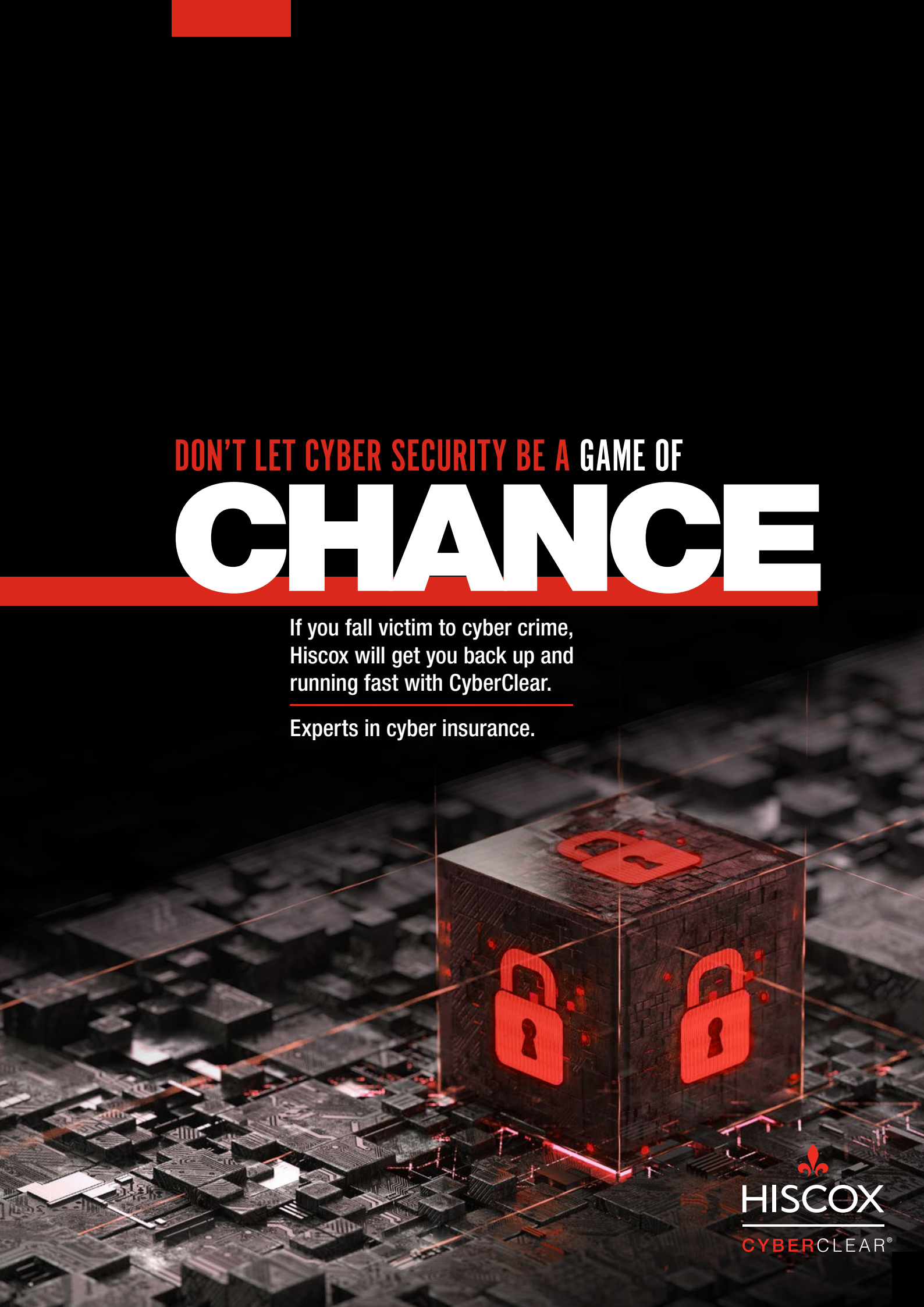
DON'T LET CYBER SECURITY BE A GAME OF CHANCE

If you fall victim to cyber crime, Hiscox will get you back up and running fast with CyberClear.

Experts in cyber insurance.



HISCOX

CYBERCLEAR®

THE CYBER THREAT TO YOUR BUSINESS

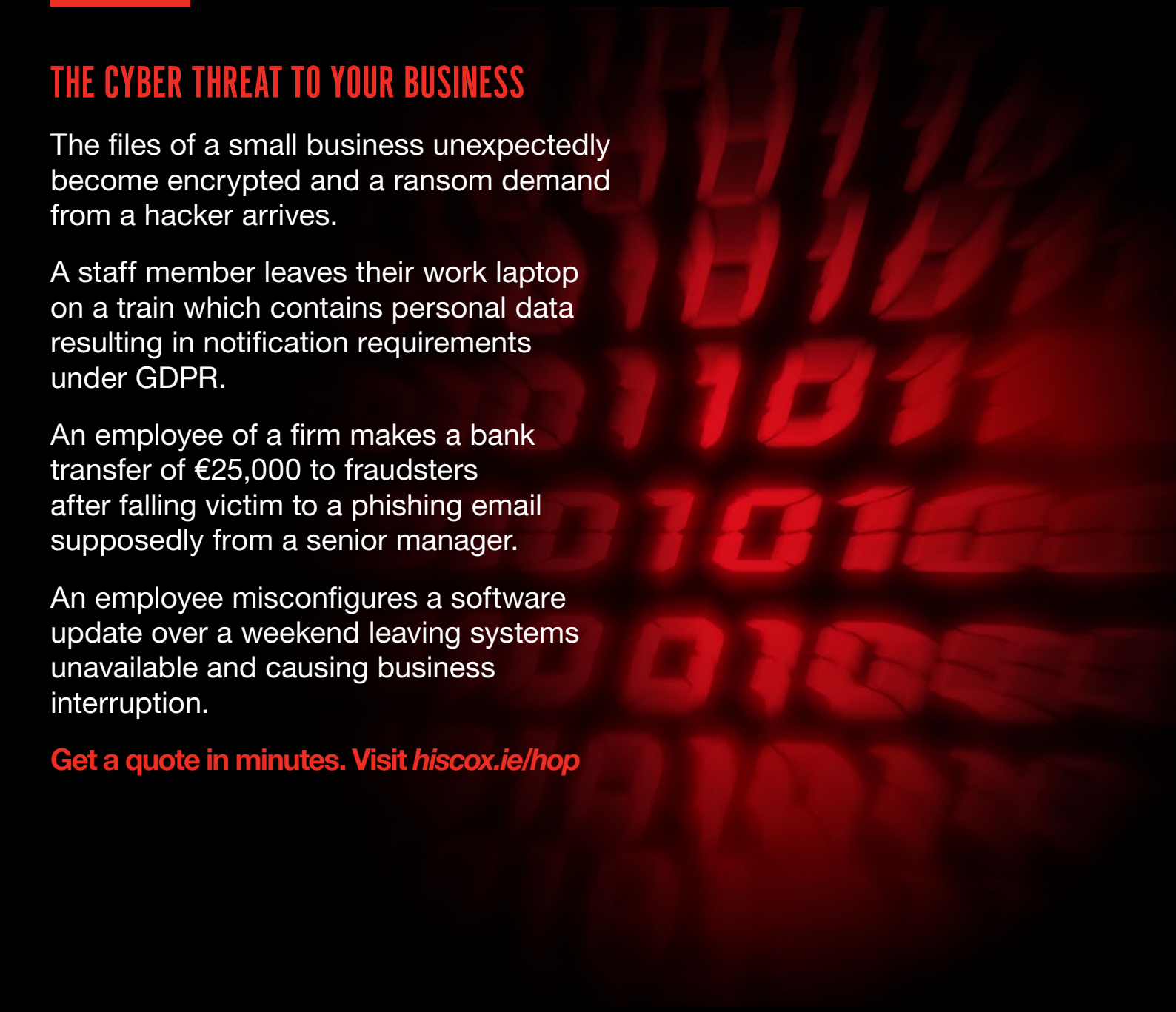
The files of a small business unexpectedly become encrypted and a ransom demand from a hacker arrives.

A staff member leaves their work laptop on a train which contains personal data resulting in notification requirements under GDPR.

An employee of a firm makes a bank transfer of €25,000 to fraudsters after falling victim to a phishing email supposedly from a senior manager.

An employee misconfigures a software update over a weekend leaving systems unavailable and causing business interruption.

Get a quote in minutes. Visit *hiscox.ie/hop*



A cyber attack against your business is no longer a case of ‘if’ but ‘when’.

YOUR BUSINESS IS AT RISK IF...

- you hold customer or employee data such as names, addresses, bank details, passport copies etc.;
- you use a computer to operate;
- you have a website;
- you take payment via card;
- you store data in the cloud or rely on cloud-based services;
- you make electronic payments.

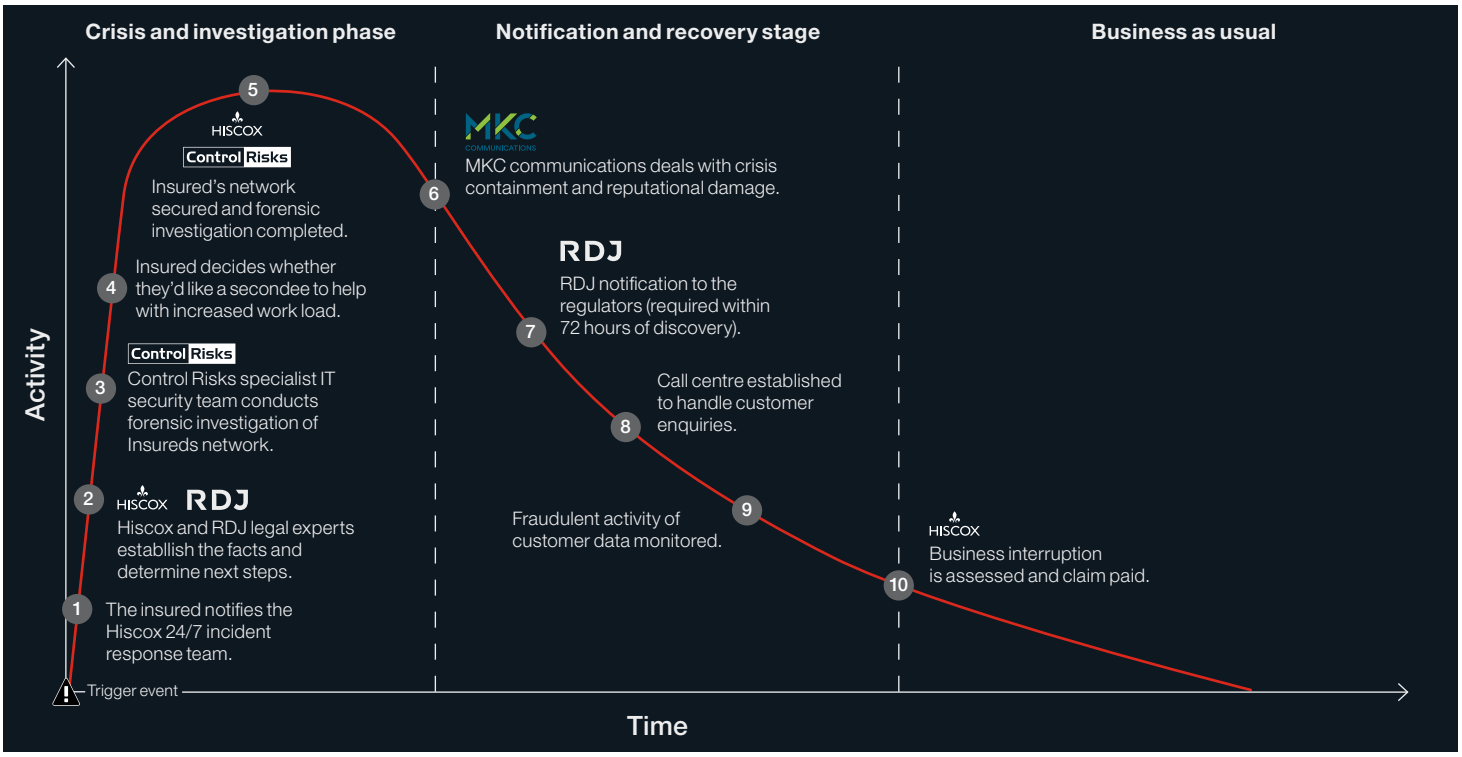
HOW YOU CAN PROTECT YOUR BUSINESS

Hiscox CyberClear has been developed to offer comprehensive, but flexible, cyber cover to Irish businesses of any size – from one-person operations to multinationals – and can include protection against:

- data breaches – where personal or commercial information (electronic or otherwise) is accessed without authorisation;
- security failure – a hacker exploits weaknesses in your security systems, leaving your business exposed;
- cyber attacks – any digital attack against your business;
- extortion – criminals holding your systems or data to ransom or threatening to publish information;
- human errors – mistakes made by staff or suppliers that results in a data breach or system outage;
- business interruption – covering the loss of income that you may suffer from a cyber attack;
- GDPR – covering your liabilities and the cost of defending regulatory investigations after any alleged breach of data protection legislation;
- reputational damage – includes PR and crisis management support, and covers lost revenue or customers;
- financial crime and fraud – the use of the internet to deceive employees, customers or suppliers into transferring money or goods;
- property damage – physical damage to equipment or property resulting from a cyber attack;
- dependent business interruption – covering lost revenue or increased costs incurred if a supplier's systems are taken offline by a cyber incident.

45% of all businesses were hit by at least one cyber attack: Hiscox Cyber Readiness Report 2023.

HOW HISCOX CYBERCLEAR RESPONDS IN AN ATTACK



HISCOX CYBERCLEAR IN ACTION

The business: Technology Company based in Co. Cork

T/O: €11,000,000

Type of attack: Ransomware attack that encrypted three servers and deleted back ups with no possibility to recover. The policy holder was told to pay a large lump sum in order to regain access.

CyberClear response:

Policyholder notified our emergency response team on discovery of attack. Hiscox deployed a response team comprised of

RDJ

- Legal: Assistance with the notification and management of the data breach with the Data Protection Commissioner.

Control Risks

- IT Forensics: Control Risks prioritised containment, eradication and recovery of the businesses data and will investigate what caused the breach.

MKC COMMUNICATIONS

- Public Relations: MKC Communications will develop and release the right message to customers, clients and relevant stakeholders affected by the ransomware attack plus manage media enquires if needed.

CyberClear coverage used in this case:

- IT forensic investigation, eradication and restoration
- Legal advice and crisis management assistance
- Business Interruption
- Ransom payment and ancillary costs i.e. access to cryptocurrency wallets, AML searches etc.
- Data review, notification of data subjects
- Reputational Damage / PR expenses

Outcome:

- Our rapid response and crisis management teams provided immediate response within hours of initial contact and remained with the policyholder to assist for as long as needed.
- Following receipt of the encryption key, the policyholder was able to gain access to their servers and data within a matter of days.
- The client was able to return to approximately 80% of their BAU within one week and back to 100% within two weeks.
- The handling of the data breach with the Data Protection Commissioner took several months and the policyholder was assisted by our legal team at every stage.
- The PR / Communications that were deployed avoided unnecessary reputational damage to the business.
- Matter reported to Gardai.

The business: Management Consultant based in Co. Dublin

T/O: €500,000

Type of attack:

Phishing scam involving an employee who thought they paid a supplier €15,000 30 days previously, but in fact received a fraudulent email impersonating the supplier. The attackers were monitoring emails and intercepted a number of email changing bank details.

Following internal procedures, the policyholder had phoned the threat actor, thinking they were phoning the client who was to be paid and confirmed the new bank details. The payments were then made.

CyberClear Response

Policyholder notified our emergency response line on discovery of attack. Hiscox deployed a response team comprised of

RDJ

- Legal: Assistance with the notification and management of the data breach with the Data Protection Commissioner.

Control Risks

- Control Risks: Priority put in place for containment, eradication and recovery of the email account.
- Full IT infrastructure audit to ascertain where the threat actor had been and what files / email accounts were accessed.

MKC COMMUNICATIONS

- Public Relations: PR comms to communicate the right message to customers, clients and relevant stakeholders affected by the invoice redirection fraud.

CyberClear coverage used in this case:

- IT forensic investigation, eradication and restoration
- Legal advice and crisis management assistance
- Recovery of some of the funds transferred. The amounts not recovered were paid out under the financial crime and fraud extension on the policy.
- Data review of breached email accounts. Data subjects notified where personal data had been breached.
- Reputational Damage / PR expenses
- Repeat event mitigation costs paid

Outcome:

- Our rapid response and crisis management teams provided immediate response within hours of initial contact.
- Business interruption was minimal to the policyholder's business once we were notified. Had they not noticed the missing funds and had we not eradicated the threat, the policyholder could have lost significantly more.
- Partial recovery of the funds transferred were recovered.
- The handling of the data breach with the Data Protection Commissioner took several months and the policyholder was assisted by our legal team at every stage.
- The PR / Communications that were deployed avoided unnecessary reputational damage to the business.
- Matter reported to Gardai.

WHY CHOOSE HISCOX CYBERCLEAR?

Hiscox CyberClear will help to protect your business from the financial and reputational costs of a cyber incident. If the worst should happen, you know that you will have the reassurance, support and advice from Ireland's market-leading cyber insurer.

Access to the best experts in the business

Through Hiscox CyberClear you have instant access to a network of market-leading expertise from IT forensics to privacy lawyers and reputational experts.

Future proofed

Not only will Hiscox CyberClear cover you for today's risks, our extensive policy wording means that you're protected from emerging risks, threats and digital attacks that criminals may adopt in the coming years.

Breadth of cover

Hiscox CyberClear covers the financial cost and business impact of an incident, as well as offering a range of additional features; from worldwide cover as standard, key person cover and no overall policy aggregate limit, to a 72-hour excess waiver, directors' personal cover and no retroactive date.

Simple to understand

Hiscox CyberClear is just that… clear. There are no complicated modules.
You know what you are buying and what you are covered for.

We know what we're doing

Hiscox has been providing this type of insurance since 1999, and has handled thousands of claims in that time. We know the risks your business faces – whether you're a two-partner accountancy firm or a tech business with hundreds of employees – and how best to manage and mitigate them.

VALUE ADDED SERVICES

Hiscox CyberClear Academy

Prevent a cyber incident happening through access to our online suite of cyber security training modules for you and your employees. Access to the academy is free to all Hiscox CyberClear customers with a revenue of less than €10 million.

HISCOX
CYBERCLEAR®
ACADEMY

HISCOX CYBERCLEAR: YOUR QUESTIONS ANSWERED

Why should I buy insurance for cyber risks?

You're most likely covered for risks like fire, flood and professional negligence but you are just as likely to suffer a cyber attack which can lead to loss of business, revenue and reputation; significant extra costs involved in dealing with the attack; and, regulatory penalties.

Doesn't my business insurance cover this risk?

No. Your standard business insurances will not provide the comprehensive protection you need against a cyber attack.

Hackers aren't interested in me, are they?

Much of the criminal activity online isn't specifically targeted at a particular business; those behind the attacks will often use tools to search the internet for any system that has a vulnerability. They will then exploit that vulnerability, regardless of who is sitting behind it.

I'm not an online business, so is this cover relevant for me?

A lot of companies identify as 'offline' and assume they don't need cyber insurance. However, nearly all Irish businesses rely on some form of digital communication or services, such as staff email addresses, websites, online banking and the ability for customers to shop online, which exposes them to cyber security risks.

What does Hiscox CyberClear offer that other cyber insurance policies don't?

Hiscox CyberClear offers the broadest cyber cover available in the market, accompanied by a team of experts who will get your business back up and running fast in the event of an attack.

Does the policy only protect against hacking attacks?

No. Whilst cyber criminals are one of the biggest sources of claims, issues can also occur from human error, such as sending an email to the wrong address, leaving a briefcase on a train, or mistakes in configuring a system.

I don't hold any customer personal data – do I still need this cover?

The definition of personal data under GDPR is very broad, and would still include things like a business email address. You also need to consider suppliers' details, as well as information relating to employees (past, present and prospective). Additionally, the majority of claims that we deal with do not involve a breach of personal data, but loss of funds, data corruption, or system downtime – all of which you may be vulnerable to even if you do not hold much personal data.

For more information please contact your insurance broker.

Hiscox SA
The Observatory
7-11 Sir John Rogerson's Quay
Dublin 2
D02 VC42

T + 353 (01) 238 1810
www.hiscox.ie

20103 06/19

HISCOX

CYBERCLEAR®