IF'S RISK
MANAGEMENT
MAGAZINE
03/2020

CYBER
ISSUE

Risk Consulting

Cyber crime and digital risks skyrocket

Content

Insights into cyber and digital risks

Why did we dedicate an entire issue to cyber now? For one thing, cyber is something invisible and abstract in nature. Also, digital risks and cyber threats are relatively new and unknown to many yet are a critical and evolving area of risk management. As cyber attacks are on the rise, the cyber insurance market is growing rapidly, making this topic very timely indeed.

During Covid-19, cyber crime has skyrocketed. Criminal gangs and hackers quickly began to benefit from the fear and confusion that ensued, as the virus spread around the world. The past months have really highlighted the importance of digital tools that today's employees depend on. It is hard to imagine a situation where all those assets would not be available, or the data processed by them compromised.

The current cyber threat landscape and future risks are actively followed at If. With the launch of the Digital Risks & Cyber unit, we offer solid inhouse expertise to support our clients and partners. The unit is responsible for underwriting and risk management of If Industrial's cyber insurance portfolio.

Meet our authors

Mikko Peltonen
Head of Digital Risks and Cyber

Kalle Pohls
Reinsurance Manager, FI

Preben Danielsen
Head of Investigation, DK

Anders Nilsson
Head of Architecture and Platforms, SWE

Mika Rintamäki
IT Security Manager, FI

Publisher If, Nittyportti 4, Espoo, FI-00025, Finland, +358 10 19 15 15, www.if-insurance.com
Editor-in-chief Kristian Orispää
Project Editor Carita Hämäläinen-Tallgren
Art Director Ero Tsirika

Production If Creative Agency
Printing Newprint
Change of address industrial.client-service@if.fi
ISSN 1459-3920
Cover Photo Getty Images

Disclaimer This publication is and is intended to be a presentation of the subject matter addressed. Although the authors have undertaken all measures to ensure the correctness of the material, If P&C Insurance does not give any guarantee thereof. It shall not be applied to any specific circumstance, nor is it intended to be relied on as providing professional advice to any specific issue or situation.

Editorial

Cyber crime on the rise

Poul Steffensen
Head of BA Industrial, If

During the Covid-19 pandemic, cybersecurity experts and officials witnessed a significant rise in cyber attacks. In fact, the number of attacks, as well as the severity of these attacks, have both grown.

According to a U.N. counter-terrorism official, there was a 350% increase in phishing websites, while UK-based Iomart reported large-scale data breaches increased 273% in the same time period. Over the past months, Covid-19 related malware attacks have increased, but also advanced attack methods, such as island-hopping, are becoming increasingly common.

As the coronavirus spread, office buildings were locked down and many organisations had to make the shift to remote work quickly. Hackers and cyber criminals took advantage of the confusion, spotting opportunities to break into corporate networks as they struggled to keep pace with the new way of working. In fact, IT security teams around the world were working around the clock to maintain network security as hundreds, thousands, even millions of people began to log on to their company networks from home.

Digital risks come in many different shapes and forms. Last summer, the European Union set sanctions against multiple nations over alleged cyber attacks. Governments, businesses, individuals are all being targeted as criminals seek to gain financially from the panic and upheaval.

Cyber attacks are not going to go away. Therefore, it is critical to take the necessary precautions, be vigilant and maintain a proactive approach to your network security. Organisations need to be prepared on many levels (e.g. risk management, security awareness and security operations) and have the right capabilities in place to act before, during and after the attack has taken place.

In this issue of Risk Consulting magazine, we offer you insights from If's leading digital risks and cyber experts. Learn about the latest trends in ransomware, what to look for in cyber insurance and gain insights from experts at Danish Crown on how to secure production from an IT perspective.

Sources used: CNBC, ABC News, Iomart, ZDNet, PWC

If P&C Insurance, contact information
Finland: +358 1019 15 15 Sweden: +46 771 43 00 00 Norway: +47 98 00 24 00 Denmark: +45 7012 24 24 France and Luxembourg: +33 142 86 00 64
Germany: +49 6102 710 70 The Netherlands and Belgium: +31 10 201 00 50 Great Britain: +44 20 7984 7600 Estonia: +372 6 671 100
Latvia: +371 7 094 777 Lithuania: +370 5 210 89 25

GETTY IMAGES

Cyber insurance market evolving with the support of reinsurance

Information technology is widely seen as a major contributor to the growth of the global economy during the past decades. For example, business productivity, democratised information (alongside the emergence of fake news) and various other impacts caused by the digital revolution during the past two decades. These are known facts but come with a cost – dependency on the technological infrastructure. Increasingly material cyber risk, with a common definition still developing, splits into various components. These include malicious and non-malicious intent and covered objects such as intangible and tangible assets.

Article by Kalle Pohls

Yes – the insurance market for cyber insurance exists. Increasing demand for cyber risk transfer and services as well as product development are making cyber insurance a fast-evolving marketplace.

CARRYING CYBER RISK

In addition to the insurers' balance sheets and underwriting excellence, the cyber marketplace is supported by reinsurance and modelling of the aggregation of the risk on both portfolio and individual risk level. Reinsurers offer crucial back-up which enables insurers to provide cover and services to insureds while managing their balance sheet against both loss frequency and severity – as well as against a potential cyber catastrophe, which still remains to be seen.

The key functions of an effective cyber reinsurance market from the insurers' point-of-view are risk transfer, knowledge sharing and portfolio management. In the current financial world, the reinsurance market has been attracting new capacity year-on-year and cyber already has a freshly established role and underwriting community besides the conventional lines of reinsurance.

Warren Buffet of Berkshire Hathaway wrote in his annual letter to shareholders that there is a 2% risk of a $400 billion "super-cat" global cyber insurance disaster. Cyber is now akin to hurricanes, wildfires and earthquakes, carrying a similar level of risk. Despite the risk, many reinsurers, and insurers alike, are committed to providing services to the market.

CYBER INSURANCE LANDSCAPE

What makes the cyber insurance landscape slightly different – besides its accumulative nature – is the limited loss history and understanding of the pattern and nature of the losses. Compared to e.g. property covers, where hundreds of years of loss data is in some cases available, the reinsurance market views cyber as a relatively new source of losses. On top of the intellectual and experience development, cyber market is also seeing a collateral-impact derived from 'conventional' development e.g. from the COVID-19 implications for the markets. Risk Consulting Magazine (Issue: 02/2020, p.5) discussed the supply chains affected by COVID-19 but relevant parallels of a globally contributing, hardly modellable and far-from manageable factor can be found.

> *"I don't think we or anybody else really knows what they're doing when writing cyber"*
>
> *– Warren Buffett, 2018*

The key alternatives for an insurer to reinsure its participation into the cyber insurance market are non-proportional and proportional reinsurance. Proportional relates to a model where the reinsurer and insurer share the risks with agreed split (such as for example 50% of each and every loss) from ground up whereas non-proportional refers to a type of reinsurance where the reinsured retains a loss of certain amount and the reinsurer agrees to pay for losses exceeding the amount. The proportional reinsurance has been the dominant instrument in the genesis of the cyber reinsurance marketplace. As the exposure modelling capabilities are still developing, it has been considered fair to share the risk from the ground up.

UNDERSTANDING THE RISKS

Insurers and reinsurers share an interest in better understanding the exposure in order to design products, underwrite the risk transfer and ensure appropriate capital for the portfolio of risks. Combining the knowledge of the reinsurers and insurers benefits the policyholders as pricing becomes more accurate and insurance market solvency is secured in case of a grand cyber catastrophe.

The cyber loss modelling market has developed tremendously over the past years but still lacks consensus (as e.g. CAT modelling has gained) in forecasting, for example, 1-in-200-year losses. Various suppliers are working globally to put together sophisticated views on the market and portfolio loss potentials.

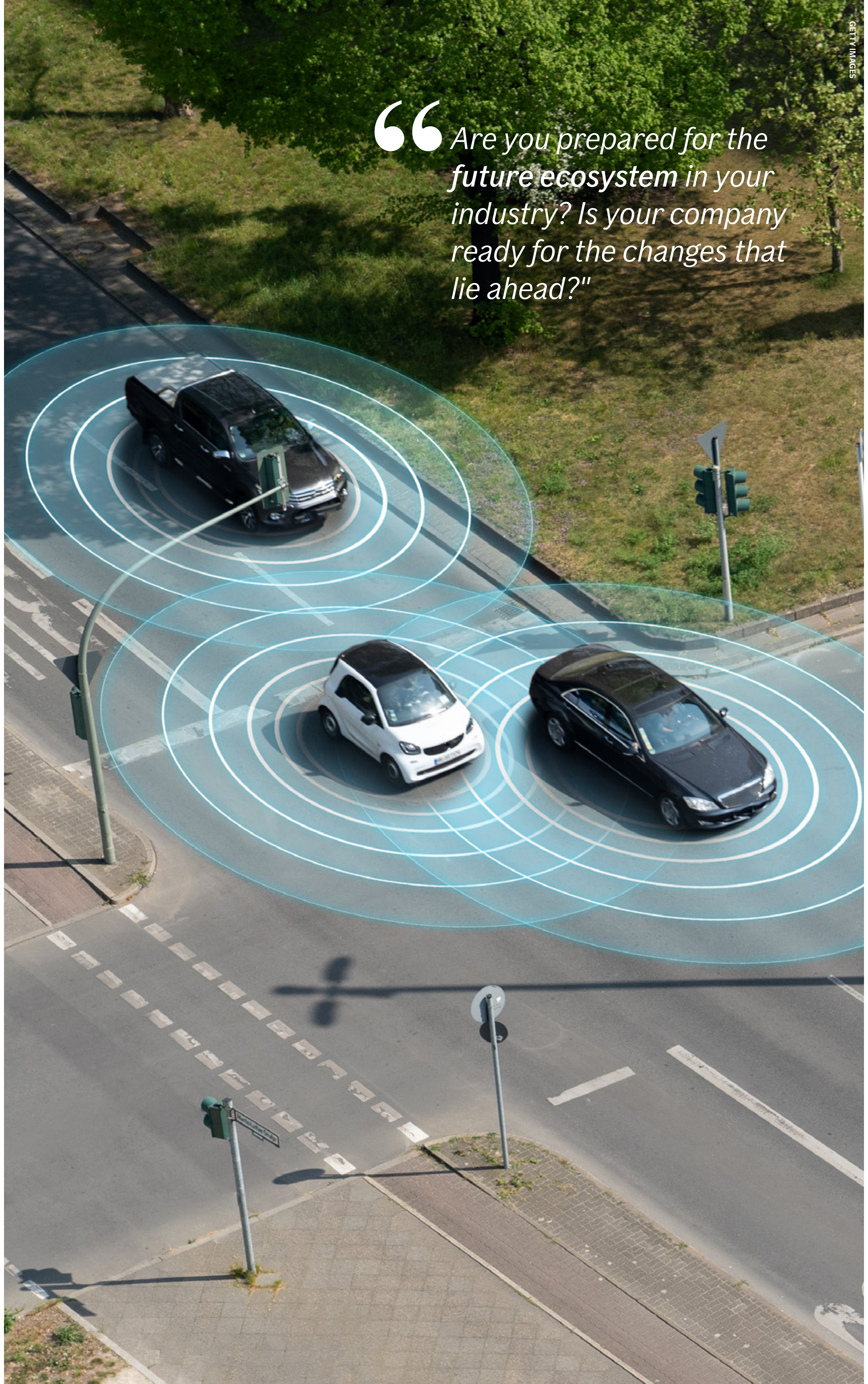
The methodology combines probabilistic and deterministic approaches in order for the insurers to prepare and allocate capital for the losses – whether frequency or severity in nature. Eventually the development radiates into the direct cyber insurance marketplace, by enabling insurers to help their customers by offering increased capacities and services.

Warren Buffet has a very fair concern: caution is needed when dealing with a 'new' exposure and with limited loss history. However, over the past years there have already been significant developments in the amount of reinsurance capacity available in the market. Furthermore, a substantial amount of information and knowledge is available - most importantly on the sophistication of the loss / accumulation modelling - which has helped insurers in preparing and alleviating the cyber risk with better coverage and services, more capacity and more accurate, predictable pricing for the risk. □

Data at the core of mobility

Internet of Things, Big Data & Artificial Intelligence will fuel new partnerships and ecosystems in the Insurance industry

Article by Anders Nilsson



GETTY IMAGES

> “Are you prepared for the ***future ecosystem*** in your industry? Is your company ready for the changes that lie ahead?"

Let's imagine a simplified “mobility ecosystem”, where we have three parties involved. First, we have the customer, who buys the car and uses it to get around. Secondly, we have the original equipment manufacturer (OEM), who builds the car and sells spare parts for it. And finally, we have the insurer, who insures the OEM against product liability risks, and the customer against accidents and theft.

Insurers have historically been sitting on a “treasure trove” of data, based on their superior knowledge of the accidents that happen. They have used it to deduce which factors affect the likelihood for a given customer in a given car to have an accident. Simply put, insurers have been in a unique position to understand, price and help customers manage risks.

However, the recent advances in sensor and processing technology – as well as connectivity – are changing the game in the mobility ecosystem. OEMs can now cheaply build sensors and intelligence into their products, that enable them to understand how their cars perform and how they are being used. This information is utilised to improve the product and create a better experience for the customer. Today, being able to reach your car via your smartphone to switch on your heater and having a smart infotainment system are standard in several brands.

But for the OEM, the value of the connected and intelligent car does not stop there. They get access to unparalleled details of information, not only about accidents that happen, but also close calls and how driver behaviour affects risk. And by extension, OEMs use this information to build active risk prevention measures – often called active safety systems – into their cars where the sensors and intelligence decrease the risk of having an accident altogether.

Simply put, OEMs will be in a unique position to understand how their products are being used, what risks they are exposed to, and even design active risk prevention measures into their products. I would argue that this increased “scope” of the OEMs' role will enable them to become – more broadly – mobility providers, where customers no longer need to take on the risk of owning a car, but can simply use a mobility service to get around to where they want to go. Because really – if you had the choice of using a car “as a service” with a truly predictable cost that covers “everything” – would you still want to buy and own a car?

The risk is, that arguably bad drivers prefer to pay for the service rather than ownership, while good drivers prefer to own their car. This would imply, that clients paying for the car as a service carry higher risks, thus the cost would go up. However, in a data-driven world that does not have to be the case as the data will allow for more accurate pricing to reflect a customer's true risk.

But OEMs and drivers will still be exposed to risk, although it is changing in nature. Systems still fail, accidents still happen, but the factors behind them will change. With all the connectivity and intelligence in modern cars, new risks such as cyber emerge. Collaboration between OEMs and Insurers will need to develop in order to keep pace with the advancements in insights enabled by sensor technology and AI.

Even for OEMs with a truly unique view into their customers' risks, insurers have a relevant role to play beyond being a financial carrier of risk. When the customer is involved in an accident, insurers will remain a key bridge between the parties that need to be involved to help the customer through it. The unique value proposition of the insurer is the knowledge of how to best take care of a customer that has an accident – through the network of medical help, roadside assistance, repair shops, and so on. This “accident care infrastructure” is simply too challenging for each OEM to maintain on their own.

Similar trends can be spotted in other ecosystems as well, where the role of players, including insurers, will change. In the home ecosystem, smart home technology is powering new insight into risks in the home. And in the health ecosystem, smartwatches are enabling new levels of preventive care.

For many companies, when faced with this type of change, it makes sense to consider how well positioned one is to “win” also in the future ecosystem. Is your company ready for the changes ahead? But just as importantly, is your company prepared for the digital risks involved? And are you participating in the change as a driver or as a spectator?

onnect to address 192.168.1.1
sername:
assword:
ccess granted...
ed after 0.006146 seconds with return value
to continue . . .

GETTY IMAGES

Trends in ransomware

Article by Mikko Peltonen

Ransomware is a very powerful weapon, causing a disproportionately high amount of disruption for the financial gain. Year 2017 was the year of ransomware. So was 2018. In 2019, things became much worse. In 2020 we are again reaching all-time highs in ransomware in terms of prevalence but also in business disruption caused. In this article, we look into how ransomware has evolved over the years, and consider the current trends.

Let's go back a couple of years. Ransomware has been around for quite a long time. Already in 2013-2014 there were ransomware strains such as CryptoLocker and Cryptodefence. The first real game changer in this business though was the simple invention of wormable ransomware such as WannaCry. This combined the ransomware payload (the code encrypting the files and requiring ransom in exchange) with a worm that spreads it inside the target organisation. This was an easy and logical step in the evolution; just combining two existing malware types into one powerful weapon.

> *“Criminal gangs target the individual person, a specific employee for example, who has been hand-picked to be the victim in a highly-specialised attack.*

DATA STEALING RANSOMWARE

In 2020, the ransomware business has further evolved, and the criminal gangs have come up with new business models. The rise of the new type of attack that first encrypts, then steals your data have been anticipated in the industry for years, and in 2020 this has unfortunately materialised. Even if you were well enough prepared to recover from an eventual attack with backups, you would still need to pay the criminals “hush money” to prevent them from spreading the data, or face the equally bleak prospect of hefty GDPR fines that could amount to higher costs than the ransom demand. On top of this, there is the bad publicity for your organisation. Talk about being between the rock and a hard place.

There have been real life cases of stolen data leaked by ransomware gangs by e.g. Maze and Ryak ransomware organisations. The Maze network’s modus operandi is that they publish some elementary proof in the form of data that they only can possess by having breached the company network. This can be names or contact details which are then published on their web page, which also applies public pressure for the affected organisation, forcing them to come out publicly that they have been breached.

TARGETED RANSOMWARE

Another trend, alongside of data-stealing ransomware, is the rise in far more targeted ransomware attacks. Instead of a generic attack that works against many organisations (but require a low level of sophistication), the new method is to tailor the attack for the targeted company and then exploit their weaknesses.

This approach is called Human-Operated Ransomware, and it combines the raw processing power of computers and the human brain with knowledge of target, instincts and problem-solving ability.

The rise of human operated ransomware is bad news in many ways.

1. ***Tools:*** *Very sophisticated criminal tools only available for well-equipped criminal gangs such as 'zero day' vulnerabilities may be used in the attacks. Compared with the run-of-the-mill ransomware that preys on those who are not adequately patching and protecting themselves with up to date malware protection, the rate of success for a skilled human attacker with the precision tools to penetrate the chosen organisation is very high.*

2. ***Skills:*** *cybercrime gangs have decade-long experience in data breaches. They know what and where to look for, how to fly under the radar and maintain foothold in the environment for extended periods of time.*

3. ***Time horizon:*** *These gangs are well funded and are not in for a quick cash. They can take all the time they need: weeks, months or years, to gather as much data as they believe it will take for a jackpot.*

CRIMINAL STRATEGY

It is obvious that the gangs have shown a change in strategy in monetising from ransomware. Previously, attackers sent a large number of spam emails to multiple addresses with a generic attack payload. Today, the recipient is hand-picked and carefully targeted, receiving a highly specialised and well-crafted attack, which specifically exploits their weaknesses. This requires higher sophistication, but also unlocks the possibility of tailoring the ransom demand to maximise earning potential and increase the likelihood of payment.

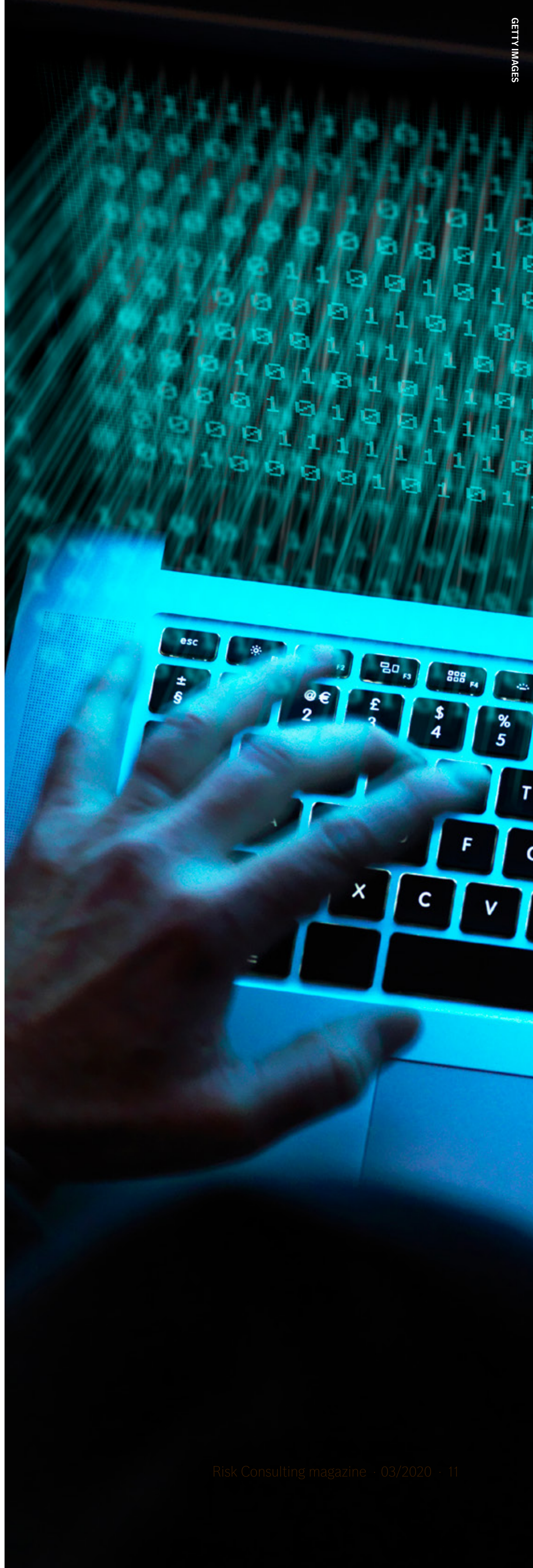
Using an automotive analogy, this is a strategy change from making all-purpose cars that work well enough for most everyday use to building a Formula 1 car that has been optimised for just one narrow set of circumstances, fine-tuned to be really, really good at what it has been designed to do. Or consider a mass-produced fast fashion item that anyone can wear but gets the best out of nobody, to a haute couture piece tailored specifically for the individual client.

In summary, there are two new features with regards to how ransomware gangs are operating, both obviously aiming at maximising their profits:

- *an added earning logic, on top of the lucrative basic concept from demanding ransom to decrypt the files, but now also stealing the data, making it possible to exploit the targeted company twice on a single attack.*
- *changed strategy from mass spreading to targeted attacks and human-operated ransomware, making attacks harder to fend off and adjusting the ransom demand to match the pain threshold of the target organisation, to maximise earning potential.*

This means that if you are the unlucky chosen target of one of these attacks, the chances are very high that the adversary will eventually succeed.

Is there any good news in this? Yes, there is. Most of these threats can still be defeated with elementary means: basic hygiene measures, such as keeping internet facing assets rigorously patched, applying the principle of least privileges everywhere, and deploying a properly configured host firewall to all eligible workstations goes a long way.



GETTY IMAGES

Shopping for Cyber

How to ensure proper coverage?

Building a good level of cyber security is a moving target, and those of us who have been in this industry long enough have come to learn, that the cyber threat is always evolving faster than the countermeasures against them are being developed. In the world of rapid digitalisation, no company is guaranteed to be fully protected against cyber threats. This has led many organisations to seek protection also in the form of cyber insurance.

Article by Mikko Peltonen

Cyber insurance is an unconventional insurance product in the sense that most cyber products today are a combination of first- and third-party coverage, thereby crossing borders of multiple lines of business. It also makes it harder to understand and compare various products on the market. Determining the appropriate cyber insurance coverage might be a tricky task though, and with the plethora of different cyber insurance products available with widely varying covers, terms and conditions, it can become downright daunting. In this article, I will explain some of the considerations every cyber insurance buyer should keep in mind.

IT ALL STARTS WITH YOU!

Understanding your needs is where you always should start. All organisations are different, and what works for one company may not make any sense at all for another. Therefore, you should start by identifying what your crown jewels are: data, applications and processes that are business critical or sensitive, and therefore should be safeguarded. Easier said than done, but without this knowledge, it's impossible to protect yourself.. If you don't even know what assets you have, you can also rest assured you don't know how to protect them!

Once you know what your weak points are, you should look into what the loss of these crown jewels would mean to you.

This understanding is also key input for the insurer. Insurers are much more likely to provide you with a reasonably priced cyber policy, if you can show that your organisation understands their strengths and weaknesses well and is adequately protected.

FIRST-PARTY COVERAGE

The bread and butter of today's cyber policies are Incident Response, Restoration and Business Interruption covers. They would cover containment and mitigation of security incidents, as well as any loss of income caused by malicious and non-malicious cyber events, respectively. Malicious cyber events caused by external entities are colloquially known as cyber attacks. These attacks may use a combination of tools ranging from malware, exploitation of unpatched vulnerabilities in target's systems, to social engineering and phishing. The motive is usually to steal information or extort the target for money.

Of course, the malicious actor is not always an external party. According to some studies, more than 50% of all data breaches (and for instance Insider Threat Report 2019 by Verizon claims a whopping 57%) are carried out by malicious insiders. So, it is good to make sure that your policy would also respond to insider jobs in an expected manner.

The cover purchased should be driven by your needs. Ask yourself which of the cyber event consequences would have the biggest financial impact to your business. For many businesses, business interruption is the main concern therefore make sure you get this cover right.

THIRD-PARTY COVERAGE

Most cyber insurance products also contain one or more third-party covers for claims against your organisation. The most typical ones are Confidentiality Liability, indemnifying losses of confidential or personal information, Network Security Liability, protecting you against claims from third parties for their losses caused by your network or security incidents, and Media Liability, that protects your online activities from liability claims (e.g. defamation, copyright infringements and privacy breach).

Another typical third-party cover is PCI-DSS, which should be considered whenever your business accepts payment card transactions. It will provide indemnification in case of failure to comply with PCI-DSS regulations, re-certification costs and so on.

For many, cyber insurance is seen as the last line of defense against digital risks and cyber crime.

ENVATO

ADD-ON SERVICES

As with most insurance offerings, the main feature of cyber insurance is obviously the financial indemnification in case of a loss. However, when choosing a cyber insurance for your organisation, the value of the add-on services might also be significant. The add-on services range from cybersecurity assessments, security consultancy or discounts from third-party services or products.

Also, the post-claim services, such as the expert help that you can get through the insurer in case something unexpected hits you can't be underestimated. Even if your organisation is well enough resourced to deal with regular day-to-day security incidents, in case of a large-scale cyber incident – be it malicious or non-malicious in nature – may require considerably more resources than you are able to deploy in-house at a very short notice. Most cyber insurance offerings will instantly give the insured access to various expert services ranging from legal help to reputation management consultants, but perhaps most importantly cybersecurity consultants that are experts in cyber incident containment, coordination and attribution. The service providers should be reputable names in your area and have the ability to deliver support when you need them.

You should also pay attention to the deductible applicable to using post-claim services. Some of the best services in the market will give you the first 24/48/72 hours of incident response with zero deductible, lowering the threshold to access these services. As a known fact, 'time is of the essence' in any incident response. Therefore, engaging these services early in the incident can potentially reduce the total impact immensely. □

Summary

KNOW YOURSELF AND YOUR ENEMY

Identify your assets of importance, and the safeguards you have for them in place today. What do you stand to lose if any of these key assets are compromised?

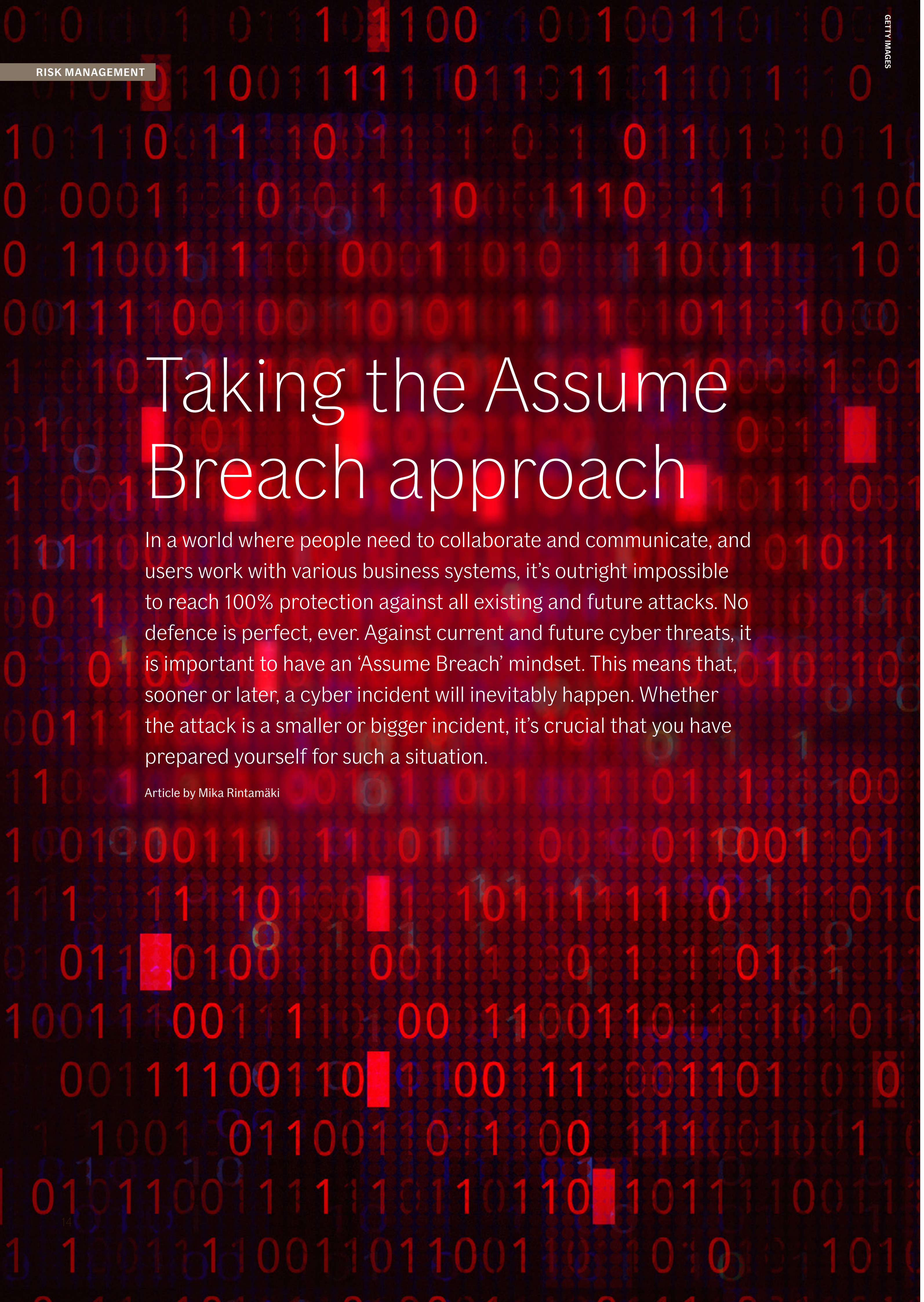
What would be the biggest impact if your organisation was hit by a cyber event? What is the insurance cover that best protects against that?

SHOP FOR INSURANCE TO COVER YOUR NEEDS

Based on the work done above, shop for a policy that has coverage, policy limit and deductible that are most appropriate for your organisation's needs and requirements. It is recommended to work with reputable insurers with proven claims handling, so you get the help you need when a disaster hits . Don't forget the value of pre-claim services, and make sure they actually add value to you. You shouldn't be paying extra for bells and whistles that you don't need.

MONITOR THE PERFORMANCE OF THE INSURANCE AND ADJUST ACCORDINGLY!

As with all service providers, do follow up regularly with your broker or insurer to ensure your insurance policy consistently meets or exceeds your expectations!



GETTY IMAGES

Taking the Assume Breach approach

In a world where people need to collaborate and communicate, and users work with various business systems, it's outright impossible to reach 100% protection against all existing and future attacks. No defence is perfect, ever. Against current and future cyber threats, it is important to have an 'Assume Breach' mindset. This means that, sooner or later, a cyber incident will inevitably happen. Whether the attack is a smaller or bigger incident, it's crucial that you have prepared yourself for such a situation.

Article by Mika Rintamäki

The traditional approach has been for companies to focus mainly on preventive controls. Here, efforts are focused on for example network security, firewalls and anti-virus solutions, which seek to prevent the attacker from breaking into your systems. Today, preventative security controls are not enough.

By taking the 'Assume Breach' approach, companies will have both the technical capabilities and softer process capabilities in place. On the technical side, we refer to Detect and Response security capabilities. In these cases, the objective should be to detect a cyber attack on the company environment as quickly as possible.

> “Assume Breach” is for those who look at cyber security holistically and are preparing for all cyber risk scenarios

During an attack, time is of the essence. Through early detection, companies can better mitigate the impacts of an incident. Having a playbook ready, or as ready as possible, will help your company survive an attack. In the playbook, you should have clear procedures on what actions need to be taken, how these will be completed, and by whom. The focus should be on restricting or isolating the damage as early as possible.

YOU HAVE BEEN BREACHED

To succeed you need to have very good visibility on the endpoint level as well as on network level. This helps security teams successfully manage:

- *network traffic (e.g. traffic logs, NetFlow, full packet captures)*
- *endpoint usage statistics, such as process trees network traffic, memory contents etc.*

Automation and predefined rules can help you detect indicators of compromise, also more modern artificial intelligence or machine learning solutions can be used to detect behaviour-based alerts. This is especially needed when the attacker is not directly utilising previously known methods. In fact, skilled attackers are able to carefully cover their tracks, and do not need to apply much brute force. This helps them avoid detection, for example by increased traffic volumes.

Use a structured approach to perform what is commonly known as 'Red Team' testing. Essentially, working with a trusted partner, preferably a skilled and trusted security company, to attempt to break into your environment. This will help you test your security controls and uncover any issues or shortcomings in your protection systems.

From a risk management perspective, cyber risk scenarios need to be included in both Disaster Recovery planning as well as in other company crisis exercises. Once you have completed a major cyber incident crisis exercise, you are better prepared for such an attack if it were to occur in reality.

It is worth noting that larger cyber incidents often happen by surprise and are executed in a way that you were not expecting. The truth is that you cannot train for every possible scenario, however a good practice is to prepare for various situations, practicing how to handle these, and testing for attacks regularly. This will increase confidence in your system for when an actual cyber incident happens.

In closing, it is important to note that the “Prevent Breach” mindset remains vital, as this is most definitely still needed. Companies must have good preventive security controls in place, e.g. security patching, malware protection and firewalling. These are fundamental requirements that have not gone away, they are still mandatory.

By applying both of these approaches, companies can increase their preparedness for a cyber attack and capabilities to reduce the impacts of an incident when it occurs.

Note that it is an essential and valuable practice to regularly test and verify that your existing prevention systems are in working order. This will help to evaluate how detection and response is working in practice, if you were attacked today.

GETTY IMAGES

The threat from within

Today, the threat from within a company is far more complex and difficult to deal with. When it comes to addressing traditional fraud, such as investigating the misuse of corporate funds, companies are often well-prepared and alert to various scenarios. However, these processes are being challenged by cyber attacks that are increasingly problematic to detect, expensive to investigate and challenging to prosecute.

Article by Preben Danielsen

Employees today work very differently to those just 15 years ago. At the core of this, lies data and information which is increasingly valuable to criminals. As cyber attacks are increasingly commonplace, companies must have reliable and trustworthy employees, who are both diligent in their work and savvy to potential cyber threats, such as email phishing. Employers also need to be constantly developing the skills of their employees in order to keep up with the latest threats.

INSIDERS ENABLE ATTACKS

Insiders are defined as current and former employees, contractors, business partners or others who have access to confidential information regarding an organisation's IT systems or security practices. However, not all insiders are malevolent. In fact, according to some statistics mistakes and misuse cause more harm than a disgruntled employee. Negligent or ignorant behaviour can lead to errors and misuse. This can include incompetence, such as misconfiguring servers to allow for unwanted access or publishing data to the wrong server or online.

According to an Observe IT[*] study , "organisations are spending 60% more on dealing with all types of insider threats than just 3 years ago and 25% more since 2018." These investments are made into detecting and investigating insider threats, with costs in these areas "increasing by 86% in only 3 years."

This is not just an IT issue, every area in the organisation is at risk. Insiders can be in almost any department, from sales teams for example, offering to sell confidential information about new products to competitors.

The employee´s ethical compass should be based upon the values of the organisation. This is about trust, and perhaps more importantly companies need to be attentive - there may be plenty of policies, guidelines and rules in place, but if an employee's ethical compass is not intact, these will be of little value.

Importantly, society and commercial organisations absolutely cannot afford to be naïve. We must maintain a high level of trust, but at the same time secure and implement good and well-functioning control measures.

From the factory floor or the mail room to the executive offices, all employees pose a potential risk for fraud. Consider which employees have access to critical IT infrastructure or are aware of details relating to the company IT security systems and practices. It is common for employees working in certain roles and with specific responsibilities to have access to such information on a daily basis.

THE AGE OF DIGITAL ESPIONAGE

Corporate espionage not only still exists, it is becoming increasingly sophisticated, with some attacks being state-sponsored. Over the years, there have been cases involving third parties that facilitate and fund individuals to apply to work in a targeted company with the sole purpose to work as an insider.

Expert criminals posing as interns or contractors can quickly learn for example what IT systems are in place, how these are protected, and locate possible vulnerabilities in the IT infrastructure. This form of espionage requires exceptional alertness from the targeted company's employees to ensure that such persons are not recruited into the organisation or selected as service providers or partners of the targeted company.

On the darker corners of the internet, current and former employees can also be found selling information or offering to provide access to their employer's IT network. This criminal activity makes hacking into a company extremely easy for organised criminal groups.

As technology continues to move the boundaries of what is possible, it can be difficult for companies to keep up. Artificial intelligence and machine learning are just a few examples of emerging technologies that can also become valuable tools for cybercriminals.

WHY TRUST MATTERS

By default, employees are expected to behave in a way that protects the company and secures its operations. Partners and stakeholders are likewise entrusted to be working with good intentions, in support of the targets and purpose set by the organisations they serve. However, organisations must have processes and practices in place to secure their operations thoroughly.

One such practice is the principle of segregation of duties, which is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department. Without this separation in key processes, fraud and error risks are far less manageable.

Alongside regular audits which help to safeguard their operations, products and services, as well as their business, companies need to implement and use fraud detection tools effectively to protect themselves.

Organisations can reduce their exposure to risks by being vigilant about the people they hire and the company's they engage with– even when these risks are becoming more difficult to recognise and mitigate.

A certain degree of awareness combined with due diligence and implementation of well-functioning control and security routines should help to reduce the risk of insiders harming organisations. This includes limiting the level of access and permissions for employees. It is also important to train your staff on a practical level, e.g. to spot phishing attempts in their Inbox. Perhaps most importantly, organisations must clearly communicate their set of values and highlight the importance of everyone taking responsibility for protecting the company's assets, even if the threat comes from a colleague.

[*] *Source: Observe IT, https://www.observeit.com/cost-of-insider-threats/*

IMAGES COURTESY OF DANISH CROWN

Securing production at Danish Crown

Article by Kristian Orispää

By conducting a risk assessment, you can detect existing problems, locate potential issues and review existing controls. When it comes to assessing IT risk, conducting a factory risk assessment will help you understand what improvements need to be made to bring IT systems up to standard.

When preparing for digital risks and cyber attacks, it is vital to understand that the factories you work with or are leasing, or plan to purchase, must meet security requirements as well as maintain quality and reliability of production. For companies working in the food industry, this is highly important for survival.

UNDERSTANDING THE RISKS

Danish Crown Group, a food processing company and the leading meat processing producer in Europe, has experienced an increase in malware attacks and other security related incidents. Like most of the companies in the food and beverage industry, the company places IT Security high on the corporate agenda.

As **Lars Sleimann**, Senior Manager, Factory Solutions with Global IT at Danish Crown explains, “It is important to minimise the risks on our IT infrastructure in administration and production. Today, cyber criminals are chasing big corporations. Cyber crime is no longer just geeks causing trouble from their bedrooms, this has become a professional 600 billion USD business, with service centres and hackers for hire.”

To mitigate cyber attacks on its operations, Global IT at Danish Crown has a high focus on protecting its business. Lars Sleimann explains that, “In an enterprise context, hackers are chasing a company’s core values, its intellectual property, production control systems or client data, basically the type of information that will increase the likelihood of a ransom payment, when the alternative is to no longer be in business.”

BUILDING A SAFETY NET

At Danish Crown the IT security consists of two areas. First, technology measurements, which is dedicated to the protection of users, software and hardware. Second, the behaviour and awareness of employees and the efforts to increase IT security awareness.

“There are many basic requirements to creating a safe IT landscape, or at least an environment that is as safe as possible. Using MFA (Multi-factor Authentification), complex passwords to protect identity, for example, and managing permissions and access to systems based on needs only. Just as importantly, employees need to be aware of digital risks and exercise caution. You also need to focus on employee behaviour, to use common sense, so they apply simple rules. One example would be to avoid using the same password across multiple apps and services.”

UP TO CODE

Factory IT assessment places a high focus on stable and secure production environment with high availability. Evaluating the server rooms, the server platform, VLAN segmentation for production and administrators – all of which must be secured and stable. Similarly, the disaster recovery plan and industrial security are integral parts of factory IT. By conducting an IT assessment, you can ensure that the required standards and best practices for production and automation IT are in place at each production facility.

To measure the level of IT security, Global IT at Danish Crown utilises the same standards as similar companies, specifically ISO 27002:2013 (IT Security) and IEC 62443 (Industrial Security).

All new factories in Danish Crown Group are measured as one of the first IT initiatives, to establish informed decision making. Meanwhile all factories are regularly measured to ensure progress in the agreed activities, monitor progress and make sure targets are met.

In the first phase, data is collected and analysed on the existing systems. An onsite assessment is completed of the physical and environmental security incl. production or server room, for example. Next, a Service Level Agreement is evaluated to ensure that all IT systems meet the business requirements for availability. Finally, an IT Security Assessment is completed to review relevant controls regarding IT/OT Security based on ISO27002, CIS20 and IEC62443.

Findings, conclusions and recommendations for improvement and, if any, future CAPEX investments are then collected and evaluated in Phase 2. In this stage, the average score from the IT Security Assessment for all factories will be summarised for benchmarking and reporting.

IMAGES COURTESY OF DANISH CROWN

In the final stage of the Factory IT assessment, the report is presented to the factory and relevant stakeholders. Here, all IT Service Management approved activities will be registered and assigned. A Site Level Agreement between the factory and the Global IT Factory Solutions team for the services provided is also presented. The working relationship and areas of responsibility are defined and agreed upon in the Operational Level Agreement and any approved CAPEX investment will be applied for through due process. Finally, follow-up procedures are agreed upon to ensure successful implementation of the findings and conclusions of the assessment.

IT must have a place at the board room level.

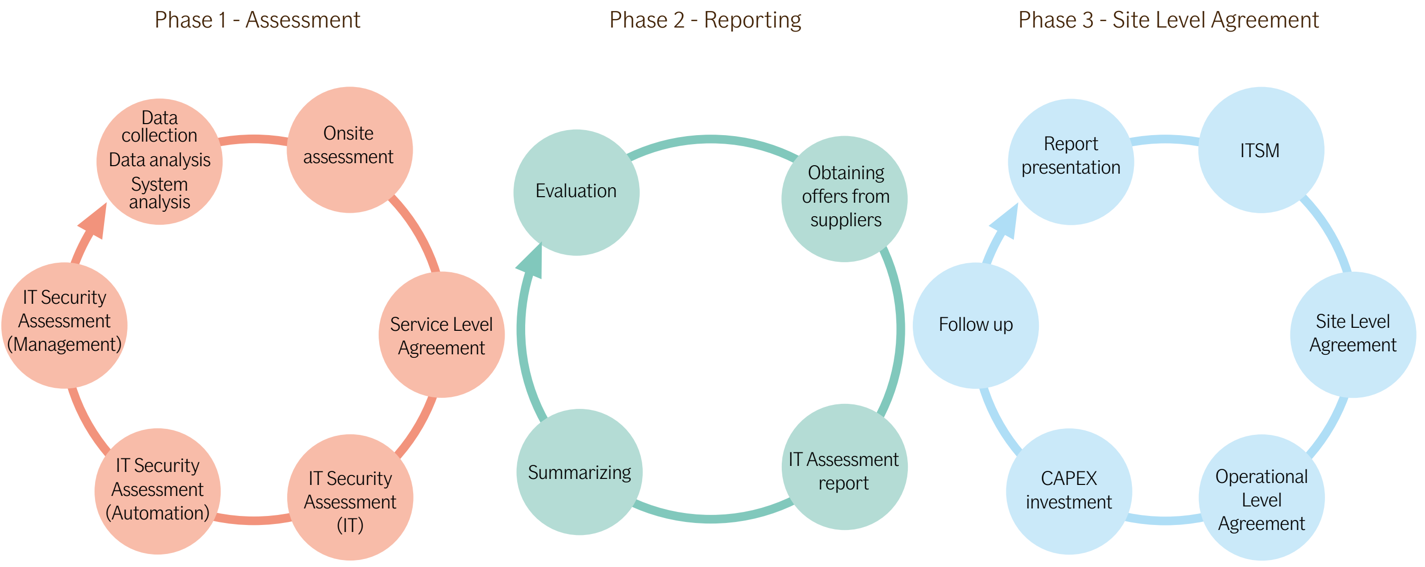
GETTING TO THE NEXT LEVEL

At Danish Crown, the processes are constantly evolving. As Lars Sleimann concludes, “From the technology perspective we need to be on top of our game, standard systems, with a high level of IT security, to ensure business continuity. Also, as in any company, IT must have a place at the board room level. This helps to ensure funding is in place as well as streamline decision-making for business-critical IT. Awareness is also key, employees need training and tools in order to understand and help protect the business from the risks involved during their daily work. In many ways these components are on the next level, as we must also focus on people and the business itself, not just hardware, to mitigate digital risks and cyber threats.” □

IMAGES COURTESY OF DANISH CROWN

Factory IT Assessment

Protect our Business



Phase 1 - Assessment

Data collection
Data analysis
System analysis

Onsite assessment

Service Level Agreement

IT Security Assessment (IT)

IT Security Assessment (Automation)

IT Security Assessment (Management)

Phase 2 - Reporting

Evaluation

Obtaining offers from suppliers

IT Assessment report

Summarizing

Phase 3 - Site Level Agreement

Report presentation

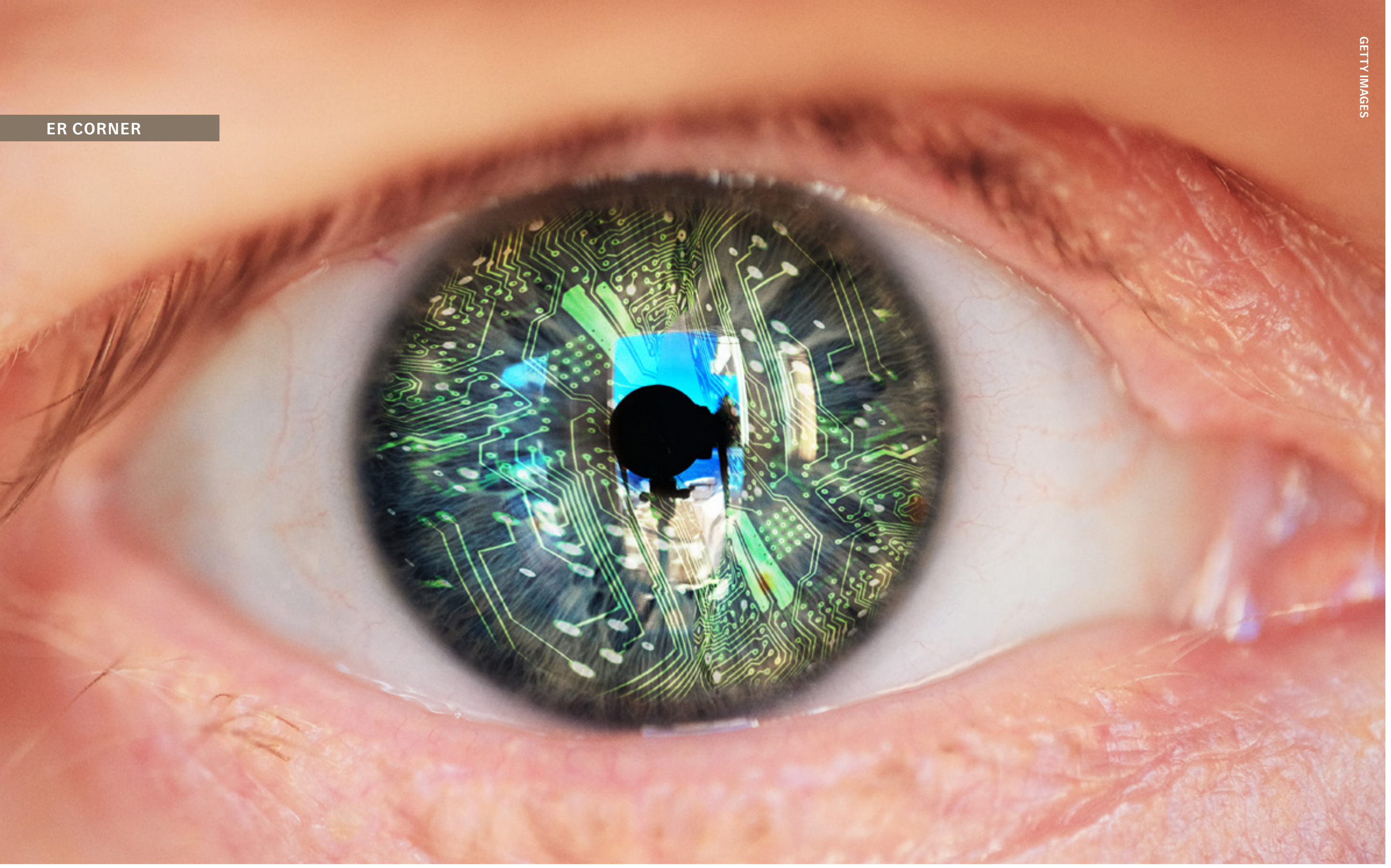
ITSM

Site Level Agreement

Operational Level Agreement

CAPEX investment

Follow up



GETTY IMAGES

The promise of 5G

In 2013 European Union declared its 5G Infrastructure PPP – the Public-Private Partnership to secure Europe's leadership in the areas where there is a potential for creating new markets such as smart cities, e-health, intelligent transport, education or entertainment & media. Indeed, the newest mobile technology standard 5G has plenty of promises in the core of the 4th industrial revolution.

Article by Matti Sjögren

The increased bandwidth will enable - besides smooth videos through smart phones also fully autonomous traffic systems and obtaining and analysing big data. The technology is going to connect more devices in Internet-of-Things with low latency thus releasing the full potential of IoT and increasing efficiency and reducing costs on every level.

The infrastructure has started to materialise since 2019 and there are 5G networks already in major cities in dozens of countries with millions of subscribers. What are the risks considering the key nature of 5G having an impact everywhere in the digitalised world? First comes to mind the possible direct risks of the technology. 5G operates in the same wavelengths like 3,5 GHz as partly also 2G, 3G or 4G, but significantly higher, radio frequencies (RF, 24 GHz) are going to be used later. This means that there have to be very dense network of base stations within just few hundreds of meters from each other.

There have been tens of thousands of studies on the health effects of electromagnetic fields (EMF) during the last 30 years with very few showing any adverse health impacts. However, there are precaution measures instructed by the authorities, e.g. to minimise the use of mobile phones by children. But the 5G will also operate in new radio frequency lengths not so well researched. The Swedish Radiation Safety Authority's (SSM) Scientific Council states in their report [*] published in April 2020 , that "even though there is no established mechanism for affecting health from weak radio wave exposure there is a need for more research covering the novel frequency domains used for 5G".

With IoT connecting billions of devices and handling large amount of data the cyber risks and personal data related risks will increase. 5G enables sophisticated interactive systems from financial transactions to industrial processes and vital communications. New security methods need to be created.

In 2013, the EU was expecting also desirable societal changes would be made possible by the new technology. But with people involved there can always be other changes too. When complicated technology, that is difficult to understand, is being developed, humans tend to be cautious and distrustful. This year there have been plenty of physical attacks by people against 5G support stations e.g. in UK and the Netherlands. There are even allegations in the web that the networks contribute to the spread of coronavirus. Another aspect of this is often linked to the sudden wave of making general liability or product liability claims especially in the USA against some new technology or product.

But as said, the 5G radiation is somewhat different from previous technologies. The Radiation and Nuclear Safety Authority in Finland says that "there is also no reason to suspect, on the basis of current knowledge, that the millimetre waves to be implemented later would have harmful health effects in exposure under the limit values."

Last year the meteorological agencies in the USA were warning that the massive increase in the use of radio frequencies would possibly deteriorate the accuracy of weather forecasts.

The 5G technology related fears have spread, from conspiracy theories to concerns over national security, to accusations of espionage against the Chinese network system producer Huawei, for example.

[*] *Recent Research on EMF and Health Risk - Fourteenth report from SSM's Scientific Council on Electromagnetic Fields, 2019*

Cyber appointments

Johan Hedenstedt,
Nordic Cyber Underwriter

Glossary

IoT	*Internet of Things*
AI	*Artificial Intelligence*
Ransomware payload	*The code encrypting the files and requiring ransom in exchange*
Zero day vulnerability	*A vulnerability in software that is previously unknown to the vendor, and therefore no patch or fix for it is available yet.*
A zero-day exploit	*Malicious code making use of a zero day vulnerability*
PCI-DSS	*Payment Card Industry Data Security Standard, a standard governing the cybersecurity of the card payment solutions globally*
MFA	*Multi-Factor Authentication – a method of authentication requiring at least two "factors" to authenticate. In most common enterprise deployment, password is the first factor, complemented by an Authenticator application as the second factor.*
DoS, DDoS	*Attack that floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Modern attacks are typically distributed (DDoS), meaning it originates from a large amount of computers, e.g. a Botnet.*
Botnet	*A collection of hijacked computers remotely controlled by a cybercriminal to perform tasks such as email spamming or DDoS attacks*

Don’t miss the next issue

Subscribe at www.if-insurance.com

Risk Consulting is If’s professional magazine on risk management and loss
prevention, and is one of the oldest client magazines in the Nordic countries.