WHITEPAPER

PREVENT. PROTECT. INSURE.

HOW GOOD CYBERSECURITY POSTURE, COMPLEMENTED BY CYBER RISK INSURANCE IMPROVES A COMPANY'S CHANCE OF SURVIVAL

PREFACE.

SPREADING FINANCIAL RISK FROM ONE TO MANY IS NOT NEW, IT'S A METHOD FOR THE ONE TAKING THE RISK TO ENSURE SURVIVAL IF THEY ENCOUNTER AN INCIDENT. ACCORDING TO THE 'HISTORY OF INSURANCE' ON WIKIPEDIA THERE ARE EXAMPLES THAT DATE BACK THOUSANDS OF YEARS, BUT MODERN INSURANCE, AS WE UNDERSTAND IT TODAY, DATES BACK 350 YEARS.

Source: Lloyd's of London

Today's focus has evolved to include risks to the digital realm, specifically risks to information and data. Here, the risk of a cyber incident rendering a company financially inviable has created an opportunity for insurers to spread this risk by offering Cyber Risk Insurance. The cyber attack on Change Healthcare is an example of the huge cost that a cyber incident can inflict on a company. In February 2024, the company suffered a ransomware attack, despite paying an alleged US$22 million to the attacker. The company's owner, UnitedHealth Group, reported the incident will cost the business nearly US$900 million initially, with a final estimate to be between US$1.3-1.6 billon.

The reason for these huge figures is simple, cybercrime is the go-to crime for the 21st century and is incredibly attractive for several reasons. The principle reason is the unlimited value proposition stemming from the scale of the data economy and the profits that can be made from cybercrime. A useful parallel can be drawn with the 20th century crime of armed-bank robbery, which in the UK at the time of the beginnings of cybercrime, around the late 1990s, would net those taking part an average of £20-30,000. However, more audacious bank robbers, such as those involved in the Brink's-Mat robbery, could net millions, in their case £26 million in 1986. The risk of getting caught was above 80% and the subsequent jail sentences awarded up to 25 years. The parallels that can be drawn here are that small cybercrime amounts for the likes of fraudulent transactions, through to ransomware payments such as Change Healthcare handing over US$22 million.

UNITEDHEALTH GROUP
(Change Healthcare Cyber Incident)

$595m

- CLEARINGHOUSE PLATFORM RESTORATION
- RESPONSE EFFORTS
- MEDICAL EXPENSES DIRECTLY RELATING TO THE TEMPORARY SUSPENSION OF SOME CARE MANAGEMENT ACTIVITIES

$280m

- BUSINESS DISRUPTION
- LOSS OF REVENUE

$1.35-$1.6bn

- EXPECTED FINAL COSTS

Due to the nature of cybercrime and the complexities of attribution as to who the perpetrators actually are, the risk of being arrested and jailed is much smaller, likely a reversal of the risk posed to the physical robberies conducted by bank robbers.

Another similarity is the stance on handing over the cash. Banks instructed tellers to comply with the robbers extorting money from the branch. In the Coalition 2024 Cyber Claims Report it states: **'Among policyholders that experienced a ransomware incident, 40% opted to pay a ransom, deeming it reasonable and necessary.'**

With an average cyber incident costing approximately US$4.5 million, according to the IBM Cost of a Data Breach 2023 Report, then it's not surprising that insurers have stepped in to spread the risk just as in the maritime industry in the 13th century.

As the industry matures and the relationship between cybersecurity and cyber risk becomes quantifiable through claim data and incident forensics, the requirements on the insured are being increased to lower risk. Companies looking to protect their business from a financial catastrophe caused by a cyber incident may find themselves having to provide considerable information on their cybersecurity posture, and then needing to modify this posture to become insurable.

There is one certainty: cyber risk insurance is here to stay, and according to a leading source in a top insurance house, the value of the industry has jumped from US$7.2 billion in 2020 to US$13.8 billion in 2024. The figure the insurance giant, Zurich expects to reach, is US$33.3 billion by 2027.

This whitepaper, hopefully, provides a useful background for any company or organisation that is exploring cyber risk insurance.

Author: Tony Anscombe - ESET

CONTENTS.

PREVENT.
PROTECT.
INSURE.

THE THREAT AND RISK COMPANIES ARE FACING FROM CYBERCRIME/ HACKERS.


PREVENT.
PROTECT.
INSURE.
01

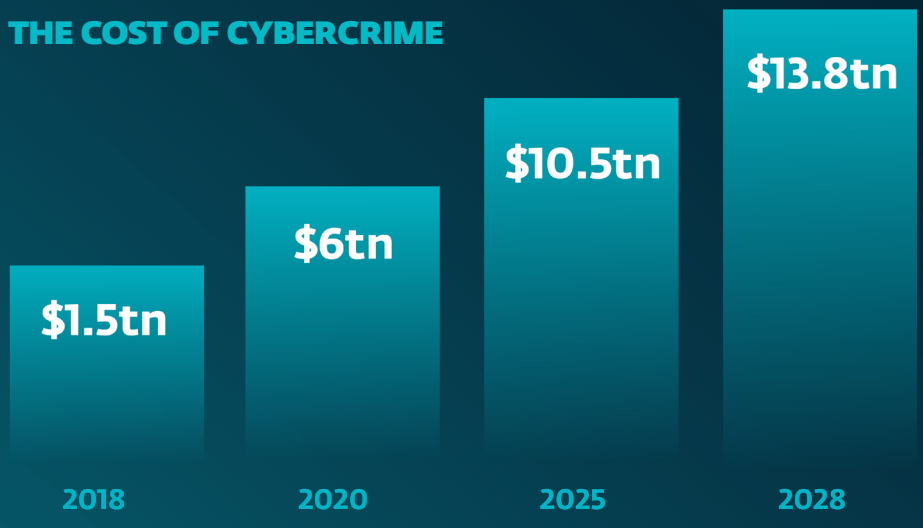
THE EVER-INCREASING CYBERSECURITY THREAT

From communications and financial transactions to information-seeking and recreation, human society is ever more reliant on digital interconnectivity and data access. Along with the speed and convenience of online interactions has come the relentless rise of cybercrime, digital fraud, and privacy rights abuse.

The more interconnected and digitised we develop, the more vulnerable we become to cybersecurity incidents of all kinds, and the greater their potential impacts on individuals, businesses, governments, and even the environment.

Not only do vendors inadvertently create new vulnerabilities for hackers to exploit, but also attackers' techniques are more sophisticated, collaborative, and destructive. According to Statista research, the global cost of cybercrime is predicted to escalate from US$9.22 trillion in 2024 to US$13.82 trillion in 2028, a 67% jump.

THE COST OF CYBERCRIME



Source: Dr Michael McGuire, World Economic Forum; CyberVentures; Statista

In the minds of business leaders globally, cybercrime represents the biggest threat to organisations. Data breaches, ransomware attacks, and other common cyber incidents are a CEO's worst nightmare, capable of halting operations, decimating brand reputation, imposing onerous expenses, and putting business continuity at grave and ongoing risk.


PREVENT.
PROTECT.
INSURE.

INCREASED COST OF DOING BUSINESS.

Effective cybersecurity requires investments in technology, expertise, monitoring, governance, insurance premiums, risk management, legal support, and more.

OPERATIONAL DISRUPTION.

Downtime leading to lost productivity and revenue can be one of the worst impacts following a cybersecurity incident.

REPUTATIONAL DAMAGE.

Sensational data breaches can harm a brand's image long after the news has cooled. Not just customers but also partners, investors, and other stakeholders may shift allegiance to a competitor they perceive as more trustworthy.

THE CYBER THREATS ORGANISATIONS FACE

As the cybercrime industry ups its game with generative AI, machine learning, and other advanced tools to automate attacks and avoid detection, any connected organisation faces a direct threat. Failure to protect valuable or sensitive data can lead to negative outcomes.

LOWER STOCK PRICE.

As a knock-on to reputational damage, publicly traded companies often see a short-term loss of market value or even a stock price crash after disclosing a data breach. The sensitivity of the data involved, plus the company's perceived transparency around disclosing the breach, can significantly influence stock price fluctuations.

REVENUE LOSSES.

Businesses often see a drop in revenue following a cybersecurity incident as customers and prospects turn elsewhere to avoid cyber risk to their data or the business relationship.

CONSTRAINED BUSINESS MODEL.

Cybersecurity risks and costs may force an organisation to make changes in what data they store and/or handle, what products and/or services they offer online, how they use cloud services, how they relate to vendors, and more.

LOSS OR INFRINGED INTELLECTUAL PROPERTY.

A company's IP is probably its most valuable data. Theft or exfiltration of research data, new product designs, business strategy, or customer lists can wipe out a firm's competitive foundation or even threaten national security.

55%

OF CYBER INCIDENTS ARE DUE TO EMPLOYEE NEGLIGENCE

19%

OF ALL REPORTED CLAIMS ARE RANSOMWARE

Despite the prevailing view that nearly all data breaches are malicious, Ponemon Institute's latest global research shows that 55% of cyber incidents are due to employee negligence, with no intent to cause harm. The staggering average annual cost to contain these incidents was US$7.2 million in 2023 (Reference: Ponemon Insider Risks Global Report 2023), about ten times the average cost to remediate malicious insider attacks.

Non-malicious cyber threats stem from the accidental, unintentional, or careless exposure of a company's data or IT assets, with associated harmful results. These risks can manifest through everyday mishaps, for example:

- Emailing sensitive data to an unauthorised recipient
- Disposing a sensitive document improperly
- Clicking a link in a phishing email

These threats can also manifest through negligence or ignoring policy, such as reusing passwords, failing to update device software, or putting sensitive data on a flash drive and then misplacing it.

Human factors are one of the most common entry points to a computer system by an attacker. Cyber attack reports repeatedly state that 'phishing,' the sending of fake emails to an individual containing links that they are deceived into clicking on, is a serious issue. The links take the user to fraudulent websites that either download malicious software onto the company systems or divert them to a website developed to facilitate fraudulent payments from a company by siphoning off funds; an activity that may be spurred by something innocuous such as creating or sending an invoice.

Ransomware may attract most of the headlines due to its high-profile cases including the BBC, British Airways and the UK Election Commission, but email compromise is actually the threat that accounts for a higher level of insurance claims.

"RANSOMWARE WAS THE LARGEST DRIVER OF THE INCREASE IN CLAIMS FREQUENCY, ACCOUNTING FOR 19% OF ALL REPORTED CLAIMS. CLAIMS RELATED TO FUNDS TRANSFER FRAUD (FTF) REMAINED STEADY AT 28% WHILE BUSINESS EMAIL COMPROMISE (BEC) DECREASED TO 28%," according to Coalition's 2024 Cyber Claims Report.

While many phishing emails are sent out as part of mass mailings that aim to hook the unwary, others are specifically targeted at certain individuals within a company because of the position that they hold, commonly known as spear phishing.

Cybersecurity analysts expect the advent of AI to increase the number of spear phishing attacks. With social media providing information about workplaces, roles, friends and interests, AI systems can cull this information to create tailored and even more convincing emails to individuals in valuable job roles that hackers may exploit.

Companies currently attempt to reduce the risk of phishing and spear phishing attacks on employees using education and awareness programs - a process that will become even more challenging with the arrival of AI targeted email.

THE CYBER THREATS COMPANIES FACE

NATION STATE PARTICIPATION

The threat from cybercrime globally is huge and growing. In 2018, the Centre for Strategic and International Studies estimated that cybercrime cost the world almost US$600 billion at that time - equivalent to 0.7% of global GDP or 14% of the value of the global internet economy.

The exact cost of cybercrime is not known for the simple reason that it is not accurately reported, leaving observers to arrive at estimates that vary between US$8 trillion from Cybersecurity Ventures and US$11 trillion from Statista.

In parallel, the opportunity has arisen to transform espionage from a physical activity, to a digital one. Nation states have created highly sophisticated capabilities that are used for spying, attacking and disrupting their enemies. The cyber tools created and used by nation states often find a migration path and are ultimately used by cybercriminals too. Examples of this can be seen on both sides, west to east, EternalBlue – an exploit attributed to the U.S. National Security Agency, and Petya, allegedly the work of Russian intelligence agencies. This becomes more confused when NotPetya, a variant of Petya, uses EternalBlue as the method of exploitation.

Due to the sophistication and capability of nation state hackers, insurance underwriters decided in 2022 to exclude nation state attributed attacks from policies. With the complexities of attribution, this is likely to be a discussion in insurance court cases against insurers for many years.

CYBERCRIME TARGETS ALL COMPANIES - REGARDLESS OF SIZE

In the Suffolk village of Debenham, the local secondary school was taken offline for three months due to a ransomware attack. Some months later, a local Debenham based hairdresser lost her online candle making business due to the same reasons - in her case the attackers were only seeking a ransom of £200.

This incident shows that the lack in understanding of digital risk is not just apparent in businesses but also lies across the board in society.

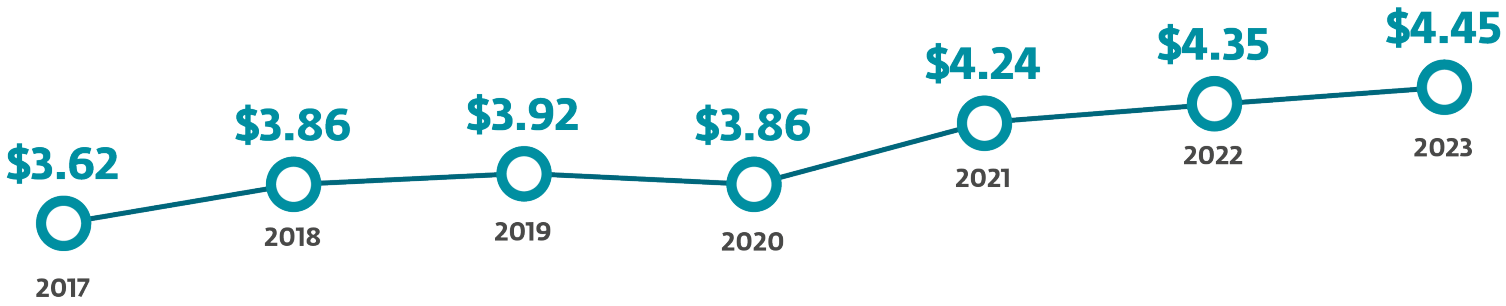
"SMALLER COMPANIES HAVE SIMPLY NOT ACCEPTED THAT THEY HAVE A DIGITAL BUSINESS MODEL AND I FULLY UNDERSTAND. BUT IF I GO TO MY HAIRDRESSER, IF I GO TO MY DENTIST OR TO A LAWYER, THEY WOULD ALL CLAIM THEY SIMPLY USE TECHNOLOGY THAT USES UPGRADED OFFICE EQUIPMENT, BUT THEY ARE SO DEPENDENT ON IT."

Source: Anonymous leading insurer

Sparda Bank in Germany has recognised this weakness and now requires all new account holders to take out cyber insurance and agrees to pay their premiums for the first year.

This move should theoretically provide the bank with both protection and data on the cyber attacks including, phishing and fraud that are targeting their customers, partnering businesses and individuals; the same attacks which are likely to increase due to the availability of AI.

TOTAL COST OF A DATA BREACH



THE COST OF A DATA BREACH

According to IBM, the average worldwide cross-sector costs of a data breach was US$ 4.45 million in 2023, a 15% increase from 2020. Other longer-term impacts are also increasing, such as the US$7.8 billion cost from downtime losses for the healthcare industry in 2021 alone.

Of those breaches, the main culprit was ransomware, according to IBM, causing nearly one-quarter of attacks. Destructive attacks that left systems inoperable accounted for one out of every four attacks, and another 24% involved ransomware. Software and business partner chain attacks accounted for 12% and 15% of attacks, respectively.

At the same time, ransomware attack costs increased. At US$5.13 million, the average cost of a ransomware attack in the 2023 IBM Report increased by 13% from the average cost of US$4.54 million in 2022. At US$5.24 million, the average cost of a destructive attack in 2023 also increased 2.3% from US$5.12 million in 2022.

A concern reflected by Keith M. Martin, the Professor of Information Security, Department of Information Security at Royal Hollow, University of London:

"IF WE'RE GOING TO MAP BACK 10 YEARS, I THINK I COULD PROBABLY BE PRETTY CONFIDENT ABOUT WHERE MY DATA IS, WHAT IT'S USED FOR, AND WHAT MY CONTROLS ARE. IF YOU HAD A DATA BREACH, YOU KNEW WHAT WAS OUTSIDE, AND HOW IT MIGHT BE USED. BUT NOW OF COURSE, THE CHANCE THAT YOU KNOW THAT IS NOT THERE."

Source: IBM.

TRUE COSTS OF A CYBER INCIDENT

Worrying figures, but by no means the whole picture, as the statistics listed by IBM are the costs of recovery, not of the ransom itself, which according to analysts adds up to only about 15% of the total cost of a ransomware attack. It should also be noted that only one in seven organisations that pay a ransom actually get their data back. The targeted organisation will also incur higher insurance premiums, perhaps a reflection of the fact that around 80% of businesses that suffer an attack state that they are threatened a second time.

The main costs from a ransomware attack result from downtime and recovery. It takes an average of 221 days to get a business back up and running after a ransomware attack. Often the cost of downtime can be 50 times greater than the ransom demand as the entire business focuses on recovering the data and restoring operations whilst dealing with crisis communications.

When a cyber incident like a ransomware attack or data breach compromises sensitive documents, the damage extends beyond the ransom amount or the exposed records. Ongoing costs include incident response costs, legal fees and settlements, as well as any regulatory sanctions, as detailed in the NetDiligence 2023 Cyber Claims Study.

80%

OF BUSINESSES THAT SUFFER AN ATTACK STATE THAT THEY ARE THREATENED A SECOND TIME

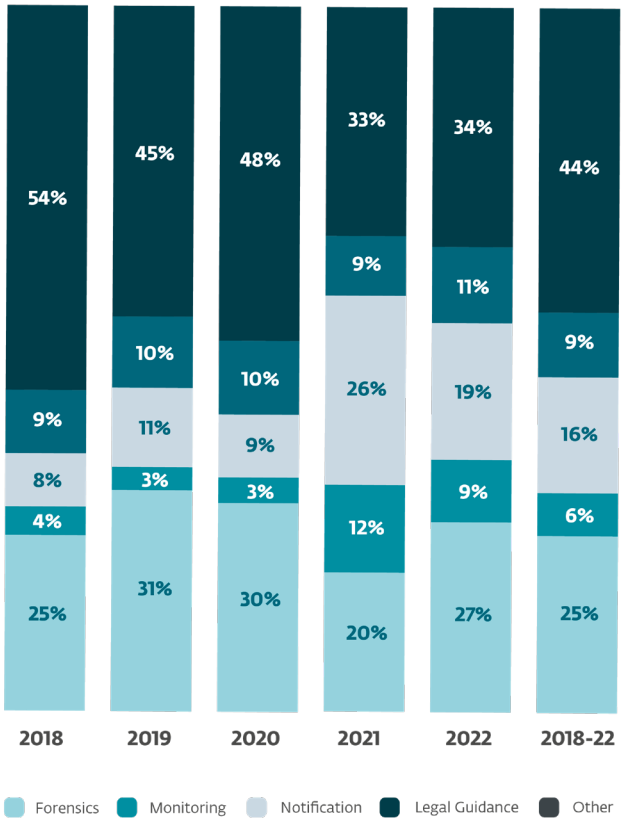
221

DAYS TO GET A BUSINESS BACK UP AND RUNNING, ON AVERAGE, AFTER A RANSOMWARE ATTACK

Unfortunately, recovering your business is not the end of the affair. Often costs continue long after a business is back up and running as multi-million-pound class action lawsuits are common, particularly in the US, when the organisation's customers' financial and personal data is compromised in an attack. In fact, recent research shows that exposure of personal customer and business information was what cost the most for a company recovering from a cyber attack. In the US, this may also extend to litigation which potentially could take years to resolve.

Long-term, the erosion of trust caused by reputational damage can be the most harmful cyber incident impact, with net income dropping and remaining low for up to two years after an incident is made public. Entities known to have weak cybersecurity can eventually suffer a downgrade in their credit rating, making it harder to obtain financing and leading to higher borrowing costs. Overall losses can be challenging to quantify, running into hundreds of millions, or even billions of dollars.

DISTRIBUTION OF CRISIS SERVICES COSTS (SMES)

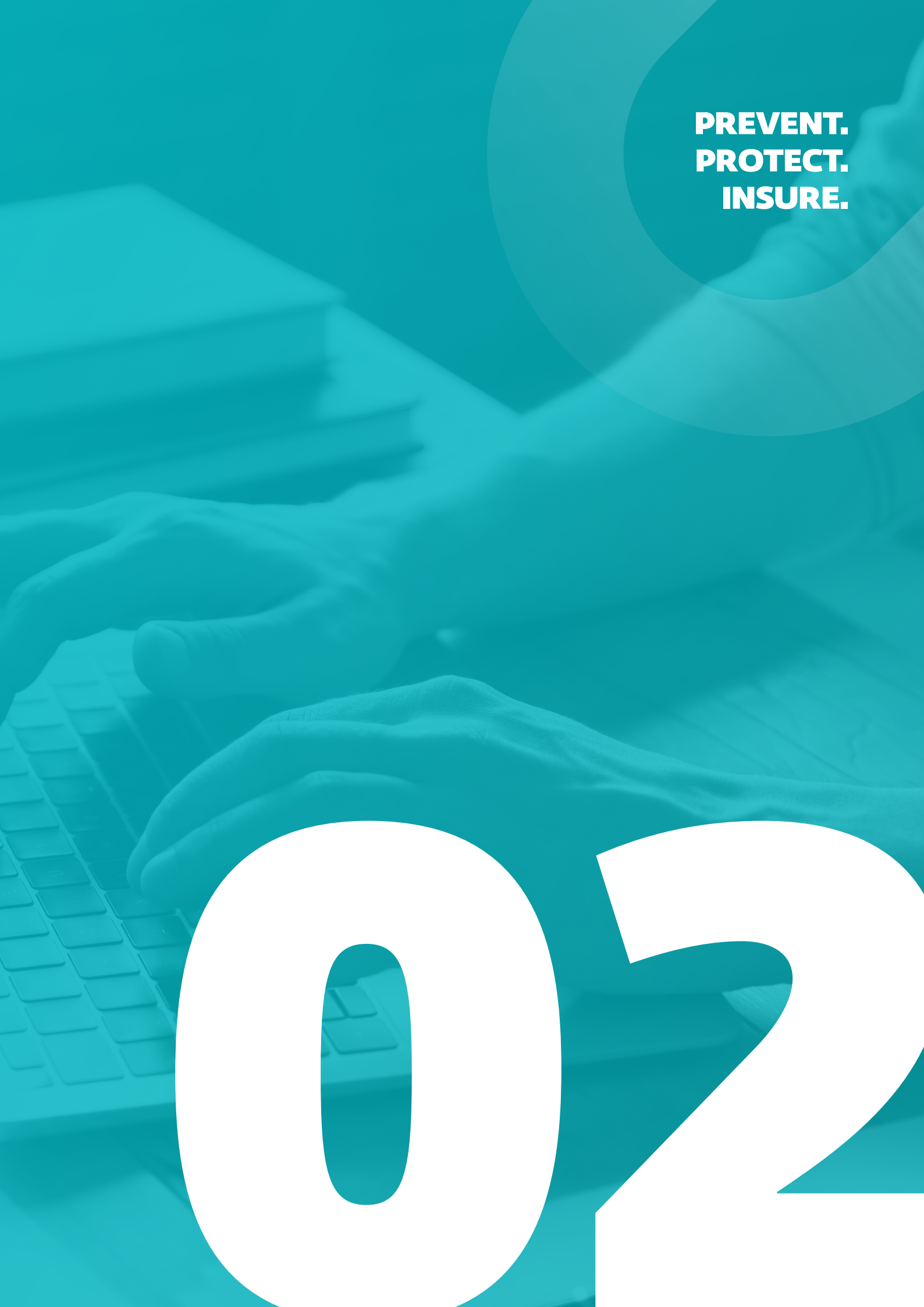


Source: NetDiligence.

MITIGATING THE RISK: CYBER INSURANCE.

Cyber insurance, also called cyber risk insurance, cyber liability insurance, or cybersecurity insurance, covers a company's financial risk and liability due to cybersecurity and privacy incidents like data breaches, ransomware, data loss, regulatory compliance violations, and cyberterrorism.

Cyber insurance often reimburses costs for data loss, incident response, regulatory sanctions, and business downtime. It may also cover remediation services, such as a breach investigation, litigation services, repairs to damaged IT assets, and data recovery, including paying a ransom.



PREVENT.
PROTECT.
INSURE.

02

$850k

THE AVERAGE INTERNATIONAL COST OF AN SME RANSOMWARE INCIDENT

WHY DO BUSINESSES NEED CYBER INSURANCE?

21st century cybersecurity is now not only about operations, but also about data, something that was famously termed as 'more valuable than gold'. Securing data is not just about knowing exactly where information is and what it is doing, it's so much more than that.

Cyber insurance helps protect businesses from the growing intensity and complexity of cyber threats, as well as the unpredictable and potentially devastating fallout that can result from some of these threats manifesting. Traditional insurance policies like general liability insurance or errors and omissions coverage do not specifically address cyber incidents and are unlikely to redress cyber claims.

WHO NEEDS CYBER INSURANCE?

While emphatically not a substitute for preventive controls, cyber insurance is a vital part of a robust, risk-based and, importantly, more holistic cybersecurity program for almost every business, especially SMBs. Among the major reasons why:

- Contrary to the misguided hope of "security through obscurity," attackers preferentially target smaller businesses, knowing they often do not make comprehensive and effective cybersecurity investments to keep pace with ever-advancing threats.
- The shift to remote working has radically increased the attack surface for many SMBs, introducing new vulnerabilities and exposing significantly more data.
- Amid the disruption of a cyber incident, SMBs may struggle to find the money, expertise, and other resources to mount a strong incident response and/or cover upfront costs and liabilities—especially if they have no contingency plan.

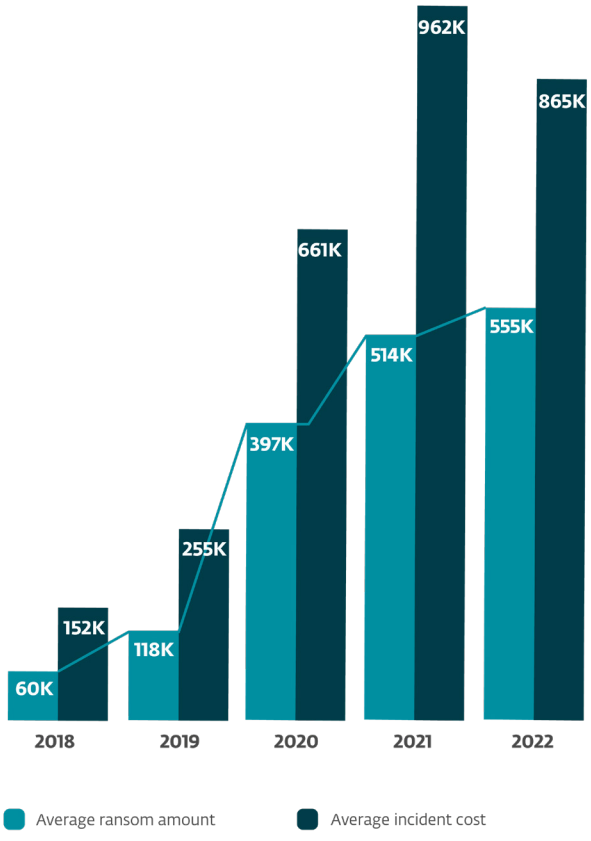
The International Monetary Fund (IMF) in its April 2024 Global Financial Stability Report states that extreme financial losses from cyber incidents (the worst 10% of losses) have escalated over 400% since 2017 and continue to increase rapidly. The SMB cost of a ransomware incident, one of the most expensive incidents, now internationally averages US$850,000 plus a US$555,000 average ransom payment.

Coupled with associated revenue losses, recovery costs, and reputational damage, these financial shocks can cripple or shut down unprepared organisations.

A comprehensive cyber insurance policy will safeguard business continuity and take these worst-case scenarios off the table. In the UK only 10% of SMBs have a cyber risk insurance policy. In Germany, this rises to 12% and in the US, to 21% - all lower than expected given the benefits. A likely explanation for this is the complexity of providing the information required by insurers, the pre-requisite of a security posture analysis and the challenge of adhering to insurance requirements through the lifetime of the policy.

However, the process of obtaining cyber insurance can help SMBs resist attacks by identifying and offsetting their top potential risks within a comprehensive risk management approach. Many cyber insurers also pair their policyholders with specialist expertise and resources to help mitigate the impacts of an incident and reduce payouts.

AVERAGE COSTS FOR RANSOMWARE



Source: NetDiligence.

WHAT COVERAGE DOES CYBER INSURANCE PROVIDE?

The cyber insurance market has been constantly evolving alongside the cyber threat landscape since its inception over 20 years ago. The first cyber insurance product/service was derived from professional liability policies and focused on risks from online software and website media/content.

With the advent of eCommerce and digital business processes came coverage for data loss, damages from viruses and malware, and network security breaches. Regulatory sanctions, business interruption, insider attacks, and damage to network assets were often explicitly excluded from this coverage.

Today's cyber insurance policies are much more likely to cover first-party damages to a policyholder's own organisation, as well as third-party damages to customers or partners. There has always been, and still is, considerable variation between cyber insurance policies. However, most of today's underwriters offer similar first-party and third-party terms.

UK businesses can expect most current cyber insurance policies to cover the following classes of damage:

- Data loss
- Incident response costs
- Forensic analysis
- Costs from business interruption, including revenue loss
- Liabilities stemming from network security failures

A policy may also cover:

- Regulatory and compliance sanctions
- Reputational damage
- Damage to physical assets
- Legal liabilities, including expenses from lawsuits and costs to notify stakeholders affected by a data breach

CYBER RISK INSURANCE COVER

(POLICY DEPENDENT)

- Incident response costs
- Legal and regulatory costs
- IT Security and Forensic costs
- Crisis communication costs
- Privacy Breach management costs
- Third Party privacy breach management costs
- Post Breach Remediation
- Funds Transfer fraud
- Theft of funds held in Escrow
- Theft of personal funds
- Extortion
- Corporate Identity Theft
- Telephone hacking
- Push payment fraud
- Unauthorised use of computer resources
- System damage and rectification costs
- Direct loss of profits and increased cost of working
- Additional increased cost of working
- Dependent business interruption
- Consequential reputational harm
- Claim preparation costs
- Hardware replacement costs
- Network Security Liability
- Privacy Liability
- Management Liability
- Regulatory fines
- PCI fines, penalties and assessments
- Defamation
- Intellectual property rights infringement
- Technology errors and omissions
- Court attendance costs

As underwriters analyse a growing volume of claims data, the cyber insurance marketplace is expected to continue its rapid development and maturation, propelled by greater risk awareness, as well as the ongoing digitisation of business processes and the rise of AI.

For example, recent analysis has shown that businesses using managed detection and response (MDR) services reduced their cyber incident response time by 50%—with a parallel reduction in incidents and per-incident costs. For businesses with MDR or equivalent, insurers are responding with finely tuned premium discounts and credits.

WHAT RISKS MAY NOT BE COVERED?

With interconnectivity and data exposure rising relentlessly, cyber insurers are likely to expand their coverage accordingly. This trend will further amplify the importance of cyber insurance for risk management not only among individual entities but for the entire global economy.

At the same time, insurers are leveraging data analytics to improve their loss ratios through stricter underwriting and ongoing rate increases. Insurers are reducing their risk exposure through steps like:

- **Reducing pay-out limits** for different damage classes
- **Increasing policyholders' self-insured retention amounts,** which is the amount a policy says the insured must pay before coverage starts
- **Requiring greater visibility into organisations' cybersecurity programs** (up to the level of an audit) to more accurately judge their true exposure and set pricing
- **Continuing to emphasise proactive cybersecurity controls** to drive down cyber risk
- **Becoming more selective** about what risks to accept and what industries to serve

WHAT ARE THE MOST COMMON POLICY EXCEPTIONS?

The negative fallout from cybercrime is highly variable, and few cyber insurance policies provide blanket coverage. Among the most common exceptions in today's cyber insurance policies in the UK and elsewhere are:

- **Financial fraud from social engineering attacks** like business email compromise (BEC) or spearphishing. Often the lost funds are explicitly not reimbursable if they were paid voluntarily by an employee.
- **The costs of hardening a company's cybersecurity posture following a successful attack.** This can be a major expense, but these investments can reduce future cyber insurance premiums and/or help a firm get or keep cyber insurance. Although coverage for this may not be included, the insurer may provide or recommend a breach coach or consultant to identify areas of weakness and recommend improvements in the impacted company's cybersecurity framework.
- **Potential loss of future profits** caused by lingering damage from data loss, theft of intellectual property, reputational harm, etc. These longer-term impacts can hurt sales, market share, talent recruiting and more, but are notoriously hard to link exclusively to a cyber incident.
- **Reduced value of intellectual property** following exfiltration of proprietary materials like new product designs. Losing its IP "secret sauce" through a cyber attack can put a company out of business or crush its market share, but this risk is usually excluded from cyber insurance coverage.
- **Nation state attacks or acts of war.** Following the example of Lloyd's of London and others, some cyber insurance policies now include clauses explicitly denying coverage for attacks declared 'acts of war' or attributed to a nation state actor. There are many open questions around applying such clauses, including how stakeholders decide what constitutes a nation state attack.
- **Geographic restrictions** on where coverages are in effect. For example, operations outside the home country may not be fully covered. Or a policy procured outside the home country may place coverage restrictions on home country-based operations.

Insurers may offer cover for some, or all, of the above risks as policy extensions. Organisations should carefully evaluate the likelihood of any of these risks manifesting and the potential damages before passing up add-on cover or otherwise forgoing needed protections.

As always, the specific language of policies and exclusions will largely dictate the extent of coverage. It is critical to read cyber insurance contracts carefully and consult a legal professional if you have questions.

"WORKING OUT WHO WAS BEHIND A PARTICULAR HACK HAS ALREADY MADE THE NEWS. MONDELEZ, AN AMERICAN FOOD COMPANY HIT BY THE NOTPETYA MALWARE, IS SUING ZURICH, A BIG INSURANCE FIRM, FOR REFUSING TO PAY OUT UNDER A GENERAL INSURANCE POLICY. ZURICH CITES AN EXCLUSION CLAUSE FOR LOSSES RELATED TO WAR, ON THE GROUND THAT THE NOTPETYA ATTACK IS THOUGHT TO HAVE BEEN CARRIED OUT BY RUSSIA.

"EVEN A TECHNOLOGICALLY SOPHISTICATED GOVERNMENT WOULD HAVE TROUBLE PROVING SUCH A CLAIM TO THE STANDARD DEMANDED BY A COURT,

"BUT IF ZURICH DOES WIN, IT COULD CAST A CHILL ACROSS THE ENTIRE MARKET— UNLESS INSURERS ACCEPT THAT CYBER INSURANCE MAY INVOLVE SHOULDERING THE SORTS OF RISKS THEY HAVE PREVIOUSLY SOUGHT TO AVOID."[3]

Andrew Coburn Risk Management Solutions

WHAT ABOUT RANSOMWARE COVER?

Ransomware incidents, or more commonly referred to in insurance policies as 'extortion' or 'cyber extortion', factor into most cyber insurance claims regardless of business size or industry. According to NetDiligence research, ransomware accounted for 85% of claims from 2018 to 2022, including recovery expenses (costs incurred to avoid or minimise business disruption).

Even if victims do not pay a ransom, these attacks are often costly and highly disruptive to operations. Organisations should do everything possible to prepare for the potential of a ransomware attack, including investigating cyber insurance options alongside best-practice cybersecurity controls like offsite backups and frequent tabletop exercises to test internal processes and policies.

Hoping to improve their loss ratios and reduce ransomware payouts, insurers are putting more ransomware-specific limitations on their policies and finding more ways to deny ransomware claims in whole or in part. Increasingly, insurers are also requiring ransomware readiness assessments and assigning expert ransomware negotiators, among other steps to limit their exposure. According to the Insurer Coalition, insurers have successfully negotiated the reduction of ransomware payments by 64%.

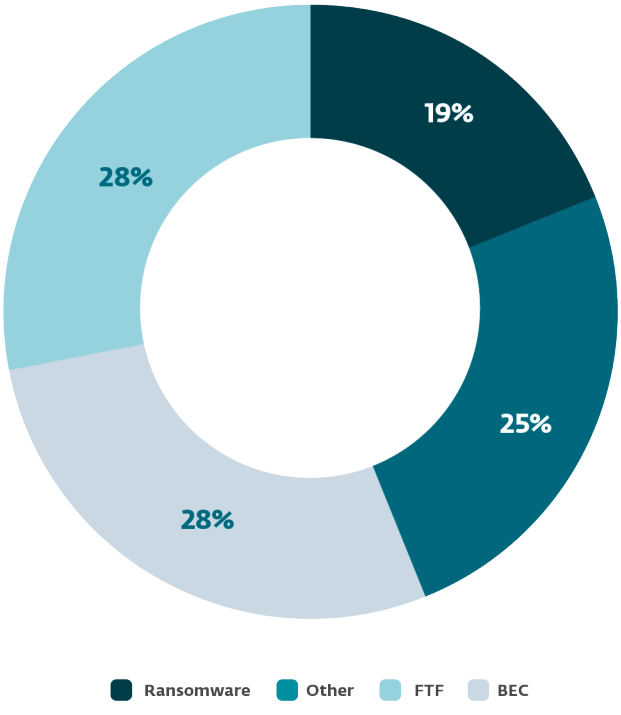
Ransomware coverage is usually included with a sublimit as an add-on to a wider cyber insurance policy. For example, a £1 million policy might include a £50,000 ransomware sublimit depending on a policyholder's ransomware risk. Standalone ransomware covers are an increasingly popular alternative, especially since some policies now explicitly exclude ransomware coverage.

While every policy has different terms, ransomware coverage may include:

- The ransom/extortion payment
- Services of an expert ransomware negotiator
- Forensics/investigation costs
- Damages to software and hardware/infrastructure
- Costs to recover and restore data
- Reimbursement for lost revenue due to downtime, reputational harm, etc.

Whatever type of ransomware insurance you procure, it is vital to carefully review and analyse policy language before making a claim so you know what coverage you can expect, including which costs are/are not subject to a ransomware sublimit.

GROSS REPORTED CLAIMS BY EVENT TYPE



Source: Coalition.

CYBER WARRANTY AND HOW IT DIFFERS FROM INSURANCE.

A cyber warranty is a new and developing concept that puts the onus on a technology supplier to guarantee the security of its product.

It is essentially exporting the Development Security and Operations (DevSecOps) concept from the company and embedding it into any technology that a company will buy in. DevSecOps is an application development practice that automates the integration of security and security practices at every phase of the software development lifecycle, from initial design through to integration, testing, delivery, and deployment - a process that echoes the underlying thrust of the EU legislation mentioned later in this report. It basically means that a cybersecurity company or software developer guarantees that they will pay out if their customers suffer a breach.

The conditions of the warranty can vary. For example, it could be that the customer has to prove they were using the company's product when they were breached. Or, alternatively, some providers will expect the customer to adhere to a set of security standards – say the five basic controls that make up the Cyber Essentials certification covered in the following section.

Again, the losses that the warranty will cover varies from provider to provider, but it's typically a fixed amount, for example, £1m. This could be useful to SMEs for two reasons. Firstly, if something goes wrong and your business gets breached, you'll get some money to cover the damages. Secondly, this provides software suppliers with an incentive to ensure their products are secure. However, this may also complicate things. Does the liability to pay then get bounced between two insurers with each claiming the other is primary?

A process that does not just benefit the SMEs; a cyber warranty can also give managed service providers a cost-effective method of remediating breaches for clients. Most providers allow any company doing remediation work to bill it on the warranty, covering the costs.

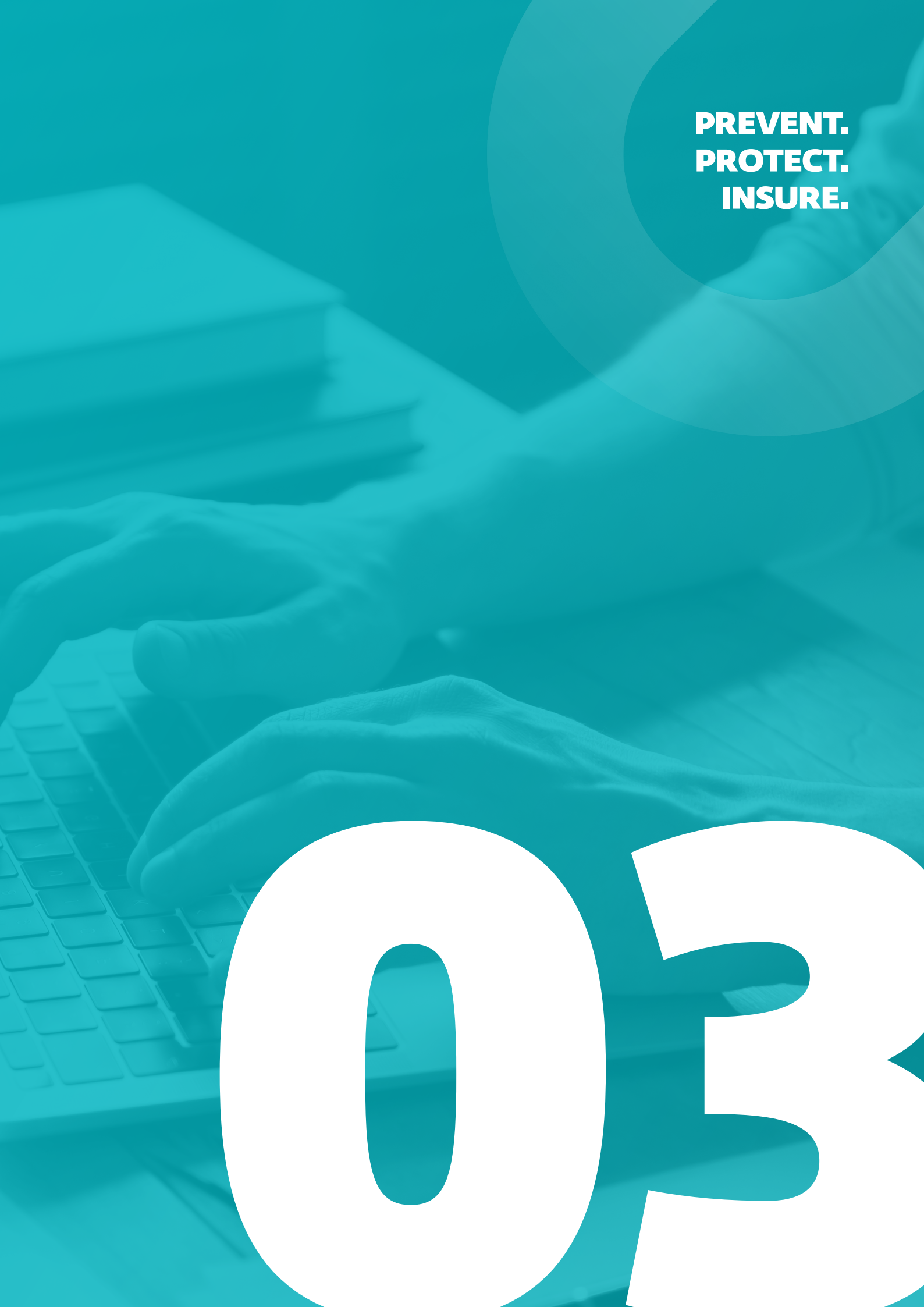
PAYING AN ATTACKER TO UNLOCK YOUR SYSTEMS SHOULD NOT BE THE FIRST COURSE OF ACTION IN A RANSOMWARE ATTACK

Before pursuing this course of action, you should report the matter to the police and speak with your insurer to establish the conditions for them paying cyber extortion expenses. Upon the resolution of a ransomware attack, your business should then look to repair the breach and improve security.

MEETING THE REQUIREMENTS FOR CYBER RISK INSURANCE.

Cyber insurance policies are a relatively new development in relation to other insurance policies. In the early days of cyber insurance, carriers were more relaxed about writing policies. As Richard Breavington, pointed out, "they didn't have a good understanding of the risks involved, and as a result, they dramatically reworked the way they were writing and issuing policies and the amount they were charging. The insurance carriers now have more of a grip on the risk and cost of cybercrime and have begun raising the security requirements of those they are insuring."

Most cyber insurance applications start with a detailed questionnaire, often in a "yes/no" format. If you have a robust cybersecurity program, this step will be straightforward. If your program is less mature, you should evaluate and enhance your cybersecurity posture before applying for cyber insurance to ensure you qualify and can get the best terms possible.


PREVENT.
PROTECT.
INSURE.
03

ASSESSING YOUR CYBER RISK BEFORE APPLYING FOR CYBER INSURANCE

There are various approaches for companies to assess their own cyber risk, from filling out standardised questionnaires to participating in trusted cybersecurity rating ecosystems like SecurityScorecard or Shared Assessment's Standardised Information Gathering (SIG) questionnaires. Uses for standardised questionnaires include:

- Assessing your cybersecurity posture and comparing it to peers.
- Identifying vendors that have robust security or may be vulnerable to hackers.
- Identifying fourth- and nth-party supply chain partners (your vendors' vendors, etc.) that do not meet your cybersecurity requirements.
- Assessing your insurability to determine price offerings.

"FROM SMALL START-UPS TO GLOBAL GIANTS, BUSINESSES ARE INCREASINGLY DEPENDENT ON NETWORKED DEVICES IN ONE FORM OR ANOTHER. WHILE THIS PRESENTS BUSINESSES WITH HUGE BENEFITS AND OPPORTUNITIES, THE INCREASING RELIANCE ON TECHNOLOGY ALSO INCREASES THE POTENTIAL HARM POSED BY CYBER RISKS."

Association of British Insurers

Some of the risks that cyber insurers will ask about include:

- Does your business handle, transmit, and/or process sensitive data like credit card information, healthcare data, personally identifiable information (PII) on individuals, US government contract information, trade secrets, biometric access credentials, etc.?
- How much sensitive data do you have? Just a few records or hundreds of thousands?
- Are you currently subject to any regulations with a cybersecurity or privacy component, such as HIPAA, Sarbanes-Oxley, GDPR, PCI-DSS, etc.? If so, are you in compliance and can you prove it?
- Is your cybersecurity program aligned with any comprehensive cybersecurity framework, such as COBIT, BSIMM, Cyber Essentials Plus, or ISO 27001?
- Do any vendors or other third parties have access to your IT systems? If so, what is your third-party risk management/audit program?
- Can your employees access company data with laptops, tablets, or other mobile devices?
- Do you have formal information security policies and procedures, and/or a Chief Information Security Officer (CISO) or similar role responsible for cybersecurity?

You will also need to evaluate and describe your technology environment and controls, such as:

- Do you require multi-factor authentication (MFA) for access to all critical systems and the company network?
- Do you have a firewall, and who is the vendor?
- Do you have an email filter or anti-spam solution to intercept phishing emails?
- Do you have a best-practice password policy and is it enforced?
- Do you have antivirus/antimalware protection?
- Do you have an intrusion detection system (IDS) or intrusion protection system (IPS)?

Other questions you should be prepared to answer include:

- Do you have customer contracts? If so, do they include "hold harmless" language that might reduce your liability?
- Do your cloud services providers have third-party audited cybersecurity attestations like ISO 27001?

TO HELP YOU PREPARE FOR YOUR INTERNAL EVALUATION, YOU CAN CHECK OUT SAMPLE CYBER INSURANCE APPLICATIONS, SUCH AS THESE.

Questionnaires from cyber insurance providers are likely to be long, detailed, and time-consuming to fill out. The response process may involve people from many business areas, not just an IT administrator. Any steps you can take to capture your answers for reuse across questionnaires will be worth the effort.

Even if the questionnaire has a yes/no format, it is crucial that your answers are accurate and defensible. Misrepresenting compliance with a requirement could result in legal action and/or coverage denial.

SECURITY QUESTIONNAIRE TOPICS VARY WIDELY, BUT OFTEN INCLUDE SOME OF THESE:

- Do you have a business continuity program?
- Do you have a disaster recovery program?
- Do you have a data breach notification program and policy? What is your lead time to notify stakeholders of a data breach?
- Do you have a patch management program?
- Do you monitor and manage security event logs?
- Do you have a change management program? What is your process for emergency change control?
- Do you encrypt data at rest and/or in transit?
- Do you have a backup program? Do you test it regularly? Do you have offsite backups?
- Do you conduct regular vulnerability assessments?
- Do you conduct regular penetration tests?
- Are you compliant with privacy legislation like GDPR?
- Do you have a cybersecurity awareness and training program?
- Do you have a physical security program and policy?
- Do you have a third-party risk management program?

EXTERNAL SECURITY SCANS FOR CYBER LOSS CONTROL

A growing number of cyber insurance underwriters are using automated security scans as part of their application process. This can significantly increase their knowledge of applicants' cybersecurity controls and associated vulnerabilities, allowing them to judge overall cybersecurity posture. The results can directly impact policy coverages and costs, and companies often must remediate areas of concern prior to obtaining coverage.

These scans are usually automated and assess only internet-facing assets, such as websites or customer portals. Some insurers may also scan the so-called 'Dark Web' for evidence that an applicant's system has been compromised.

While useful for reporting significant weaknesses and potentially alerting companies to major risks, automated scans cannot take the place of in-depth, third-party vulnerability assessments and penetration testing from the standpoint of risk assessment. Also, as cyber risk insurance becomes an accepted normality for smaller and medium sized businesses, it may become challenging for insurers to have the resources on hand that understand the risk the scan output highlights - it's unlikely that a local insurance broker will understand the risk of an open port for example.

MULTIFACTOR AUTHENTICATION (MFA).

Passwords alone are no match for today's attacks. If you do not have MFA for remote access, privileged accounts, and sensitive applications, you cannot protect sensitive data from unauthorised access and may not be able to obtain cyber insurance at any price.

BEST-PRACTICE BACKUPS.

The prevalence and high costs of ransomware make a robust backup strategy essential. Important elements include encryption, regular restore testing, and offsite storage.

EMAIL FILTERING.

If phishing emails cannot reach your users, they cannot threaten your systems and data. Email filtering is a cost-effective way to reduce risk, especially when combined with scanning attachments or links for malicious content.

WHAT CYBERSECURITY CONTROLS DO INSURERS REQUIRE?

Along with risk profiles obtained through questionnaires and external scans, a company's cybersecurity controls play a major role in determining insurability, coverage/ terms, and rates.

The top cyber controls that insurers now consider minimum requirements for insurance are:

VULNERABILITY AND PATCH MANAGEMENT.

The exploitation of known vulnerabilities often provides cybercriminals with an open door into a corporate network. Reducing this risk through scanning and patching automation significantly reduces risk.

ENDPOINT DETECTION AND RESPONSE (EDR).

To eliminate vulnerabilities, block attacks, and support incident response, organisations need current visibility on all the devices being used to access sensitive data, such as workstations, laptops, and phones. EDR monitors devices and tracks their location, software versions, and user activity like software installations. Some EDR solutions can also provide forensics or wipe systems following an incident.

PRIVILEGED ACCOUNT MANAGEMENT (PAM).

To safeguard the most sensitive data and help prevent the most damaging data breaches, companies need to secure privileged accounts like administrative accounts with more strict login credentials and procedures. Most PAM systems operate like a vault that protects credentials from exposure and theft, while enabling them to be used only to perform privileged activities.

REGULAR CYBERSECURITY AWARENESS TRAINING.

This ensures employees are up to date on the security threats and procedures that can help their business reduce their risk of being a victim of a cyber attack and demonstrates a commitment to the all-important cyber posture that insurers are looking for.

While the controls just listed are table stakes for obtaining cyber insurance, some more advanced controls will reduce an applicant's risk and help ensure a favourable quote. These include:

- Network segmentation in alignment with zero trust principles
- Extended detection and response (XDR) with continuous monitoring on all endpoints
- Managed detection and response which provides an outsourced EDR/XDR service with continual monitoring by dedicated analysts
- Use of a security information event management (SIEM) or managed SIEM solution
- Regular vulnerability assessments and penetration tests
- A cybersecurity certification or report based on a third-party audit, such as an ISO 27001 certification
- Documented risk assessment and data governance policies and procedures and evidence that a recognised cybersecurity framework is being followed

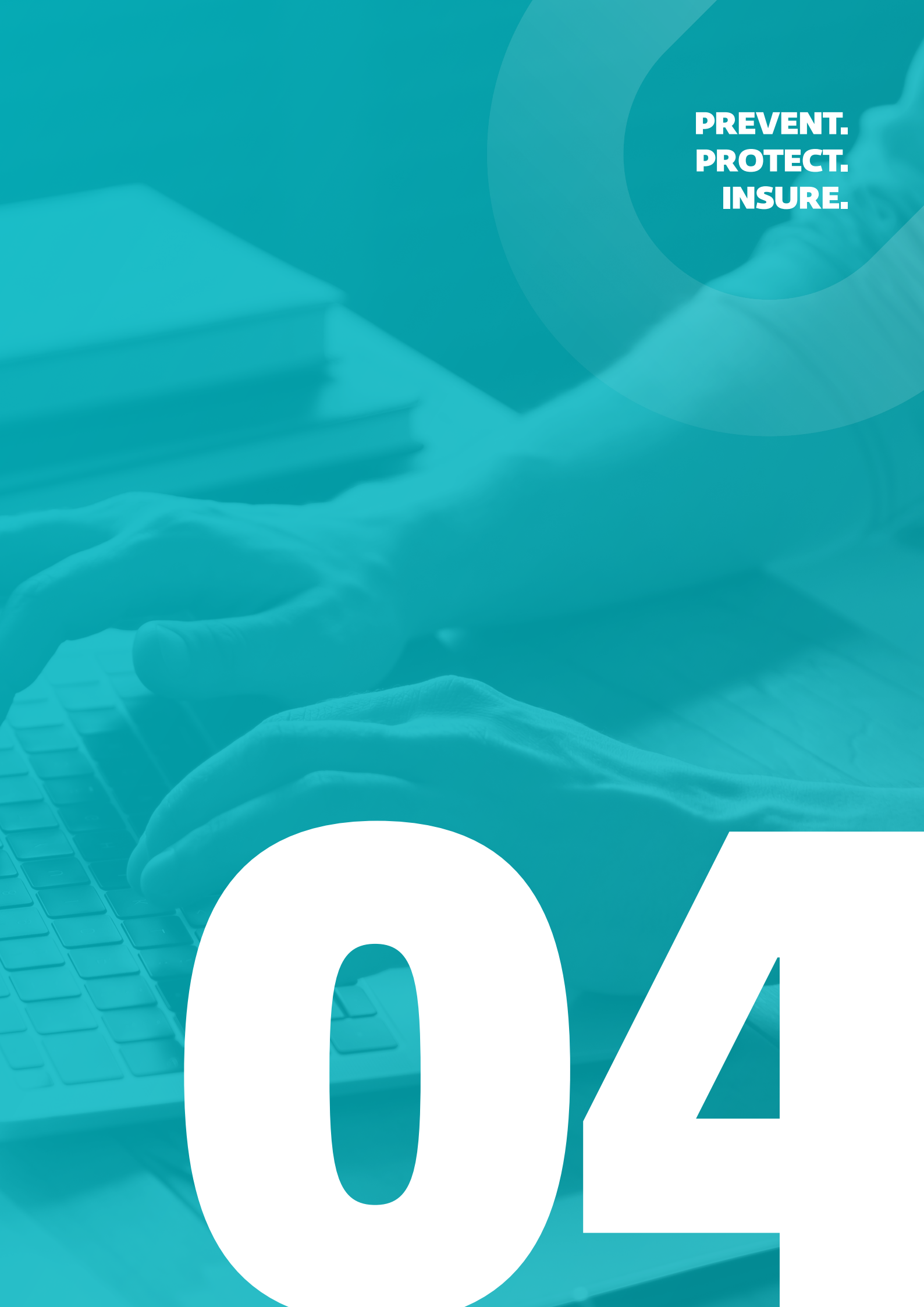
Obtaining cyber insurance is complex. It is tailored to the particular IT configuration a company has adopted and the circumstances of its business. This means businesses should carefully consider their needs before making a final decision. To obtain cyber insurance, it is essential that companies demonstrate awareness of their cyber risk and show that they are taking the appropriate steps to deal with it. For insurers, it is the virtual equivalent of inspecting a house to see if it has the relevant locks and alarms.

"IT'S A FUNDAMENTAL CONCEPT, BUT IT'S SURPRISING HOW MANY ORGANISATIONS EITHER DON'T HAVE BACKUPS OR COMMONLY GO THROUGH A PROCESS OF DOING BACKUPS OF THE DATA AND THEIR OPERATING SYSTEMS BUT HAVE NEVER CHECKED TO FIND OUT WHETHER THEY CAN BE RESTORED."

A point made by Professor Andrew Jones, one of the world's leading cyber forensics experts in the compilation of this report.

THE RELATIONSHIP BETWEEN CYBERSECURITY AND INSURANCE.

Cybersecurity, according to the technology analysts, Gartner: "is a business problem that has been presented as such in boardrooms for years, and yet accountability still lies primarily with IT leaders".



PREVENT.
PROTECT.
INSURE.

04

IN THE 2022 GARTNER BOARD OF DIRECTORS SURVEY,

88% OF BOARD MEMBERS CLASSIFIED CYBERSECURITY AS A BUSINESS RISK;

JUST 12% CALLED IT A TECHNOLOGY RISK.

Relationships between different industries can often be hard to visualise. Take, for example, the role that insurers play in the climate change arena. Areas susceptible to flooding become uninsurable forcing the residents to rely on last resort insurance which is often government backed or funded. This increases the financial and political risk on governments if there is a severe weather incident, and thus drives the political agenda to combat climate change to reduce risk.

Cybersecurity and cyber resilience are similar in that an incident can cause citizens to ask what politicians are doing to protect their everyday lives from cyber threats. An example of this is the ransomware attack on Colonial Pipeline in 2021, an incident that saw lines forming at gas stations across the east coast of the US. The issue quickly turned political with extensive law enforcement activity and a rush to publish a Whitehouse Executive Order on the mitigation of cyber attacks.

Of the issue that ransomware demands are being paid, as with the Colonial Pipeline incident mentioned above, and the funding for this could, in some instances, be attributed back to insurers. This creates a potential barrier between those that are cyber-defenders and insurers that could be seen as funding cyber-attackers. A different viewpoint on this is that the insured are purely crowdfunding ransomware payments to cybercriminals via insurers. Ironically, companies that have cyber risk insurance and have a policy of non-payment of extortion demands are indirectly funding those that do pay such demands. For example, in several states in the US, it is prohibited for state organisations funded by taxpayers to pay a ransomware demand, but many of them likely have cyber risk insurance, which indirectly funds an extortion demand.

Insurers provide stability and a detailed understanding of risk, both of which are used to combat situations such as an attack on critical infrastructure as per the example above. As details in the previous sections of this whitepaper demonstrate, the insurance industry is raising the requirements the cybersecurity technology that needs to be implemented, and are actively monitoring cybersecurity posture through scanning public facing services and the Dark Web and such like.

This places insurers at the forefront of cybersecurity spend. Without the motivation to implement cybersecurity to comply with insurance requirements, companies may not have the same cybersecurity posture. In many cases, the insurer will have preferred cybersecurity providers on a list, reducing the need for extensive questioning pre-insurance as the insurer has an in-depth knowledge of the product being used. So not only is the insurer providing the motivation for cybersecurity spend, they are also choosing the product.

Recently this has been taken to a new level with the US arm of a UK based insurer creating a managed service provider (MSP) that offers the cybersecurity solutions needed to comply with the policy requirements. For a smaller or medium sized business, this potentially becomes a one stop shop for insurance and cybersecurity, which could remove the barrier to insure and make the market scalable.

However, a word of caution, this evolution means many of the insurer's customers may be running the same cybersecurity solution which creates a mono-cybersecurity-culture. A cyber-attacker only needs to break one solution to attack the many that are insured with the single insurer. The result could be devastating as it creates a major incident with all those affected being insured by one party.

The two industries are intrinsically linked. Insuring against a cyber attack places significant reliance on the cyber-defenders, and the cyber-defenders are reliant on the insurer requiring the advanced tools as part of the insurance requirements.

"WE KNEW WE NEEDED TO DO SOMETHING FOR THE BIGGEST RISK TO THE GLOBAL ECONOMY. THE WHOLE INSURANCE INDUSTRY SHOULD BE ON A LEARNING STRATEGY CURRENTLY, WE ALL SHOULD LEARN AND SHARE MOST OF THE INFORMATION WE HAVE TO LEARN MORE QUICKLY."

Senior Manager for a leading insurance firm.

"THE CYBER INSURANCE INDUSTRY WILL BE INCREASINGLY HELPFUL IN DRIVING UP STANDARDS OF CYBERSECURITY ACROSS THE BOARD AND ACROSS SECTORS BECAUSE OF THE STANDARDS THAT ARE BEING IMPOSED TO GET THE RIGHT PREMIUM OR TO GET INSURANCE - OR NOT."

Breavington, Lawyer and Partner at RPC, Head of Cyber and Tech Insurance.

According to some high-level thinkers within the insurance industry, cyber insurance is a way of driving compliance and transparency through the technology industry by insisting that those working in technology guarantee their data and can certify the methods they have used to protect it. In effect, carrying out insurance in a similar way to that insisted on for car drivers.

THE CHALLENGE OF EITHER SIDE – INSURERS COULD BE SEEN AS FUNDING CYBERCRIME

Cyber insurance is unique among insurance offerings in that both the insured and the insurer are beginning to develop a mutual interdependency because of the continuously changing threat that they both face.

While for now, the argument that the situation many businesses now find themselves in is analogous to a war zone has been dispensed with. It is still a business environment that some of those interviewed likened to driving on a road where a few of the other drivers are actively trying to run into you. A situation that becomes even more surreal because it is a world where being insured makes you even more of a target.

This development means that cyber-attackers may actively seek out those with insurance in the belief that their insurance provider will pay out. This has led to accusations that the insurers are funding cybercrime by providing a service that the victims are extremely grateful for.

It is a charge though, that still will have little weight because of the sanctions list, and one that any organisation seeking insurance should investigate as paying a ransom in some circumstances could lay it open to significant penalties from US, EU, and UK authorities – see the sanctions section below.

A final challenge, according to the insurers, is the relationship developing between the insurers and the insured.

According to some of the senior voices in the industry, the closeness of a relationship where one organisation is actively advising the other on what it needs to do to avoid a cyber attack could lead to significant legal cases against the insurer if they fail to pay out and blame their customer for a cyber breach; with the customer claiming it did everything it was told to do by the insurer.

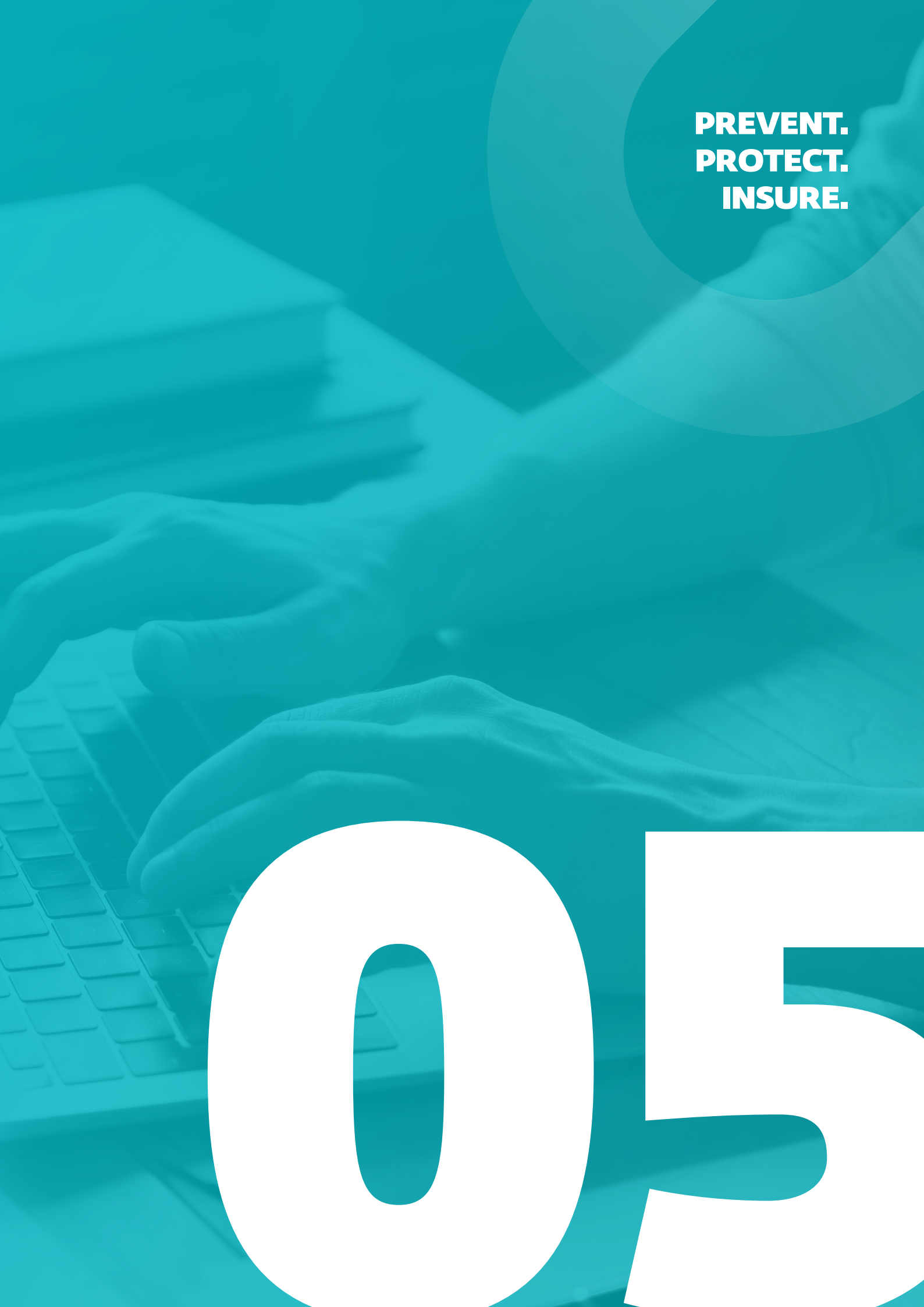
In the case of such actions, it will be down to either party to prove liability on one side or the other and is being viewed as a potentially rich area of conflict by the legal sector according to leading technology lawyer, Mark Deem of the law firm, Wiggin.

"OVER THE NEXT FIVE YEARS, WE THINK THAT DISPUTES OVER LIABILITY DUE TO BUSINESS TRANSFORMATION ISSUES WILL INCREASINGLY FOCUS ON LIABILITY AND I CAN FORESEE THAT DISPUTES OVER INSURANCE AND WHETHER A COMPANY IS COVERED OR NOT FOR AN EVENTUALITY WILL BE A HOTLY CONTESTED AREA."

Mark Deem, Commercial litigator,
Solicitor-Advocate and Partner at Wiggin LLP

SANCTIONS, LEGISLATION AND REGULATION.

While the picture in Europe has seen just as much recent activity, according to Robert Santifort, a legal associate for Eversheds Sutherland and an expert on European technology law, a framework will add to their cybersecurity obligations.


PREVENT.
PROTECT.
INSURE.

“IT’S A WHOLE NEW RANGE OF LEGISLATION. WE HAVE THE NETWORK AND INFORMATION SECURITY DIRECTIVE 2, WHICH ENTERED FORCE IN JANUARY 2023 AND WILL BE IMPLEMENTED INTO LOCAL LEGISLATION BY OCTOBER 17TH, 2024. A HUGE AMOUNT OF LAW IS COMING INTO FORCE IN EUROPE.

“WE HAVE THE DIGITAL OPERATIONAL RESILIENCE ACT (DORA), SPECIFICALLY TARGETING THE FINANCIAL SERVICES INDUSTRY AND THEIR CRITICAL THIRD-PARTY ICT PROVIDERS, WHICH IS ABOUT CYBERSECURITY SERVICES PREDOMINANTLY BUT ALSO IN RESPECT OF PRODUCTS.

“AND WE ARE SEEING THE DRAFT OF THE CYBER RESILIENCE ACT, AND THAT’S REGULATION AS OPPOSED TOA DIRECTIVE, WHICH NEEDS TO BE IMPLEMENTED.

“SO, ANY HARDWARE AND SOFTWARE WITH DIGITAL ELEMENTS SHOULD COMPLY WITH THAT NEW PIECE OF LEGISLATION. THAT’S ONLY A SMALL PORTION OF THE TSUNAMI OF DATA AND CYBER LEGISLATION WHICH IS COMING OUR WAY FROM THE EUROPEAN COMMISSION.”

Richard Breavington, a Partner at RPC
– a firm specialising in cyber insurance litigation


PREVENT.
PROTECT.
INSURE.

THE FOLLOWING ARE A LIST OF SITES CONTAINING USEFUL SANCTIONS INFORMATION:

- https://www.state.gov/cyber-sanctions/
- https://ofac.treasury.gov/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities
- https://ofac.treasury.gov/media/912981/download?inline
- https://www.gov.uk/government/publications/financial-sanctions-cyber-attacks
- https://www.gov.uk/government/publications/financial-sanctions-faqs
- https://assets.publishing.service.gov.uk/media/66015bbdf1d3a065f132acd1/Cyber.pdf
- https://assets.publishing.service.gov.uk/media/65ca0d7c14b83c000ea716bd/Financial_sanctions_guidance_for_ransomware.pdf
- https://www.gov.uk/government/collections/uk-sanctions-regimes-under-the-sanctions-act

The motivation behind most cyber attacks is monetisation, with the threat actors initiating the attack for personal financial gain. In the case of ransomware, where the payment is a conscious decision made by the business, it creates a lucrative marketplace that encourages the targeting of other victims in the same sector and motivates others to join the ranks of the cybercriminals.

Guidance from governments and regulators state that demands should not be paid and warns that the payment of ransom demands does not always result in the regaining of access. However, in reality, the ransomware groups behind such demands also have brand reputation and image to uphold. If payment fails to deliver resolution then fewer will pay, which would be bad for the cybercriminals' business.

An attempt to limit, or restrict, the payment of ransom demands by governments is made through the enforcement of sanctions, where it becomes illegal to pay an individual, organisation or, in some cases, even an identified crypto-wallet as they are included on a sanctions list. The sanctions may also involve asset freezing, travel bans and such like on those that appear on the list.

For the victim of a cyber attack such as ransomware, a result of transacting or being involved in any way with those on the sanctions list may result in considerable financial penalties and even imprisonment. Making funds or economic resources available directly or indirectly to sanctioned individuals or companies for their benefit is prohibited under the UK HM Treasury Office of Financial Sanctions Implementation, the EU Sanctions Regime, the US Department of the Treasury's Office of Foreign Assets Control (OFAC), and many other similar government departments around the world.

Sanction regimes present the victims of ransomware or anyone facilitating payments' requests (either by using a crypto intermediary or a cyber insurance carriers) with a dilemma between paying versus potential violation. An additional issue for the victims of ransomware is that attribution is difficult, especially within the limited timeframe hackers give victims to pay the ransom and increases both uncertainty and risk.

The complexity of these scenarios has been recognised by the US Department of the Treasury's Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) who, on October 1, 2020, published advisories on the sanctions and anti-money laundering risks of facilitating ransomware payments. One of the ways the US is dealing with the issue includes the possibility to apply for a licence authorising the payment, an avenue not yet contemplated under the EU regimes.

AND IN ANOTHER INTERESTING DEVELOPMENT, SOME CYBER INSURANCE COMPANIES ARE NOW CHAMPIONING THE ROLE LAW ENFORCEMENT CAN PLAY IN CYBER ATTACKS, POINTING OUT THAT IN MANY CASES INVOLVING AUTHORITIES LOWERED THE COSTS OF AN ATTACK.

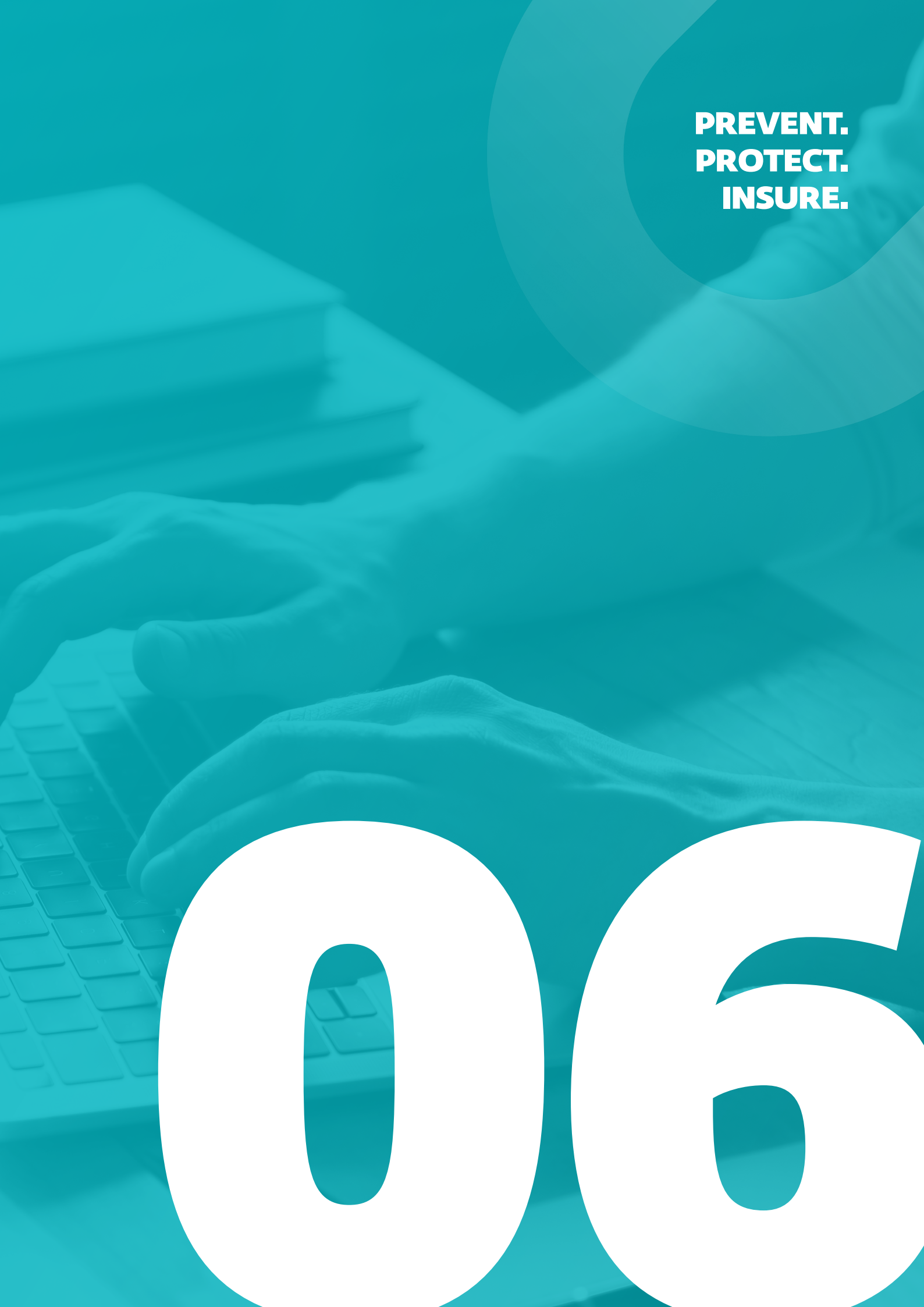
The potential that paying a ransomware demand may be illegal due to the sanctions list does not make the actual payment of a ransomware demand illegal. The creation of a new anonymised cryptocurrency wallet is a simple task, and the threat actors behind a ransomware attack are familiar enough with the restriction of paying a sanctioned entity to ensure that attribution is complex or unachievable to ensure there is no barrier to payment. Insurers are also fully aware of the restrictions a typical cyber-response team will have, including in-depth knowledge of which entities appear on a sanctions list. They can then provide advice to ensure no laws are infringed in the scenario where the ransomware demand is paid.

IN THE CREATION OF THIS WHITEPAPER, THERE WAS AN ATTEMPT TO ESTABLISH IF ANY VICTIM THAT HAD PAID A RANSOMWARE DEMAND HAD EVER BEEN SUBJECT TO PROSECUTION, IMPRISONMENT, OR OTHER RECOURSE DUE TO A SANCTIONS LIST INFRINGEMENT. WE COULD NOT IDENTIFY ANY CASE.

However, we do not recommend paying a ransomware demand nor any known sanctioned entity to find out if authorities will prosecute, and it should be noted that in some US states and certain countries, the act of paying a ransomware demand itself is illegal.

FUTURE EVOLUTION OF CYBER RISK INSURANCE.

The cyber risk insurance industry is evolving and as has been documented in this whitepaper, has faced challenges from unpredictable cyber threats causing incidents that have demanded significant payouts.



06

THE BLACK BOX

One of the most significant issues raised in this whitepaper is the issue of complying with the increasing cybersecurity requirements laid down by insurers, and from the insurer's perspective, the knowing if the insured is actively adhering to the requirements. A single point in time confirmation that the policy is being activated or renewed does not ensure the reduction of risk throughout the policy life. An analogy is car insurance: a driver answers an insurer's questions regarding their driving habits at the start of a policy but could have answered the questions in a less than honest way. For drivers there is the option to have a black box in the vehicle that reports a driver's behaviour, or at least in part. The reward for the infringement of the driver's privacy could potentially be lower premiums.

The same scenario of real-time monitoring of a company's cybersecurity posture could be implemented, with insurers using a data feed from a company's internal systems that demonstrate compliance with the insurance pre-requisites, and more importantly when there are alerts that are deemed high risk and require attention. For larger organisations this may sound too intrusive, but when considering the volume and scale of insuring smaller businesses this may be a necessity to make insurance affordable.

A potential solution moving forward could be an app that not only shows the company's current cybersecurity posture and alerts, but also has the ability to show the reduction or increase in premium should the requirements not be fully complied with.

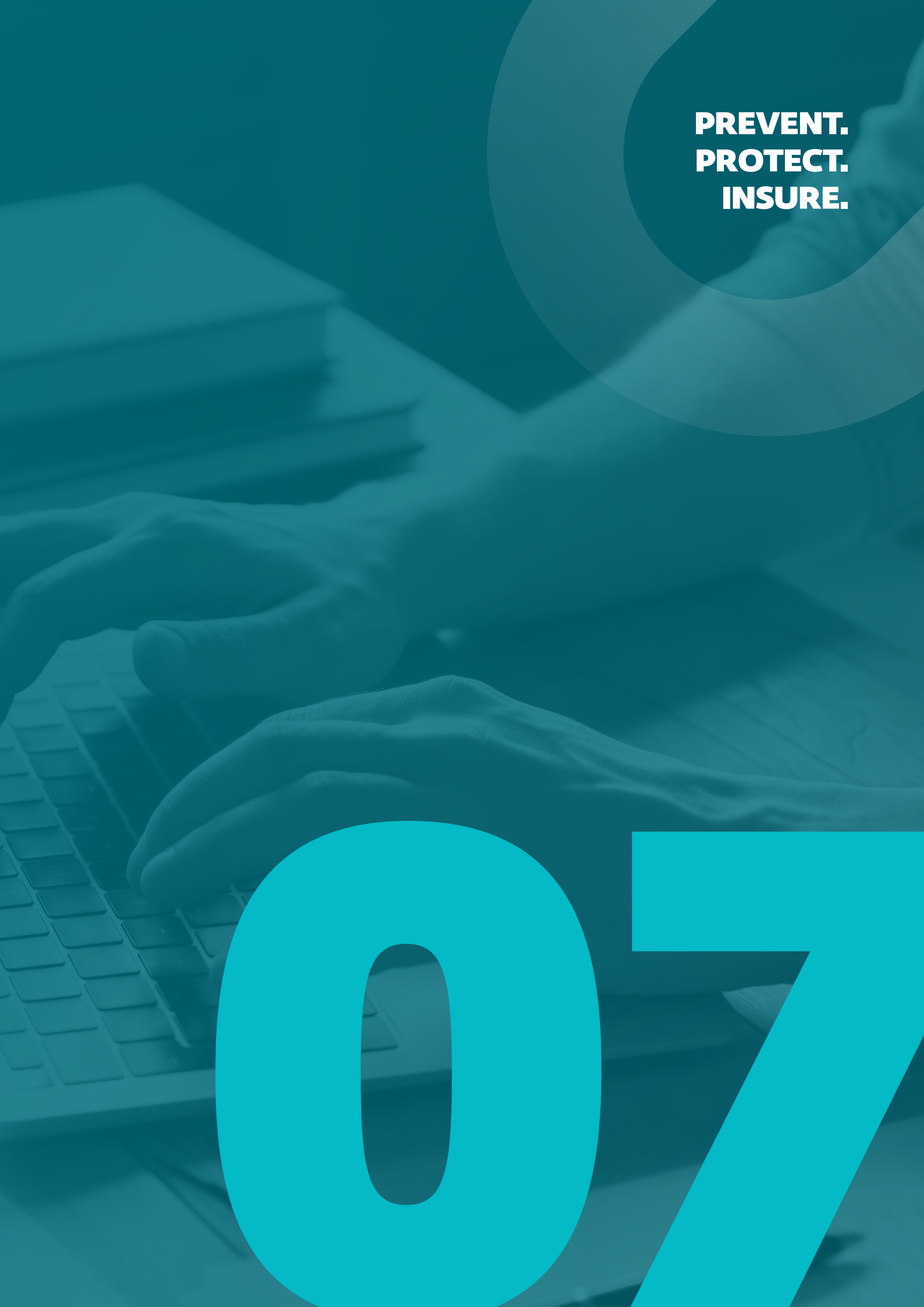
THE HUMAN ELEMENT

Another important cybersecurity risk is social engineering and human behaviour, as outlined in statistics mentioned earlier in this paper. This is, unfortunately, a challenging issue to address. For over 10 years, cybersecurity professionals, educators and governments have advised people to have strong passwords, yet we still see data in breaches that demonstrate weak passwords are still an issue.

Some sectors of the financial industry recognise that changing, monitoring, or assisting in securing the actions of consumers online reduces financial fraud. If a consumer clicks a phishing link and provides their financial details, the bank is typically on the hook to reimburse the consumer. However, in a scenario where the bank is only liable when transactions with third parties through a monitored connection are permitted, this could reduce losses due to fraud. For all other transactions, the bank customer would need to have an individual cyber liability and identity protection policy.

IGNORING PRIVACY LEGISLATION FOR A MOMENT, IF THE BANKS AND THE INSURANCE COMPANIES BEHIND SUCH MONITORING CREATED A 'CYBER RISK SCORE' ON EVERYONE, IN THE SAME WAY CREDIT SCORES ARE CREATED, THEN POTENTIALLY INDIVIDUAL CYBER AND IDENTITY INSURANCE PREMIUMS COULD BE INDIVIDUALISED BASED ON BEHAVIOUR. INSURERS MAY USE THIS DATA WHEN ASSESSING A COMPANY'S CYBER RISK IF THERE IS ENOUGH DATA ON EACH EMPLOYED INDIVIDUAL. THEIR CYBER RISK SCORE COULD BECOME A FACTOR IN THE CALCULATION OF THE CYBER RISK INSURANCE PREMIUM. PROFILING EVERYONE FOR RISK MAY SOUND FAR-FETCHED TODAY, BUT IN AN ERA OF AI AND DATA, THIS COULD QUICKLY BECOME A REALITY. POTENTIALLY EVEN TO THE POINT WHERE AN EMPLOYER MIGHT TAKE A REFERENCE FROM A THIRD PARTY TO CONFIRM A CANDIDATE WILL NOT INCREASE THE CYBER RISK.

CONCLUSION.



PREVENT.
PROTECT.
INSURE.

07

CONCLUSION.

For a business or organisation to prosper it needs to address continual challenges and risks, often needing to overcome things that put its very existence into question. Insurance provides a stable option to alleviate some of those risks, and has for many centuries passed, allowing businesses to focus on growth and opportunity, while at the same time driving requirements that minimise risks.

The digital age, even pre-internet, has provided insurers with opportunities and challenges. In the earlier years, insurers required computing dark rooms to use halon fire systems. As equipment became less expensive, this shifted to water-based fire systems. Decisions such as this are taken by insurers based on data, the probability of a claim and potential financial payout. As the equipment becomes less expensive, the risk to human life became the priority.

The challenge in today's digital environment for insurers is the lack of data. Digital transformation was expedited due to the pandemic and then extortion based cyber attacks have been empowered by crypto-currency, all within the last six years. This perfect storm of businesses needing to insure risk in order to survive and the lack of data explains why the insurers are continually adapting requirements and increasing premiums at an escalated pace.

Adding to this already complex environment is the availability of AI, it has now become an available cost-effective tool businesses can adopt to further grow their business both financially and for efficiency. As with any new technology there are unknown risks, such as cybercriminals potentially using AI poisoning as a future extortion method.

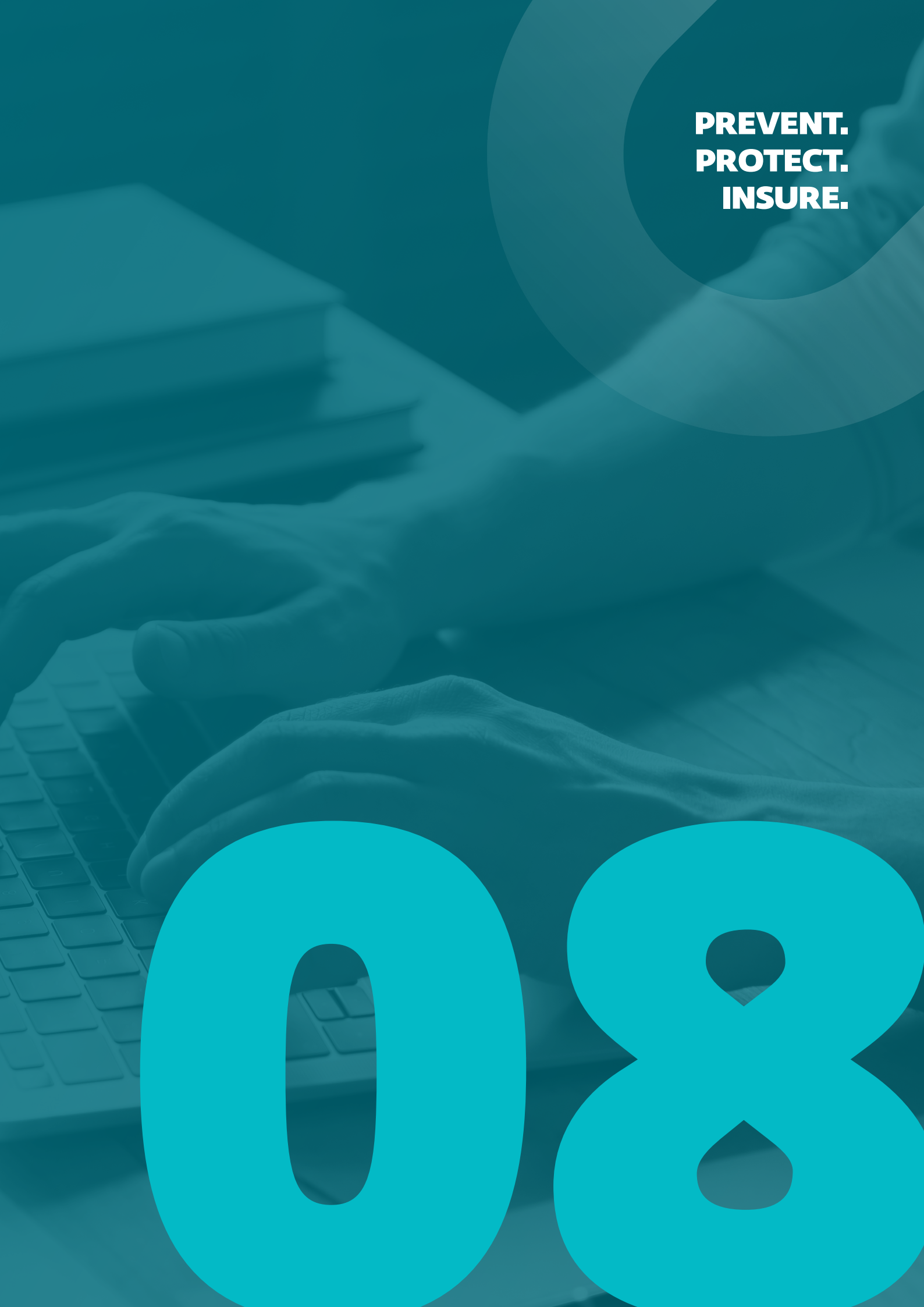
Today, it's essential that businesses adopt a cybersecurity posture that provides them with the best possible protection, whether insured or not. Insurers, who understand risk based on data require many different technologies and processes, for example the use of backup systems, multi-factor-authentication and advanced endpoint detection and response (EDR) solutions. The full list of recommendations insurers require are typically a subset of those that cybersecurity professionals and cybersecurity frameworks also recommend. While insurers are focused on reducing the potential of a financial claim, the cybersecurity industry is focused on reducing the risk of any cyberattack. The benefit to all businesses is to understand the requirements both need or recommend and adopt those that apply to your business, providing the best cybersecurity posture and lowest financial risk.

This relationship between cyber insurance and cybersecurity is inseparable and, with cyber insurance revenues expected to nearly double year-on-year, these two industries are fast becoming a marriage of convenience.

However, there remains one significant obstacle in this becoming a happy and truly fulfilling marriage - the funding of cybercrime through the payment of ransomware demands by insurers needs to stop, unless in exceptional circumstances.


85%
74%
63%

APPENDIX.


PREVENT.
PROTECT.
INSURE.
08

MANAGED DETECTION & RESPONSE SERVICES FROM ESET

ESET OFFERS MANAGED SERVICES FOR SMB AND ENTERPRISE CUSTOMERS. ESET MDR AND ESET DETECTION & RESPONSE ULTIMATE ARE 24/7 THREAT MANAGEMENT SERVICES, USING AI AND HUMAN EXPERTISE TO DELIVER WORLD-CLASS RANSOMWARE PROTECTION WITHOUT THE NEED TO MAINTAIN IN-HOUSE SECURITY SPECIALISTS.

STRENGTHENING SECURITY READINESS

Accelerate your threat detection, investigation and response capabilities with ESET's cybersecurity expertise. ESET is part of the Joint Cyber Defense Collaborative (JCDC) and collaborates with the FBI.

EXPERIENCED THREAT HUNTERS

Your business is protected 24/7 by human experts. ESET threat hunters monitor active campaigns by malware groups and continuously evaluate detections, providing you with another layer of threat hunting.

CROSS-INDUSTRY INSIGHTS

Get access to pre-built, customisable library of detection behaviour patterns that helps you to build a new set of behaviour rules.

ESET MDR

ESET MDR is our 24/7 threat management service designed to provide SMBs with sophisticated protection.

Leverage ESET's cybersecurity expertise with immediate AI-powered threat detection and response. Achieve industry-leading protection without needing in-house security specialists, and eliminate date-organisation bottlenecks that can hinder effective detection and response.

https://www.eset.com/uk/business/services/managed-detection-and-response/

ESET DETECTION & RESPONSE ULTIMATE

ESET Detection & Response Ultimate provides you with what is effectively an Enterprise-class SOC.

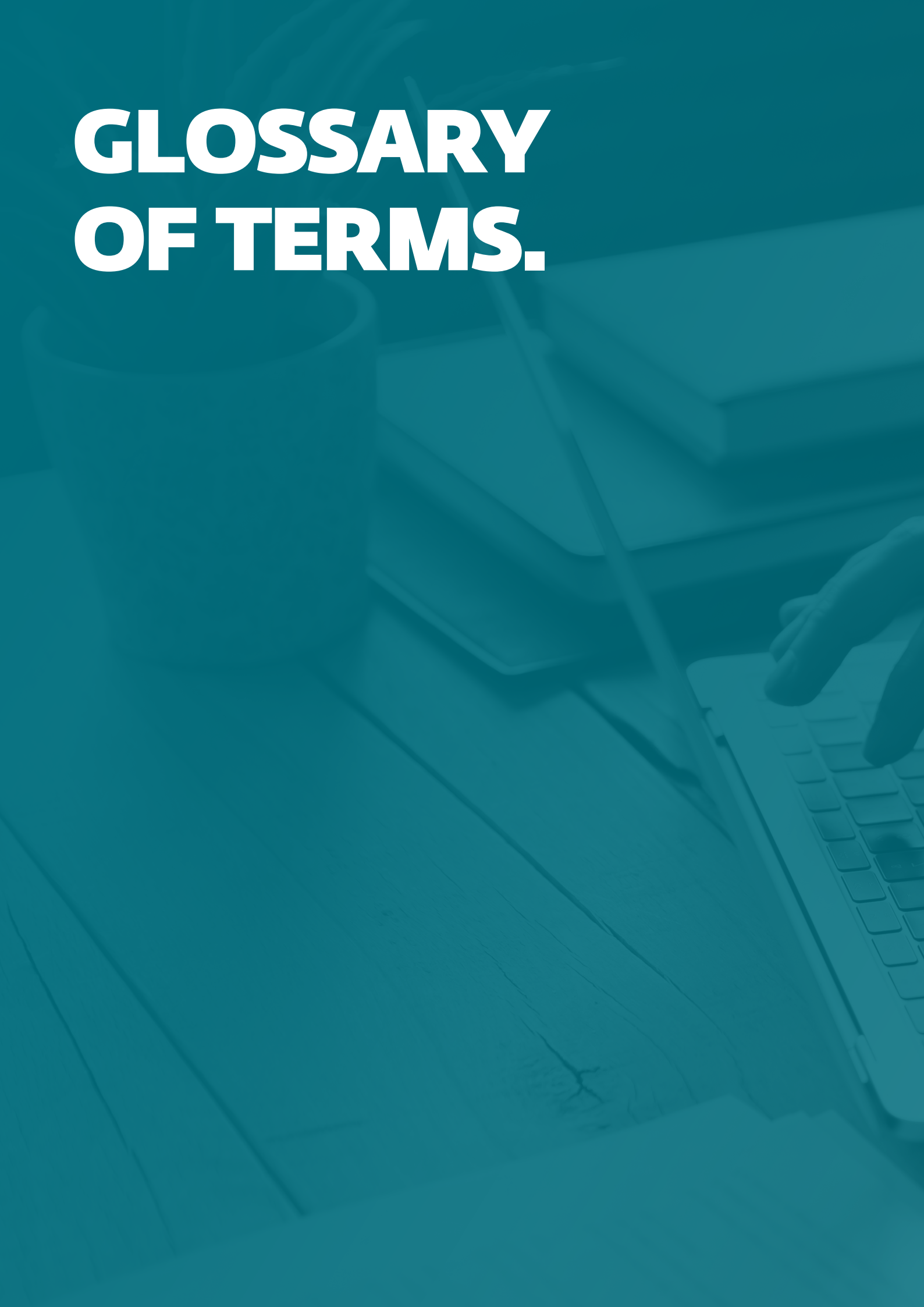
ESET's experienced threat hunters will deliver proactive Threat Hunting and Threat Monitoring, help you to analyse security incidents, and perform immediate mitigation steps. Enhance your security posture with 24/7 human-led service, and get tailored assistance like Digital Forensic Incident Response (DFIR).

"FIRST TO SEE, FIRST TO DETECT"

Emerging threat detection for APTs, cyber crime and zero-days due to our own threat telemetry and threat intelligence research.


PREVENT.
PROTECT.
INSURE.

GLOSSARY OF TERMS.



PREVENT.
PROTECT.
INSURE.

09

GLOSSARY OF TERMS.

SECURITY & PRIVACY BREACH COSTS

This is one of the largest and most critical sections to look for in a cyber insurance policy. It will cover your business for costs arising from dealing with a security breach. For example, notifying customers of a cyber breach, the costs of hiring a call centre to answer customer enquiries, the costs of public relations advice, IT forensic costs, any resulting legal fees or the costs of responding to regulatory bodies.

It will also cover your business against claims of infringement of privacy and associated legal costs in the event of a breach. Usually, this cover not only provides for payments to legitimate claimants but also the legal and regulatory defence costs arising from a privacy breach. This form of cover is especially relevant for businesses that handle or store any personal information from their customers.

POST-INCIDENT SUPPORT

Post-incident support (also known as cyber forensic support) is usually included by insurers as standard. In the event of an IT failure or cyber-attack, this will provide your business with rapid 24/7 support from cyber specialists recommended by your insurer in the period following a cyber incident. These specialists are able to assess your systems, identifying the source of any breach and suggesting preventative measures for the future. In addition, this support can often include advice on your legal and regulatory requirements as well as what steps to take to notify your customers of a data breach.

DAMAGE TO DIGITAL ASSETS

This cover protects your business from damage to digital assets, such as your website or photos. It provides protection against the loss, corruption or alteration of data as well as the misuse of computer programmes and systems. Asset replacement expenses are especially relevant for firms that rely on online business models or on automated manufacturing systems where an incident could inflict significant damage to business operations.

BUSINESS INTERRUPTION

This is an important aspect of most cyber insurance policies. If an IT failure or cyber attack interrupts your business operations, insurers will cover your loss of income during the period of interruption, including if this is caused by increased costs of conducting business in the aftermath of the incident. This can be a critical safety net as you look to recover your normal working pattern.

LIABILITY COSTS

Cyber insurance can provide cover for a business in the event that your digital media presence leads to someone bringing a claim against your business for libel, slander, defamation or the infringement of intellectual property rights. This cover is especially pertinent for companies that rely on the transmission of digital data via email or a website, rely on a large social media or digital content creation business model, or have significant advertising on their site that may lead to a liability.

CYBER INSURANCE - COMMON EXCLUSIONS

It is essential to review not only what is covered by your insurer but also what is excluded. When taking out a policy you must look at exclusions and the definitions and conditions. Many exclusions in cyber insurance are the same as those in other insurance policies such as war and terrorism but there are also some that are specific to cyber insurance, these include:

COURT JURISDICTION

Policies purchased in the UK will normally include territories in the European Union and much of the rest of the world in their cover, but North America is often excluded.

CLAIMS BROUGHT BY RELATED ENTITIES

Whilst cyber insurance will protect your business from loss of customer data and any claims which arise as a result of this loss, policies do not normally include liability claims brought by entities related to your business such as your own employees, contractors and partially owned subsidiaries of your business. For example, if employees seek redress for the loss of their personal information following a data breach, this would not be covered.

BODILY INJURY AND PROPERTY DAMAGE

Cyber insurance policies will replace losses in the digital sphere but will not usually cover damage to physical property or bodily injury (death, sickness, disease or physical injury) which results from a cyber incident, as these are often covered by other insurance policies such as property or liability insurance.

CRITICAL NATIONAL INFRASTRUCTURE

Losses arising from failure of or outage to critical national infrastructure, such as electricity, gas, water, satellite or telecommunications, are excluded. As with war and terrorism, the risk is so large and beyond the capacity of individual insurers.

CYBER WARFARE

Losses to businesses that result from cyber warfare and cyber attacks that may be linked to the actions of a particular country or government are common exclusions due to the risks being so large and beyond the capacity of individual insurers.

FINES, PENALTIES AND SANCTIONS

Cyber insurance will not cover criminal, civil or regulatory fines, penalties or sanctions that your business is legally obliged to pay.

Exclusions will vary between insurers, so it is important to understand terms and conditions. Speak to your broker or insurer directly if you are unsure about any terms.

SMALL AND MEDIUM-SIZED ENTERPRISES (SME)

A term used by the insurance industry for small and medium-sized enterprise businesses whose personnel and revenue numbers fall below US$2 billion.

SMALL AND MEDIUM-SIZED BUSINESS (SMB)

A segment term more generically used for small and medium-sized businesses that, due to their employee size, have different IT requirements — and often face different IT challenges.

FOR FURTHER INFORMATION ABOUT HOW ESET CAN HELP DRAMATICALLY IMPROVING YOUR CYBER RISK POSTURE AND HELP DRIVE DOWN CYBER INSURANCE PREMIUMS CONTACT OUR TEAM:

andrew.owens@riscitsolutions.com
01492 862 780

ACKNOWLEDGEMENTS:

Author: Tony Anscombe - ESET

Contributor: Peter Warren - Future Intelligence

RISC IT SOLUTIONS x ESET® Digital Security
Progress. Protected.