howden

Making sense of cyber risk

A simple guide to protecting your business

Introduction

Businesses often underestimate the risks posed by cyber threats. Individuals and companies of all sizes, in every industry, are increasingly relying on technology and data in some way or another.

Cyber attacks can vary in terms of persistence, sophistication and impact. They can no longer be ignored.

This guide has been put together to demystify some of the key elements of cyber risk, so you can take the necessary steps to protect your business.

61%

of firms reported a cyber-attack last year, up from 45% the previous year*

*Source: Hiscox Cyber Readiness Report 2019

In this guide

01

Assess

- Potential cyber risks to your business
- Key threats facing businesses

02

Protect

- Cyber security framework

03

Respond & Recover

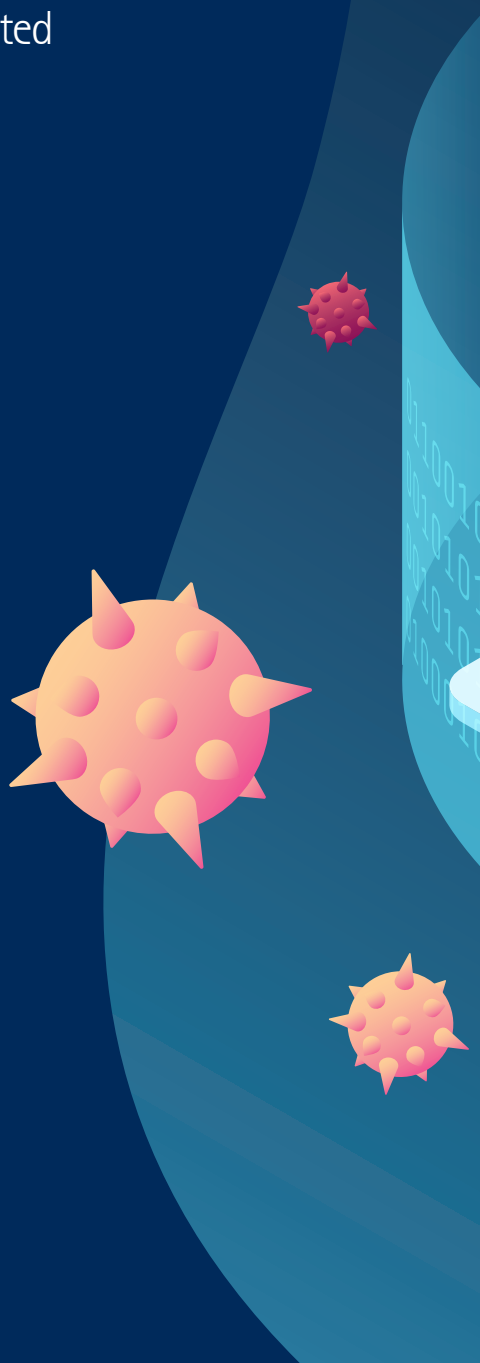
- Practical advice for business resilience
- Cyber Insurance as a risk management tool

04

Cyber myths de-coded
Definitions

Assess

- Establish your internal business risks
- Understand how your business can be targeted



Potential cyber risks to your business

People

Human error and insider threat can compromise your cyber security. High profile board members can also make businesses a more attractive target.

Information/data

If your business holds any sensitive or personal data you face an increased cyber security risk.

Intellectual property/trade secrets

This can be one of your most vulnerable assets, putting you at high risk from hostile insiders and external attackers.

Websites

Cyber criminals are constantly targeting online vulnerabilities to spoof websites, steal data and disrupt on-line activity.

Internet of Things (IoT)

Connected devices can be exploited as a way into your network. Even unsuspecting items such as kettles or printers are a risk.

Information and operational technology

Any business that uses technology or links operational technology to their networks has an increased cyber risk.

Contracts

Consider any contractual obligations to cyber security between your business, clients and third parties.

Key threats facing businesses

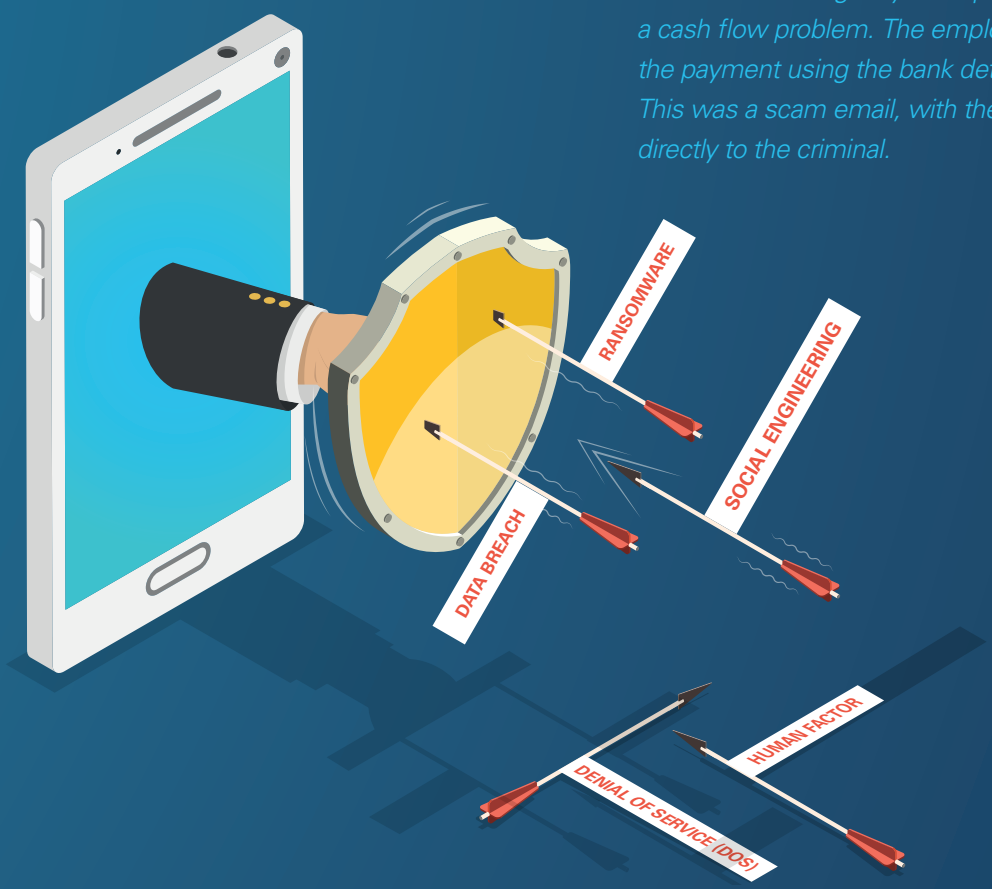
Ransomware

Once a network is infected with ransomware (e.g. delivered via email attachments or links), the malware denies you access to your systems and files with a financial and/or destructive objective.

Social Engineering

Covering a range of malicious activity, influencing users through psychological manipulation to perform actions or disclose confidential information, often through emails, links or websites.

Example: *An employee in the accounts department received what appeared to be a genuine email on a Friday afternoon from a longstanding supplier asking if payment could be made urgently to help them out of a cash flow problem. The employee made the payment using the bank details provided. This was a scam email, with the money going directly to the criminal.*



Data Breach

Confidential data is accessed and in some cases used to extort companies, or the data is just sold on the dark web. Data could include personal banking information, Personally Identifiable Information or Intellectual Property.

Example: *Following a cyber attack, a retailer needs to notify all customers affected that their personal information may have been exposed. As well as the cost of sending out thousands of notifications, the company has to cope with the extra volumes of telephone calls, emails and potential third party claims for damages.*

Human Factor

Whilst there is a malicious element in some cases, the majority of incidents are non-malicious and as a result of a lack of awareness, training or sometimes concentration.

Examples of cyber security threats caused by human factors include:

- Poor password security
- Accidentally clicking on malicious links and attachments
- Mis-delivery of sensitive information.

Distributed Denial of Service (DDoS)

An attack that aims to make a website or on-line services unavailable/ inoperable by overloading it with traffic.

Example: *A small online retailer makes the majority of their turnover in a short window of time with seasonal goods. When their e-commerce site crashes it is expected that a competitor has used a botnet to shut the business down during a busy period, leading to severe business interruption and a substantial impact on company finances.*

WannaCry

A ransomware attack that spread across 150 countries in 2017 and affected over 200,000 computers globally. The attack affected many industries, locking users out of systems and demanding a ransom. This attack hit a third of hospital trusts in the UK, costing the NHS alone an estimated £92 million.

Protect

- Determine your risk appetite
- Prioritise your risks
- Take steps to manage your risks

Cyber security framework

Basic

Extending security to include third party risk

- Employee education and awareness training
- Home and mobile working policy and guidelines
- Cyber scenarios are considered and added to your business continuity plan
- Critical Service Providers and Third Party Vendors are cyber security checked.
- Cyber Essentials PLUS Certificate

Essential

Protecting against the most common cyber attacks, such as malware & Business Email Compromise

- Firewalls to ensure network security
- A secure passwords policy and two- factor authentication
- Restricted user access and management of user privileges
- Malware protection systems
- Up-to-date operating systems, apps and software
- Backed up data
- Cyber Essentials Certificate
- **A Cyber Insurance policy**

Embedded

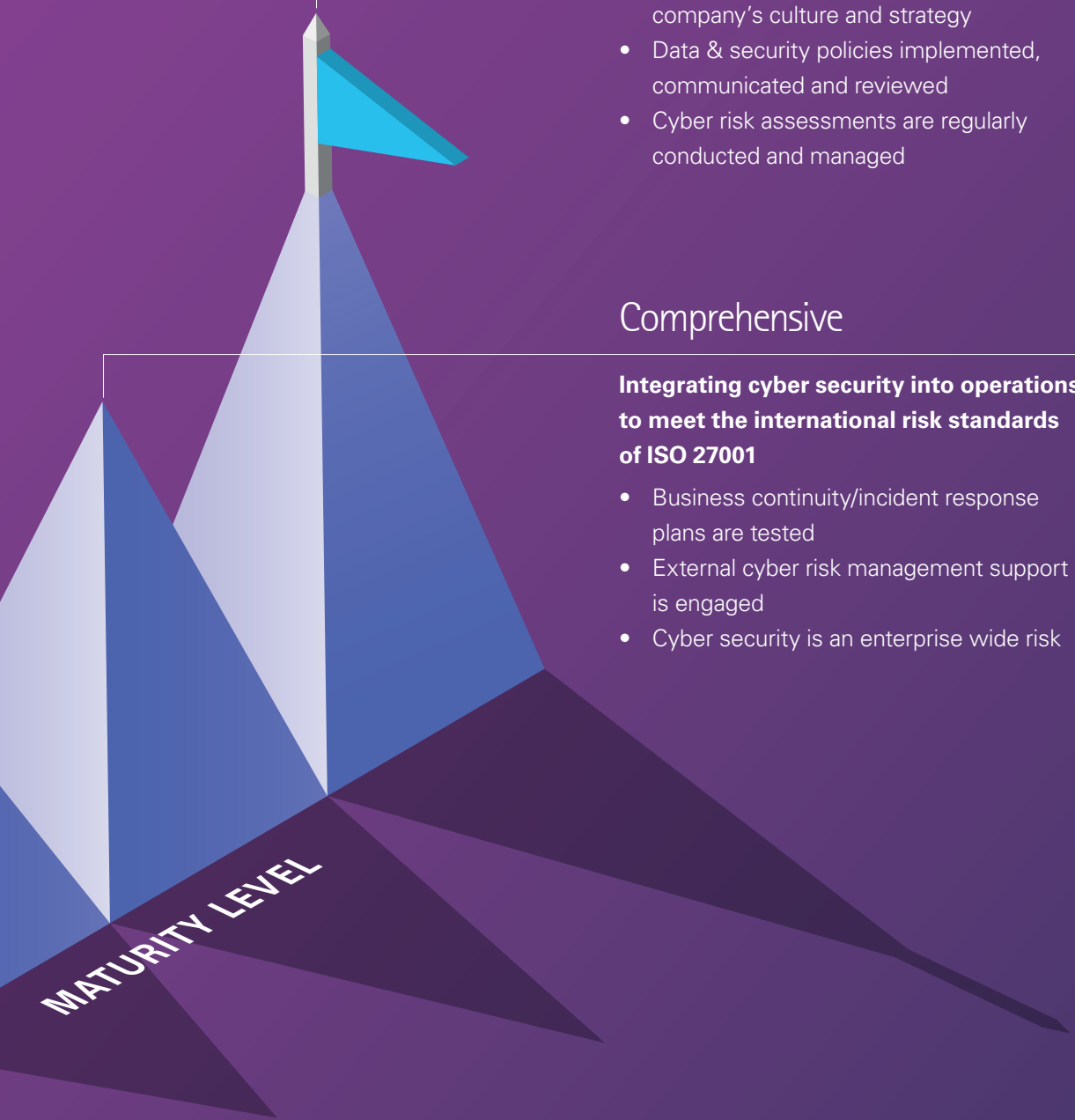
Develop a cyber security governance framework that is aligned to the function, goals and objectives of your business

- Cyber security is embedded in the company's culture and strategy
- Data & security policies implemented, communicated and reviewed
- Cyber risk assessments are regularly conducted and managed

Comprehensive

Integrating cyber security into operations to meet the international risk standards of ISO 27001

- Business continuity/incident response plans are tested
- External cyber risk management support is engaged
- Cyber security is an enterprise wide risk



Respond and Recover

- Have plans in place should things go wrong
- Restore normal operations and service

Practical advice for business resilience

Do

- Conduct regular **security assessments** and keep all IT software updated
- Use **secure passwords** and update them regularly
- Regularly **review** access and administration rights of employees
- Create a positive security culture. **Educate** employees about different cyber threats as they are one of the best lines of defence
- Have an **incident response plan** in place, with a copy kept offline in case you can't access your systems. Have designated people responsible for implementing the plan in the event of an attack to ensure the business responds quickly
- **Back up** everything, ensuring a recent copy is kept offsite and offline
- Ensure physical security is maintained at your premises, restricting access to data, portable equipment and server rooms etc.

Don't

- Be **complacent** about cyber security, keep it front of mind
- Solely **rely** on your IT team and antivirus programmes to protect you against cyber threats
- **Negotiate** with cyber criminals. Paying a ransom wont always end in regaining access, it can fund terrorism and may only fuel them to continue attacking companies – seek specialist help!
- **Destroy** any logs or computers after a cyber attack, they may be needed by experts for any investigations into the attack
- Forget to **remove** former employees access to any systems or data immediately to avoid malicious intent
- Forget to pass your cyber security requirements onto your **critical service providers and third parties**

Cyber Insurance as a risk management tool

Risk management involves deciding which risks to manage, avoid, accept, control or **transfer**.

Risk transfer

A cyber incident can affect your ability to operate, impact your financials, and damage your long-term reputation. Whilst Cyber Insurance will not protect you from an attack, it allows for some of the financial risk to be transferred and assist with mitigating disruption.

A Cyber Insurance policy typically covers:

Incident response

Specialist assistance when responding to an incident including:

- IT forensics to investigate, control and remove any threat
- Legal specialists to assist in notifying affected parties and regulators of a breach
- PR services to manage any reputational damage

Business continuity support

- Business interruption cover for loss of income incurred as a result of network interruption or outage following a cyber event, during the indemnity period
- Cover for the cost of repair, restoration or replacement of digital and data assets
- Assistance from skilled professionals in the event of ransom demands

Third party liability

Defence costs and settlements arising from your legal liability for;

- Claims made against you or investigations following a privacy breach
- Defamation claims due to your website or social media
- Breach of network security claims

The cost

Premiums depend upon several factors including the business annual revenue, industry sector, and the type of data held.

At Howden we aim to support you in your cyber journey by understanding the risks that are unique to your business and negotiating the most appropriate coverage and premium on your behalf.

We take an integrated, holistic approach when defining our client's business risks and ensure that we work with reputable insurers with proven global incident response services. Our strong, experienced claims handling team are also on hand to support you during the claims process, should an incident occur.

Cyber myths de-coded

Cyber Insurance doesn't pay out

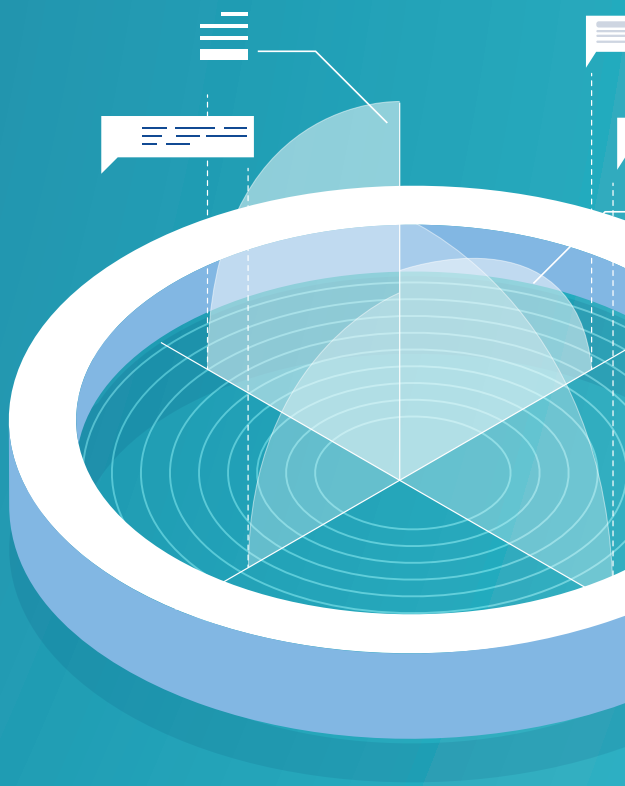
Confusion has arisen due to claims relating to cyber incidents being rejected, as they were brought against other classes of insurance policy such as Property or Kidnap & Ransom, which are not designed to cover the full range of cyber threats.

Cyber-attacks only affect big businesses

A recent Verizon report found 58% of cybercrime victims were categorised as small businesses. Smaller organisations often lack the resources necessary to invest in IT security or provide cyber training for their staff, making them an easier target.

We don't collect any sensitive data

Any business that relies on a computer system to operate has a risk. Two common sources of cyber claims are from criminals using fraudulent emails to request the transfer of funds, or ransomware attacks causing severe business interruption and potentially large financial losses.



We outsource our IT operations so we don't have an exposure

Outsourcing to a third party doesn't mean outsourcing your responsibilities for the protection of data. If your IT service provider is compromised it could significantly impact your business operations and financials too. Even if you claim against them for damages, it could take time and their liability to you could also be limited.

We don't need Cyber Insurance, we invest in IT security and my IT director can solve any cyber issue

You can have the best defences in the world, but IT security can't always protect you from all threats including the human factor or exposure via third party vendors or suppliers. They say you are only as strong as your weakest link. Whilst your IT director will be critical in the incident response, they will unlikely have the experience or specialist knowledge that might be required during a cyber attack, such as knowledge of hackers, variants of malware, how to negotiate ransoms or the dark web.

Definitions

Botnet
A network of infected devices, connected to the internet, used to commit coordinated attacks without the owners knowledge.

Brute force attack
Using a computational power to automatically enter a huge number of combination values, usually in order to discover passwords and gain access.

Cryptojacking
The unauthorised use of a computer, tablet, or mobile phone to mine for cryptocurrency. They hijack a targets processing power to mine cryptocurrency on the hackers behalf.

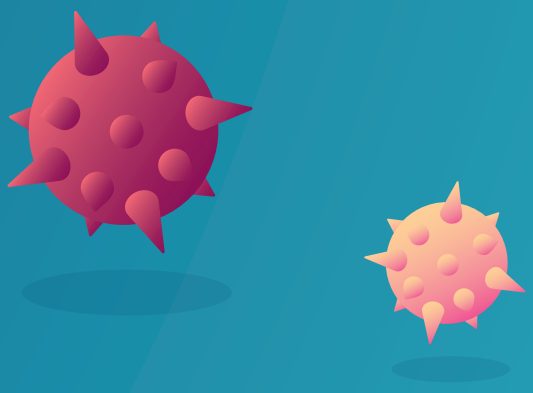
Denial of Service attack (DoS)
When legitimate users are denied access to computer services or resources, usually by overloading the service with requests.

IP spoofing
A tactic used by attackers to supply a false IP address in an attempt to trick the user into believing it's a legitimate actor.

Island Hopping
Criminals infiltrate their target organisation through smaller companies that work with the target. These smaller companies – such as HR and payroll, marketing or healthcare firms, often have more vulnerable security systems than the larger target organisations.

Keylogger
A type of software or hardware that tracks keystrokes and keyboard events to monitor user activity.

Malware
Software that is specifically designed to disrupt damage or gain unauthorised access to a computer.



Man in the middle attack
When a communication between two parties is intercepted by an outside entity via poorly secured Wi-Fi routers. They can eavesdrop on your private conversations and intercept data.

Pharming
An attack on network infrastructure where a user is redirected to an illegitimate website, despite having entered the right address.

Phishing
Untargeted, mass emails sent to many people asking for sensitive information or encouraging them to visit a fake website.

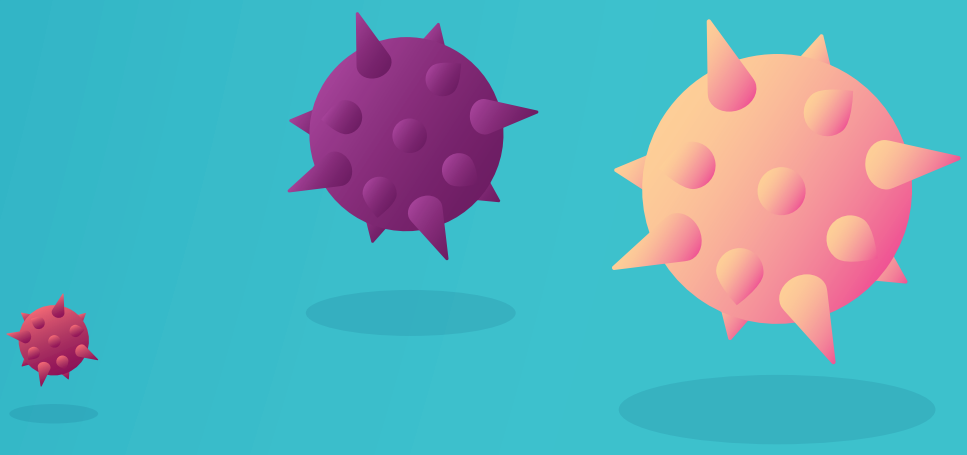
Ransomware
Malicious software that makes data or systems unusable until the victim makes payment.

Social engineering
Manipulating people into carrying out specific actions, or divulging information to an attacker.

Spoofing
Disguising a communication from an unknown source as being from a known, trusted source.

Watering hole attack
The attacker observes websites often visited by a particular group of people, and infects these websites with malware.

Whaling
Highly targeted phishing attacks that are aimed at senior executives.



howden

Howden Insurance Brokers (S.) Pte. Limited
61 Robinson Road, #07-01
Robinson Centre
Singapore 068893

Tel: +65 6258 1919

www.howdengroup.com/sg-en

Part of the Hyperion Insurance Group