware crypto-worm. As such, it spread without active aid from an individual, identifying vulnerable systems on its own. Once executed, it encrypted data and demanded a ransom. To gain access, WannaCry used an exploit known as EternalBlue, which was specific to computers running Microsoft Windows.

The EternalBlue exploit was allegedly developed by the National Security Agency (NSA) as part of their effort to find and exploit vulnerabilities in Microsoft software. This exploit was not initially disclosed to Microsoft, instead it became one of several exploits stockpiled the NSA. However, in March 2017, Microsoft pushed the MS17-010 Security Bulleting witch patched up the weakness. One month later, hacking group Shadow Brokers leaked the exploit after hacking the NSA. On 12 May 2017, WannaCry was released, making use of the EternalBlue exploit. As many clients had yet to install the now two-month-old patch, the crypto-worm spread quickly, at its peak infecting over 10,000 Windows-devices per hour.

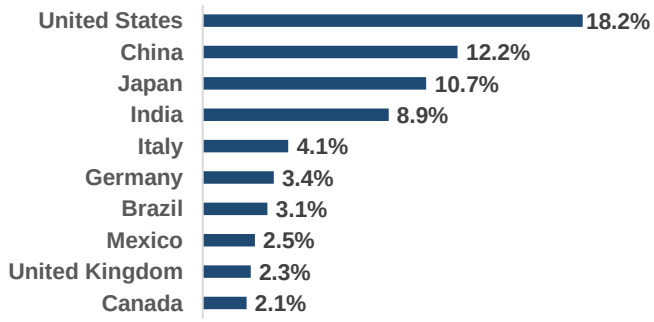
As the dust settled, around 230,000 computers had been infected in over 150 countries. The estimated global monetary loss caused by the WannaCry ransomware has been estimated at four billion dollars. The effects of the ransomware cannot only be measured in monetary losses, agencies and institutions critical to the functioning of society were hit severely affecting their ability to operate. In the United Kingdom, the ransomware severely limited the National Health Services (NHS) for a number of days with numerous hospitals having to divert patients. Out of the 236 NHS trusts (public sector corporations), 80 were affected by WannaCry.

The WannaCry attack showcased many things, but one of the most important lessons is the need to ensure that your systems are up-to-date in terms of security updates, or patches. This applies to both big business and private users. Being constantly reminded to update security solutions may be tedious, but it is threats like these that cause the updates, and it is updates like these that prevent the threats.

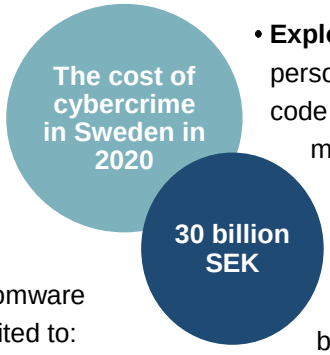
THE RANSOMWARE CHALLENGE GLOBALLY

Ransomware is detected more frequently in countries with higher numbers of internet-connected populations, and the U.S. ranks highest with 18.2 percent of all ransomware attacks.

Ransomware detections by country



When it comes to innovation or digitalisation, Sweden is one of the leading countries in the world. However, according to the cyber security index Sweden is far behind regarding cyber security, ranking number 44.The number of ransom attacks has tripled during 2020, and more Swedish companies have been victims of data breaches. The cost of cybercrime in Sweden is now exceeding 30 billion SEK per year.



There are several attack methods for ransomware used by threat actors. Including but not limited to:

- **Drive-by download attack**: a malicious code is downloaded from a website via a browser, application or integrated operating system without a user's permission or knowledge. Hackers can use drive-by downloads to inject banking Trojans, steal and collect personal information as well as introduce exploit kits or other malware to endpoints.

- **Phishing**: hackers use social engineering to trick users into breaking normal security practices and giving up confidential information, including names, addresses, login credentials, Social Security numbers, credit card information and other financial information. In most cases, cybercriminals send fake emails that look as legitimate sources.

- **Insider threats**: occurs when individuals close to an organisation who have authorised access to its network intentionally or unintentionally misuse that access to negatively affect the organisation's critical data or systems.

- **Viruses and worms**: malicious software programs designed to destroy an organisation's systems, data and network.

- **Botnets**: a collection of Internet-connected devices, including PCs, mobile devices, servers and IoT devices that are infected and remotely controlled by a common type of malware. The cybercriminals that control these botnets use them to send email spam, engage in click fraud campaigns and generate malicious traffic for distributed denial-of-service attacks.

- **Exploit kit**: a programming tool that enables a person without any experience writing software code to create, customise and distribute malware. Hackers use it to attack system vulnerabilities to distribute malware or engage in other malicious activities, such as stealing corporate data, launching denial of service attacks or building botnets.

- **Advanced persistent threat attacks (APT)**: is a targeted cyber incident in which an unauthorised intruder penetrates a system and remains undetected for an extended period of time. The objective of an APT attack is to monitor network activity and steal information to gain access, including exploit kits and malware. Hackers typically use APT attacks to target high-value targets, such as large enterprises and governments, stealing data over a long period.

- **Malvertising**: a technique hackers use to inject malicious code into legitimate online advertising systems and web pages. This code usually redirects users to malicious websites or installs malware on their computers or mobile devices.

TIPS FOR AVOIDING RANSOMWARE

The principal approach to avoid being exposed to ransomware or any type of malware is to be a cautious and conscientious computer user. Cybercriminals have become increasingly intelligent and users need to be careful on what download and what click on. Other advices:

Keep operating systems, software, and applications current and up to date.

Make sure anti-virus and anti-malware solutions are set to automatically update and run regular scans.

Back up data regularly and double-check that those backups were completed.

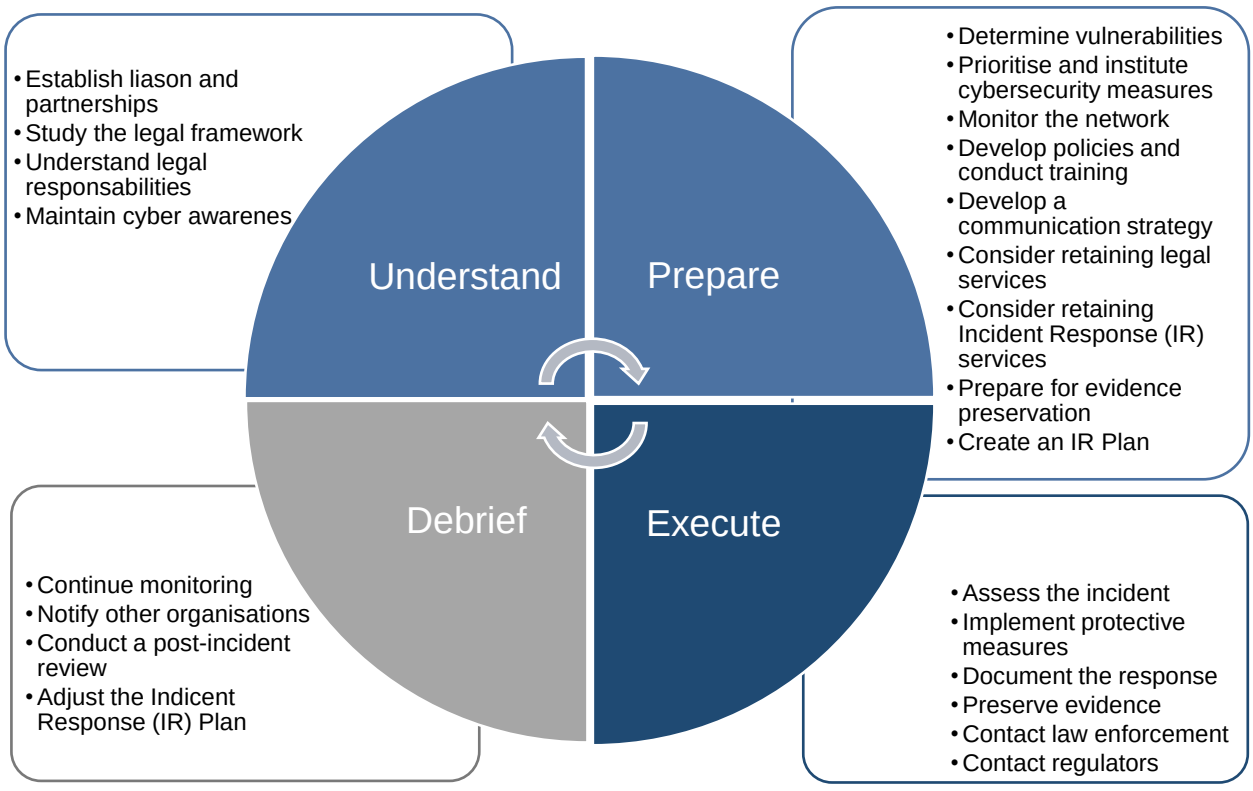
Secure your backups. Make sure they are not connected to the computers and networks they are backing up.

Create a continuity plan in case your business or organisation is the victim of a ransomware attack.

Use two-factor authentication and strong passwords mixing alphanumeric letters with uppercase and lowercase characters.

Not to reuse the same password. For this, is recommendable to use a password management tool.

HOW TO PREPARE FOR AN INFORMATION SECURITY BREACH



CASE: THE 2021 KASEYA ATTACK

In July 2021, the group REvil released a ransomware that caused downtime for thousands of companies. REvil, a Russian ransomware-as-a-service (RaaS) group, had gained access to the Kaseya-developed remote monitoring and management software called Virtual System Administrator (VSA). The service is a web-based application for monitoring, administrating, and reporting on systems within the customers own infrastructure.

By exploiting an authentication bypass within VSA, REvil managed to distribute their malware through hosts that used the service. One of the most notable Scandinavian victims was Norwegian company Visma who in turn managed systems for the Swedish food store Coop. As a result, a majority of Coops 800 food stores had to shut down their operations for several days, which not only caused severe financial loss but also affected the food supply in some of Sweden's more remote areas where Coop was the only major food store. According to Kaseya, between 800 and 1500 businesses were affected by the ransomware.

On 13 July, REvil's abruptly disappeared from the dark web making it, amongst other things, impossible for victims to pay the ransom and seek support in restoration of the encrypted data. This caused speculation on whether the Russian government had taken action following pressure from the United States president. Three weeks after the attack, the situation was resolved when Kaseya announced that they had received a decryption key from a trusted third party. According to Kaseya, they refused to pay the USD 70 million ransom and it is still unknown how the key was acquired. REvil remerged online on 7 September.

The Kaseya attack targeted a vulnerability in the supply chain, spreading downstream and got a foothold in businesses tied to the service who, to know fault of their own, had been exposed. Additionally, Kaseya had been recognised for their cybersecurity competencies, making it hard for users of their VSA to predict this type of an incident. Even when great measures have been taken, organisations still run a certain risk of becoming the target of attacks like these. It is then important to have established good incident response plans beforehand to ensure that damages are minimised and continuity ensured.

WHEN DEFENCES FAIL

This new period of sophisticated cyber and ransom attacks is keeping pace with our rapid adoption and expansion of digitalisation. Cybercriminals are just as fast at exploiting weaknesses as we are at adopting and experimenting with new technology. We must be doing more than pursuing compliance, and seeking robust enterprise cyber security risk management systems that cover the wide risk exposure all companies and government actors have today. Sadly, even when the best precautions are taken, all systems do run a certain risk of ransomware attacks, albeit to different degrees. So what can companies do when defences have failed and the demand for a ransom is a fact?

Do not pay the ransom. Paying the ransom feeds the loop by motivating threat actors to continue using ransomware as an easy source of income. Additionally, paying the ransom gives little protection from additional attacks.

A 2021 survey study by Cybereason showed that 80 percent of companies that payed ransoms in ransomware attacks suffered a second attack. The study also identified that it was often the same group the conducted both attacks. Furthermore, 92 percent of organisations don't get all their data back after paying the ransom; there is no guarantee the attacker will actually give you the decryption key.

However, not paying a ransom is easier said than done, especially when operations halt as a result.

Identify, and if possible, disconnect affected devices from the network. If possible, identify patient zero. Although disconnecting the device does not guarantee that the other devices have not been affected, it is the fastest hands-on action you can take to ensure that the device does not further reciprocate the ransomware throughout the network. It might be necessary to take the infected server offline. If the infected device cannot be disconnected from the network, you may have to power it down.

However, doing so may make you lose evidence, important to both security specialists and the police.

Contact a cybersecurity specialist. As a target, one can, and should, take several steps to minimise the damages. However, contacting a qualified professional ensures that the steps you take are right for this specific occasion. Ransomware can vary in many ways, such as in the choice of vectors, ransom sum, function etc. Cybersecurity specialists can help you understand the specifics of your situation and both advice and assist you in the choice of action.

Report the incident to the authorities. Law enforcement agencies around the globe work together to combat these threat actors. Ransomware is a constantly evolving threat and the more information they have access to, the better. By notifying law enforcement, you ensure that information that may be of use to prevent further attacks becomes known. Furthermore, you increase the chance that the perpetrators are caught and decryption keys are seized. If you are the victim of fraud, cybercrime, ransomware, or other criminal activity, contact 2Secure and we can support you to contact the relevant authorities and address the critical actions that must be taken.

Cleanse and restore your systems. To ensure that the ransomware is removed from your servers, you will have to wipe you storage. This also ensure your systems are ready for the restoration of data. Restoring backed up data can be time consuming dependent on how much data has been lost and where your backups are stored but it is a preferable option to paying the ransom.

2SECURE RECOMMENDS

1. **Plan.** As with all risks, a proactive strategy is preferable to a reactive one and the best way to prevent or minimise potential damages is to try to avoid them all together. Start by identifying your vulnerabilities. It is also important you establish or review current policies, incident response plans and cybersecurity training.

2. **Establish proper routines and processes.** When an attack occurs, having planned and established proper procedures beforehand is key. Ensuring that the organisation has implemented robust incident response plans and recovery capabilities will help mitigating the risk as well as speed up the recovery process if an attack occurs. This extends to partners as wells. Ensure proper cybersecurity processes before on boarding any new business or individual in your ecosystem and monitor to guarantee compliance of processes by all partners.

3. **A proper response.** When an incident occurs, be sure you know what to do and have tested all elements of your plan. Assess the incident and implement the protective response measures. Consider the option of not paying the ransom and the need to preserve evidence for authorities. Only turn off devices if they cannot be disconnected from the network. Contact 2Secure and we will help you with essential crisis management activities.

4. **Seek guidance**. Make use of professionals to guide you through the proactive and reactive processes if your organisation is unsure about proper measures or responses. Seeking outside help is also a good way to ensure an impartial third party review of current routines and planning.

2Secure

+46 101 740 310

Visit our website for more information on how 2Secure can support you with your international security and risk management needs.

We provide bespoke and tailored analysis, global risk monitoring and strategic foresight, enterprise security risk management support, travel risk management, trend monitoring, training, and risk assessments on a variety of issues and locations around the world. Our government, corporate, and family risk management services are tailored to your specific needs.

Email or call our experts for an obligation free discussion today.

2Secure

Box 34037 • 10026 Stockholm • www.2secure.se