COMMERCIAL BANKING

Cyber risk guidance

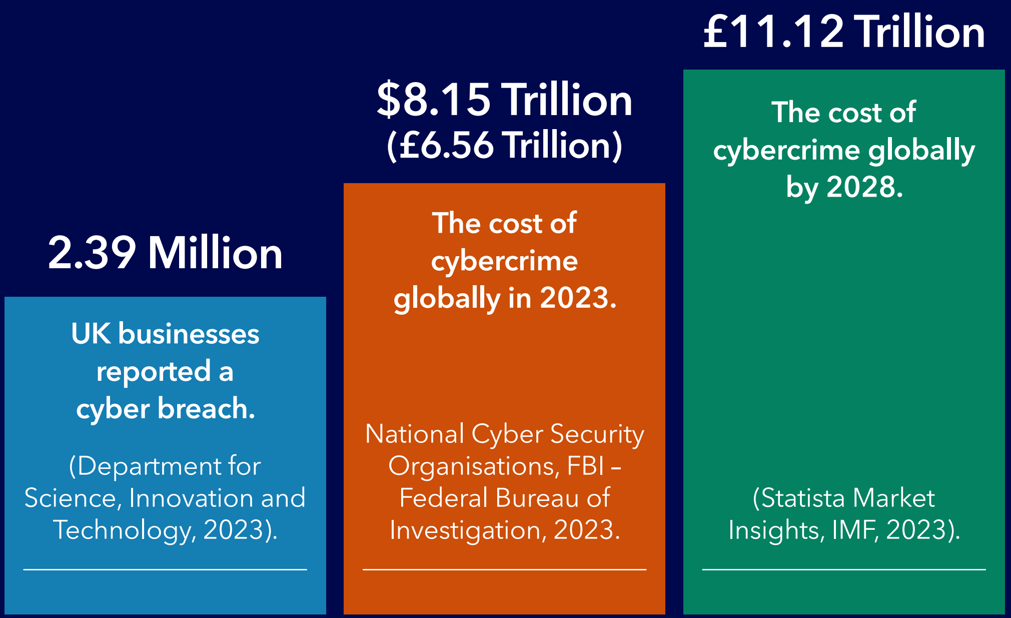
BANK OF SCOTLAND

By the side of business

Cyber risk guidance

Threats from cyber attacks on businesses are constantly growing.

This guide helps you understand and tackle these threats. Discover ways to protect your business, employees, and assets.



2.39 Million

UK businesses reported a cyber breach.

(Department for Science, Innovation and Technology, 2023).

$8.15 Trillion (£6.56 Trillion)

The cost of cybercrime globally in 2023.

National Cyber Security Organisations, FBI – Federal Bureau of Investigation, 2023.

£11.12 Trillion

The cost of cybercrime globally by 2028.

(Statista Market Insights, IMF, 2023).

> Cybercrime is a dynamic threat that can have a major impact on an organisation of any size.
>
> Businesses must prepare and adapt rapidly to protect, respond and recover from cyber attacks. It's crucial to consider operational, media, legal and financial planning and IT resilience.
>
> This guide is designed to support our clients in making their business more secure and more resilient and ultimately to help Britain prosper.

Giles Taylor
Head of Resilience and Cyber Risk,
Lloyds Bank Commercial Banking

Contents

Click the home button at the top of the page to return to this contents page, wherever you are in the document.

Cyber threats and attacks – protecting your business

Cyber threats target any combination of information technology, digital assets, the data held on them and the services they run or provide.

Constantly evolving, the threats mostly involve attacking the confidentiality, integrity or availability of data or systems.

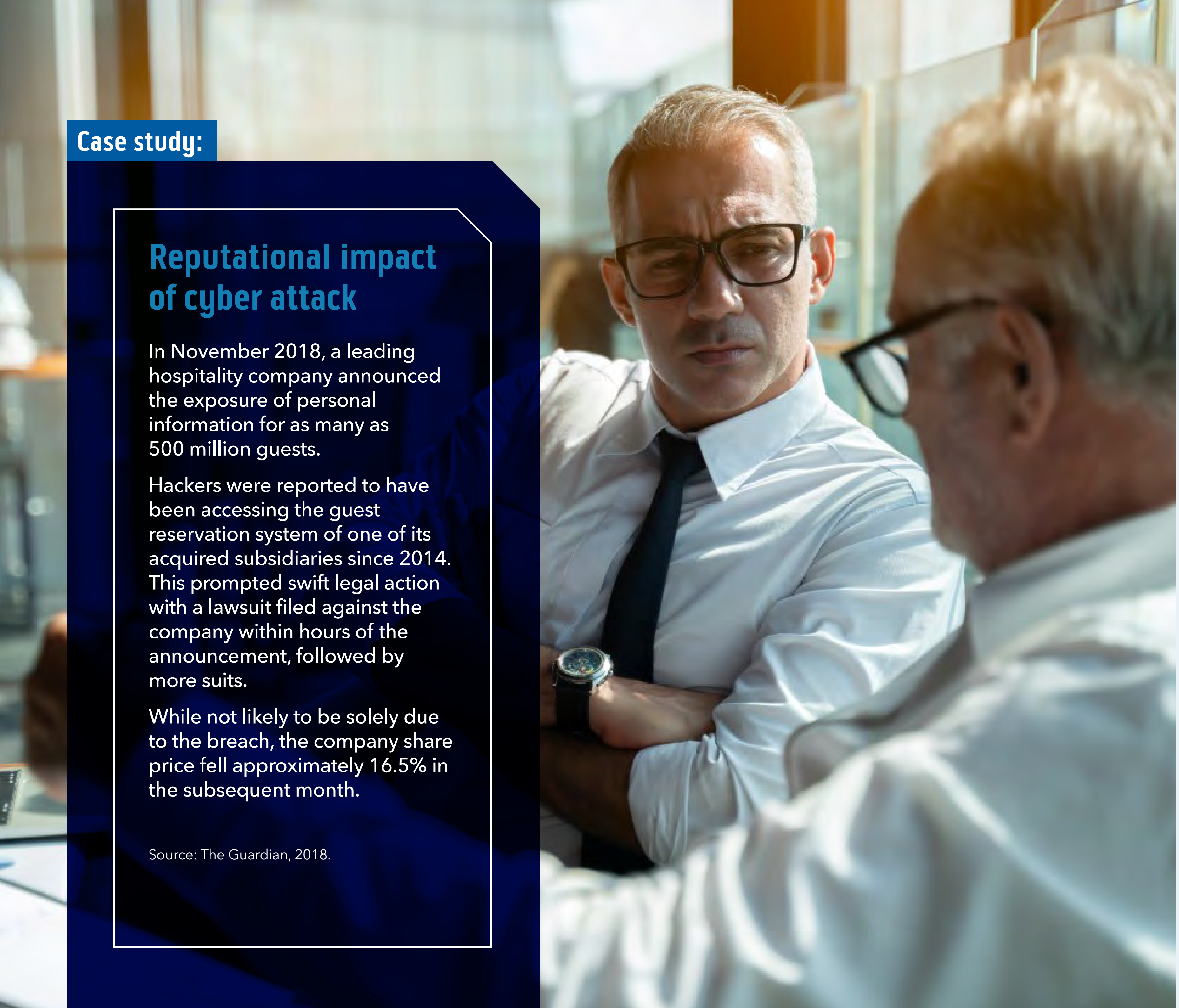
Cyber attacks can have a significant impact on businesses, such as reputational damage to a brand through the loss of customer confidence.

Other consequences can include legal or regulatory sanctions. Particularly if large quantities of customer data are stolen and regulators find that business controls for data privacy are not adequate.

The Attackers

Generally grouped into categories based on their motivations and capabilities.
Known as 'Threat Actors' they include:

Hacktivists	These groups tend to be loosely organised and target websites to deface them or take them offline. They are groups or individuals politically or ethically motivated that use cyber attacks to get a political message across.
Criminals and Organised Criminal Groups (OCGs)	Stealing billions of pounds from consumers and businesses each year, this group can range from a few individuals operating on their own to large OCGs. Financially motivated, they often use phishing and malware to get log-in credentials to online banking services or accountancy systems to steal money.
Nation States/State-Sponsored Attackers	Government-funded and guided, these attackers focus primarily on the theft of intellectual property or confidential government information. Often well-funded and well-resourced, they attract high-level talent to create and deliver the most sophisticated threats.
Insiders	Attacks can also come from within. Sometimes third-parties will threaten or manipulate people to act maliciously.



Case study:

Reputational impact of cyber attack

In November 2018, a leading hospitality company announced the exposure of personal information for as many as 500 million guests.

Hackers were reported to have been accessing the guest reservation system of one of its acquired subsidiaries since 2014. This prompted swift legal action with a lawsuit filed against the company within hours of the announcement, followed by more suits.

While not likely to be solely due to the breach, the company share price fell approximately 16.5% in the subsequent month.

Source: The Guardian, 2018.

Cyber threats and attacks

Vulnerabilities

Cyber threat management

(Spear) phishing

Distributed Denial of Service attack (DDoS)

Ransomware

Website attacks

Advanced persistent threats (APTs)

Protect your business from cyber threats

Cyber glossary

Vulnerabilities – how the attackers get in

Attackers exploit vulnerabilities in your systems, processes, or people. These can be due to:

Flaws	Software flaws or unintended functionalities, which cyber attackers regularly exploit in their attacks. Fixing known flaws is a process known as 'patching'. Flaws can often go undetected for significant periods, until a vendor releases a fix or patch.
Features	An attacker can misuse functionality intended to automate or simplify the use of computers or mobile devices to breach a system. For example, the macro feature in spreadsheet and word-processing applications enables a user to automate often performed tasks or perform complex calculations. Attackers also use this functionality to instruct the computer to perform unwanted tasks, such as downloading malware or recording keystrokes. Businesses can protect against attacks of this type by disabling non-essential functions on PC and mobile devices, such as macros or Bluetooth.
User error	Even if vulnerabilities are 'patched' or disabled through a secure build, a significant vulnerability can stay through user error. That is a systems administrator who enables vulnerable features by mistake or fails to fix a known flaw. The users' actions, whether carried out intentionally or not could reveal protected information.

Attackers actively pursue and exploit vulnerabilities

There is a criminal market that buys software flaws with 'zero-day' vulnerabilities. Recently discovered vulnerabilities, not known to the public fetch hundreds of thousands of pounds.

Cyber threat management – how to protect your business

User education and awareness

- Produce policies that cover acceptable and secure use of your business systems.
- Set up a training programme.
- Make sure you maintain user awareness of the cyber threats.

Network security

- Protect your networks against external and internal attack.
- Manage your network perimeter.
- Filter out unauthorised access and malicious content.
- Monitor and test security controls.

Secure configuration

- Create a system inventory and define a baseline build for all IT devices.
- Apply security patches to maintain the secure configuration of all IT systems.

Removable media controls

- Produce a policy to control all access to removable media.
- Limit media types and use.
- Scan all media for malware before importing onto the corporate system.

Social media

- Put in place a social media policy for employees.
- Educate users to consider what they post online, calling out the risks from discussing work-related topics on social media.
- Make sure they know that content they post could result in them being the target of a (spear) phishing attack.

Cyber threat management – how to protect your business

Malware protection

- Produce a relevant policy and set up anti-malware defences that are applicable and relevant to all business areas.
- Scan for malware across the organisation.

Incident management

- Set up an incident response and disaster recovery capability.
- Produce and test incident management plans.
- Provide specialist training to the incident management team.
- Report criminal incidents to law enforcement.

Monitoring

- Set up a monitoring strategy and produce supporting policies.
- Continuously monitor all IT systems and networks.
- Analyse logs for unusual activity that could indicate an attack.

Managing user privileges

- Set up account management processes. Limit, control and monitor privileged accounts.
- Control access to activity and audit logs.

Home and mobile working

- Develop a mobile working policy and train staff to adhere to it.
- Apply the secure baseline build to all devices. Protect data both in transit and at rest.

> Set up an effective governance structure and determine risk appetite.

> Maintain the Board's engagement with cyber risk.

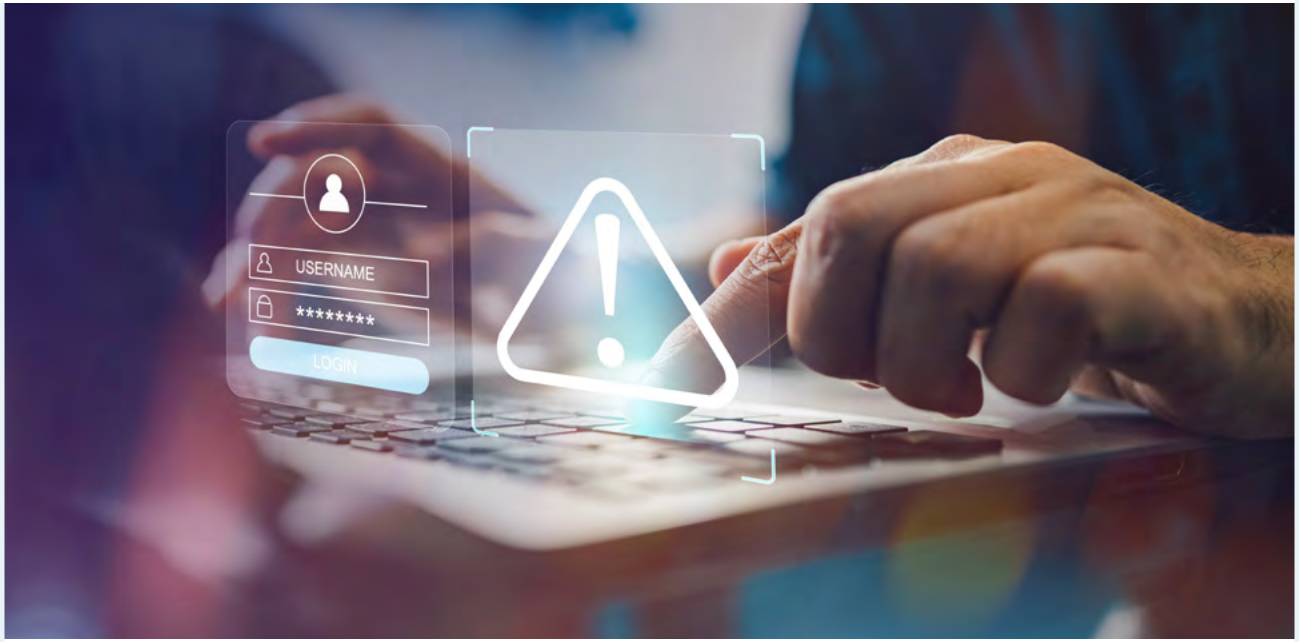
> Produce supporting information risk management policies.

(Spear) Phishing – targeting your employees

What is phishing?

Phishing is an email scam. Scammers pretend to be trusted organisations – like banks, to steal personal info or passwords. They send urgent emails asking you to click a link, which leads to a fake website.

This website will then entice the victim to enter log-in credentials or download malware.



What is spear phishing?

Spear phishing is a targeted form of a phishing attack.

Scammers pose as colleagues within your organisation. They trick you into actions like opening attachments or making payments.

Spear phishing is often a component used in more complex attacks, known as advanced persistent threats (APTs).

Cyber threats and attacks
Vulnerabilities
Cyber threat management
(Spear) phishing
Distributed Denial of Service attack (DDoS)
Ransomware
Website attacks
Advanced persistent threats (APTs)
Protect your business from cyber threats
Cyber glossary

(Spear) Phishing – targeting your employees

How to protect your business

Employee education and awareness

Educate on the risks associated with opening files or visiting websites through links in emails – even when the email appears to originate from a colleague.

Consider implementing a policy for employees around what they share on social media – which is a rich source of information for spear-phishers.

User access controls

Restrict users' permissions, limiting privileges to those needed to perform their role.

Restrict privileged accounts and the ability to run executable files*, especially if not needed for their role.

* Executable file – a computer file that contains a program and runs that program when it's opened. Typically .exe files in Windows Operating Systems.

Secure configuration

Known as 'hardening', minimise the potential attack surface on users' devices by having a secure build.

Make sure (among other things) that you remove unnecessary software and default user accounts.

Software patch management

Apply patches as early as possible (after testing), to limit the exposure to known software vulnerabilities.

Consider deploying technical controls, which could include:

Malware protection

Anti-malware defences to scan emails and attachments for malicious code.

Produce a relevant policy and set up anti-malware defences that are applicable and relevant to all business areas.

Consider having a separate device to carry out online banking activities that don't have access to email systems to minimise direct malware infection risk.

Scan for malware across the organisation.

Web Traffic Protection

Web content and site categorisation service to restrict access to websites and real-time scanning of web traffic for malicious code.

Cyber threats and attacks
Vulnerabilities
Cyber threat management
(Spear) phishing
Distributed Denial of Service attack (DDoS)
Ransomware
Website attacks
Advanced persistent threats (APTs)
Protect your business from cyber threats
Cyber glossary
< >

Case study:

Simple but effective

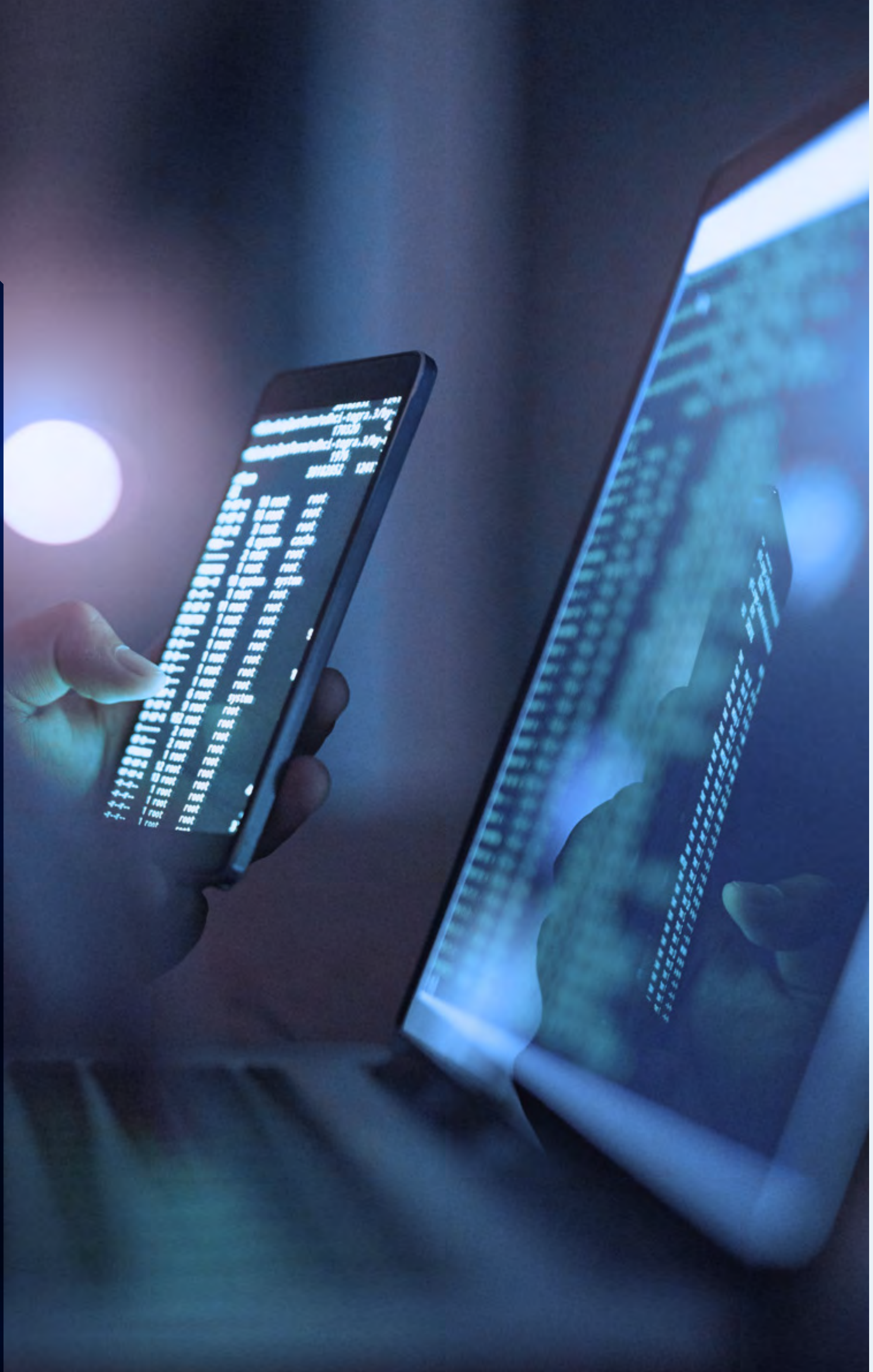
Between 2015 and 2018, a global cyber criminal group targeted more than 100 companies worldwide using tailored spear phishing emails.

Once inside a victim company's network they sought access to point-of-sale (POS) systems. They then stole payment card details of customers and sold them later on underground marketplaces.

Allegedly the group stole more than 15 million customer payment card records from over 6,500 individual POS terminals at more than 3,600 separate business locations.

This led to the loss of tens of millions of dollars.

Source: Security Affairs, 2018.



Cyber threats and attacks

Vulnerabilities

Cyber threat management

(Spear) phishing

Distributed Denial of Service attack (DDoS)

Ransomware

Website attacks

Advanced persistent threats (APTs)

Protect your business from cyber threats

Cyber glossary

Distributed Denial of Service attack – attacking your online availability

What is a Distributed Denial of Service (DDoS) attack?

A DDoS attack aims to overwhelm an online resource, like a website, by flooding it with internet traffic. The attacker's goal is to hide their origin and create massive traffic volume against the target.

A DDoS attack is a specific class of Denial of Service. The attack will originate from multiple sources, often using a huge network of computers infected with malware, known as a 'botnet'.

Historically, only a skilled individual was able to conduct a DDoS attack as they needed a keen understanding of internet and system infrastructure.

Over recent years tools have been made available on the Dark Net (refer to glossary) for a relatively modest fee. This has allowed unskilled individuals to hire botnets and conduct attacks on their choice of target.

The strength and ease of administering a DDoS attack has also increased. Partly thanks to competition among hackers, the cheap cost to launch ($25 per hour) and also powering attacks through Internet of Things (IoT) devices.

Cyber criminals threaten companies with DDoS attacks unless they pay a ransom. These attacks are politically or ideologically motivated.

The victim company will usually receive extortion emails demanding payment (usually in the cryptocurrency Bitcoin).

They use DDoS attacks as a smokescreen to distract defences from other attacks like a data breach or unauthorised access to a network.

Distributed Denial of Service attack – Attacking your online availability

How to protect your business?

There is no one way to defend against a DDoS attack. The approach and sophistication of potential attacks will vary, based on:

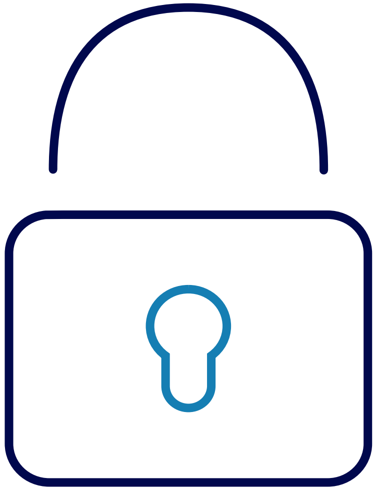
- What the target organisation is trying to defend.
- Their infrastructure.
- The controls they have in place.

In an attempt to counter the effectiveness of an attack, cyber criminals combine various mitigation techniques these include:

- Buying excess bandwidth from your Internet Service provider.
- Configure routers and firewalls to stop simple attacks. Filter non-essential traffic and block invalid IP addresses. These are typically ineffective against sophisticated attacks.
- Intrusion-detection systems can be used in conjunction with firewalls, but this is not an automated process. They need manual tuning by security experts and often generate false positives.

Given the increasing threat of DDoS, even the most technically proficient companies tend to employ external mitigation services to counter DDoS attacks.

The mitigation service will monitor your internet traffic and, when necessary, instigate numerous technical controls to mitigate an attack.



Case study:

Targeting the stock exchange

A well-known stock exchange was taken offline in August 2020 for four consecutive days due to a cyber attack.

A DDoS attack halted all the trading in cash markets and disrupted operations in its debt, share and derivatives markets.

Services were proactively suspended until protections were put in place and the attack rendered ineffective.

Source: CNBC, 2020. BBC, 2020

Cyber threats and attacks

Vulnerabilities

Cyber threat management

(Spear) phishing

Distributed Denial of Service attack (DDoS)

Ransomware

Website attacks

Advanced persistent threats (APTs)

Protect your business from cyber threats

Cyber glossary

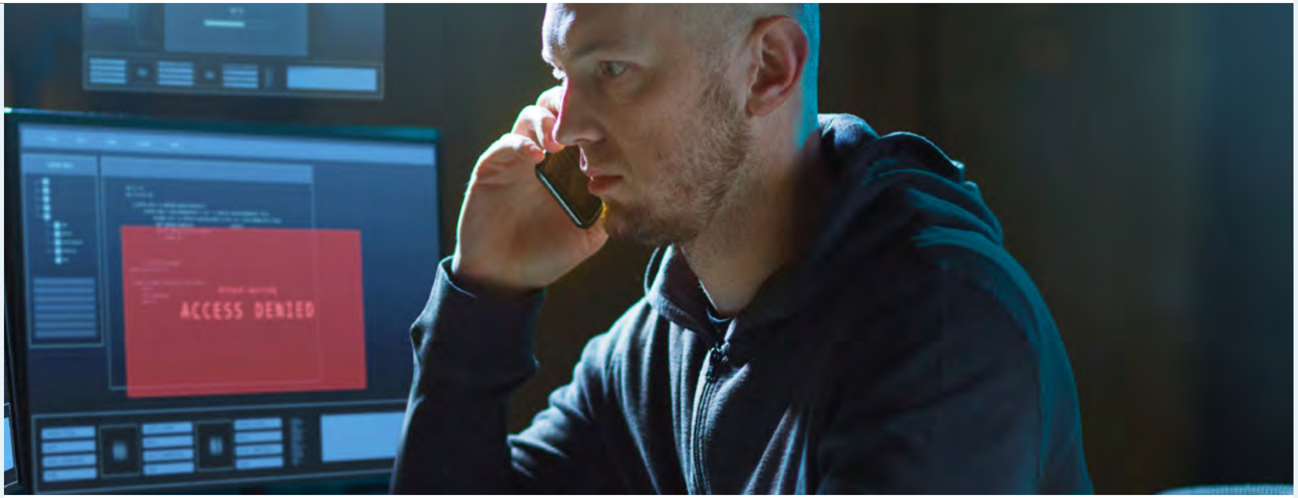
Ransomware – extortion malware

What is ransomware?

Ransomware is a type of malicious software (malware) that severely restricts access to a computer, device or file until a user pays a ransom.

It has the ability to lock a computer screen or encrypt files with a password, often using strong encryption.

It displays a demand informing the user that the computer will stay locked unless they pay a specified sum of money.



Cyber criminals usually impose a time limit to pay the ransom. Otherwise they'll delete the code to decrypt the data and render it unrecoverable.

Ransomware usually infects single machines. Some recent attacks have also incorporated exploits that allow the malware to move laterally within a network and spread to other devices.

New trend raising: Ransomware Double Extortion. In this new technique, the attacker encrypts the victim's data with Ransomware and demands a payment to unlock their information. After they pay the ransom, the attacker demands another ransom payment not to give out the victim's data (which could also lead to a substantial fine under the new EU GDPR). This ransom tends to cost more than the last one.

There are an increasing number of Ransomware attacks targeting Industrial Internet of Thing (IIoT) systems.

This is because IIoT devices do not often have adequate cybersecurity safeguards in place, which make them an attractive entry point for attackers.

The European Commission (EC) is now consulting on addressing this issue as part of the introduction of a new Cyber Resilience Act.

Cyber threats and attacks

Vulnerabilities

Cyber threat management

(Spear) phishing

Distributed Denial of Service attack (DDoS)

Ransomware

Website attacks

Advanced persistent threats (APTs)

Protect your business from cyber threats

Cyber glossary

How are users affected?

The most common ways ransomware infects a computer are through:

Email	Clicking on a malicious link in an email or opening a malicious attachment.
Websites	Visiting a social networking site or other website that is hosting ransomware.
Removable media	Inserting or connecting an infected USB or other removable media device, for example memory sticks or external hard drive.

To decrease the chance of your business being infected by ransomware visit: **www.getsafeonline.org** – a partner of Lloyds Banking Group.

If ransomware compromises any of your systems and the computer or data sources have been locked, seek professional advice. Report attacks to the police by visiting: **www.actionfraud.police.uk**

How to protect your business

Employee education and awareness

Make sure users are aware of the risks associated with allowing malware onto a system. Also educate them about the typical ways malware can get onto a device – through email, internet (websites) and removable media.

Controls Websites

The following controls (detailed in 'Phishing') will help to reduce the chance of ransomware infection:

- user access controls,
- secure configuration,
- patch management,
- malware protection,
- web traffic protection.

Other controls that will assist in preventing malware from infecting or being able to run on a device include:

Removable media controls

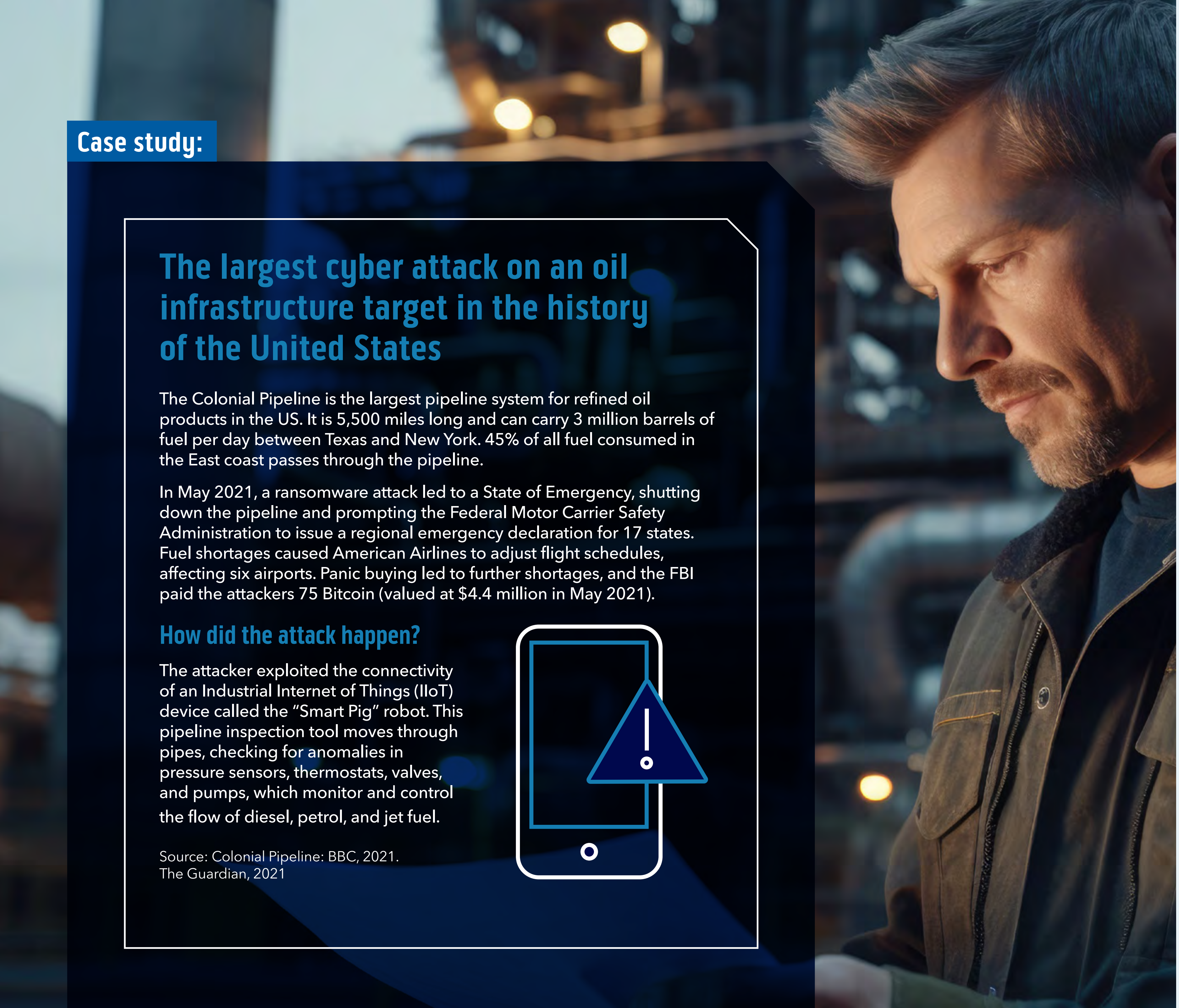
Consider the benefits of implementing a technical solution to control access to removable media devices.

Scan all media for malware before importing onto any of the organisation's systems.

Back-ups

Set up a programme to take regular back-ups. Copy your most important files often – potentially also off-site.

By doing this, in the event of an infection, machines and systems restore without causing a significant impact.



Case study:

The largest cyber attack on an oil infrastructure target in the history of the United States

The Colonial Pipeline is the largest pipeline system for refined oil products in the US. It is 5,500 miles long and can carry 3 million barrels of fuel per day between Texas and New York. 45% of all fuel consumed in the East coast passes through the pipeline.

In May 2021, a ransomware attack led to a State of Emergency, shutting down the pipeline and prompting the Federal Motor Carrier Safety Administration to issue a regional emergency declaration for 17 states. Fuel shortages caused American Airlines to adjust flight schedules, affecting six airports. Panic buying led to further shortages, and the FBI paid the attackers 75 Bitcoin (valued at $4.4 million in May 2021).

How did the attack happen?

The attacker exploited the connectivity of an Industrial Internet of Things (IIoT) device called the "Smart Pig" robot. This pipeline inspection tool moves through pipes, checking for anomalies in pressure sensors, thermostats, valves, and pumps, which monitor and control the flow of diesel, petrol, and jet fuel.

Source: Colonial Pipeline: BBC, 2021.
The Guardian, 2021

Cyber threats and attacks
Vulnerabilities
Cyber threat management
(Spear) phishing
Distributed Denial of Service attack (DDoS)
Ransomware
Website attacks
Advanced persistent threats (APTs)
Protect your business from cyber threats
Cyber glossary

Website attacks – protecting your online presence

What is a website attack?

Websites, often described as the shop window to your business, can be targeted by attackers for various reasons.

These include:

- Defacement of the website (changing the visual appearance or content).
- The addition of content (a phishing page or malware).
- The loss or compromise of customer or company data.

It could also help a DoS attack to take the site offline, or an intrusion into the back-end IT systems potentially launching malicious code.

Case study:

Large airline carrier hit twice by hackers

In early September 2018, British Airways announced that its security systems were breached in August that year. The breach affected approximately 380,000 transactions, but not travel or passport details of its customers.

A month after the announcement, it identified a second data breach affecting 185,000 customers' personal identifiable information.

It attributed both of these attacks to Magecart – a collection of at least seven organised crime groups that specialise in online card skimming.

Magecart has been linked to several high-profile data breaches.

Source: The Guardian, 2018

How to protect your business

Education and awareness

Make sure staff involved in designing and developing websites understand that security is part of their role. Train them to create secure code/sites.

Website owners must be aware of the potential risks involved in running a website – which could potentially be broader than their area of responsibility.

Strong general IT security controls

Enforce stringent access and change control.

Set up a process to run frequent back-ups.

Monitor the site regularly for suspicious activity including any unauthorised or unscheduled changes to the content of the website.

Website governance

Make sure clear policies exist, particularly around the ownership of websites and the accountability of those owners.

This should include minimum standards for the testing of the site and remediation of any identified issues.

Software testing tools and code analysis

Incorporate software testing tools and/or code analysis into the software development lifecycle to search for vulnerabilities written into software or code.

Penetration testing

Testing should take place to evaluate the security of the system or application by simulating an attack.

Ideally completed by skilled personnel before a website launch and after any significant code change.

Vulnerability scanning

To identify and discover any vulnerabilities in between penetration testing, regularly scan any internet-facing-networks.

Vulnerability management

Assess vulnerabilities identified during any testing and, where necessary, remediate on a prioritised basis.

Web application firewall (WAF)

A WAF will help to mitigate common attacks (cross-site scripting (XSS) and Structured Query Language (SQL) injection).

It could be customised to identify and block other attacks.

Third-party service providers

Make sure any service providers are able to conform to your policies (and allow testing) before signing a contract with them.

Advanced Persistent Threats – cyber attacks – the next level

What is an Advanced Persistent Threat (APT)?

APTs are sophisticated targeted attacks that employ carefully planned techniques.

These techniques will often include spear phishing but also use highly customised tools, developed specifically for the campaign, including zero-day vulnerability exploits and rootkits.

To gather information needed to customise such attacks, APTs take time to prepare and execute. This often includes a significant amount of intelligence gathering about the target organisation, its infrastructure and associated controls as well as key employees.

In the initial stage of an APT, attackers operate covertly to avoid detection. They often gather information including material from employee's social media posts. This practice is becoming more prevalent as attackers seek to exploit readily available information to launch an attack.

It's not just IT systems that are vulnerable to attack, Industrial Control Systems (ICS) are too. Originally designed to operate in isolated environments, ICSs connecting to IT systems and ultimately the internet to allow remote operation is increasing. Remote operation also exposes them to potential attacks.

Advanced Persistent Threats – cyber attacks – the next level

Who conducts APTs and why?

Well-funded and staffed groups are behind APTs. Historically, they often operate with the military support of the military or state intelligence and targeted government agencies, defence contractors or critical national infrastructure.

Many believe that nation-state actors orchestrate APT attacks against commercial organisations. Notably those involved with scarce natural resources (or example minerals and fuel) and financial institutions.

Historically, APTs typically had three primary goals:

- Theft of sensitive information from the target.
- Covert surveillance of the target.
- Sabotage of the target.

More recently organised criminals are increasingly adopting APT techniques primarily for financial gain: this means that they could target any business with valuable technology, high-value processes or intellectual property.

Financial gain is a motivation for a small subset of nation-state actors. The nation-states also appear to be using more 'open source' attack tools. This makes it difficult to differentiate them from organised criminals and makes it ever more challenging to identify the culprits.

Case study:

Nation-state threat group targeting of managed service providers (MSPs)

In 2018, it was found out that a Chinese APT group targeted MSPs in at least 12 countries, including the UK dating back to 2014.

In the first stage of the attack, MSP key staff received spear phishing emails designed to infect their computers with custom-made malware.

After gaining access, the attackers identified MSP customers that were of interest and stole hundreds of gigabytes of sensitive business data and intellectual property.

This included information from entities in the following industries:

- financial services,
- telecommunications,
- consulting,
- healthcare,
- biotechnology,
- aviation,
- space and satellite,
- government,
- commercial manufacturing,
- automotive,
- mining and drilling,
- maritime.

Source: NCSC, 2018

Advanced Persistent Threats – prevent, detect and respond

How to protect your business

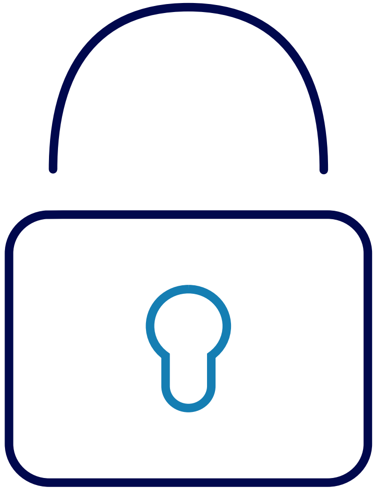
Due to the nature of APTs, there is no single solution, as they usually include a series of infiltration techniques. Individually, businesses typically know those techniques well, so can defend against them.

Having **robust information** security practices and systems in place will help to prevent or detect some APT attempts. Including efficient patching and vulnerability management routines, and effective proactive monitoring of suspicious activity, including Indicators of Compromise (IoCs).

Layers of defence will help to protect against APTs, along with a risk-based approach – making sure available resources are directed to the assets most likely to be targeted.

An essential **layer of protection** involves employee education. Spear phishing attacks often target staff to gain entry into the organisation's systems.

Knowledge of how APTs typically work will help to identify and defend against them. Numerous models exist that show different phases or stages of an APT attack. Lockheed Martin produced the most popular example called the **'Cyber Kill Chain®'.**



Case study:

Shutdown of a Middle Eastern petrochemical plant

In 2017, a threat actor likely connected to a Russian government-owned research institute compromised and shutdown the networks of a Middle Eastern petrochemical plant.

The threat actors used a destructive tool called Triton, which targets Industrial Control Systems often used in oil and gas facilities. It allows a threat actor to manipulate or remove safeguards in a compromised network.

Although the shutdown was likely unintentional, it indicated a focus on developing Triton's operational capabilities for future attacks.

This could have wide-ranging effects across various industries including the oil and gas, financial services and logistics sectors.

Source: Computer Weekly, 2019. Fire Eye, 2018

Cyber threats and attacks
Vulnerabilities
Cyber threat management
(Spear) phishing
Distributed Denial of Service attack (DDoS)
Ransomware
Website attacks
Advanced persistent threats (APTs)
Protect your business from cyber threats
Cyber glossary

Protect your business from cyber threats

The risk from cyber threats differs not only between industries or sectors, but also between businesses within the same industries.

The actual risk to your business will depend on several factors, including:

- Who might attack you?
- What they want to achieve.
- How vulnerable your assets or services are.

You can't control the capabilities or motives of attackers. Nevertheless, it's possible to make things more difficult for them by reducing your business vulnerabilities.

The following may assist your company to become more aware and protected against cyber threats.

1. Understand where you store critical information, assets, and services. Consider who has access, such as suppliers and contractors, and focus on confidentiality, integrity, and availability.
2. Think about who might want to attack your business. Understand the potential impact of a successful attack.
3. Consider if you have a risk appetite for different types of cyber events impacting your business.
4. Be aware of vulnerabilities and establish an efficient process to manage them. Consider people, processes, and technology.
5. Evaluate the protection of critical assets and identify gaps.
6. Produce a prioritised action plan to help you protect against cyber attacks. **See 10 Steps to Cyber Security.**
7. Make sure your staff and if appropriate, clients, know about cyber threats. Especially the risks associated with social engineering and phishing attacks.
8. Set up a process to regularly review critical business information, data assets, and cyber threats.
9. In the event of a successful cyber crime, have a plan and incident response in place. **See Reducing the Impact.**
10. Consider taking out adequate cyber insurance cover.
11. Consider the disruption to your working capital position, revenues – and make appropriate provisions.

Important –
If your business falls victim to cybercrime, contact Action Fraud for assistance.

Where to find out more:

- Action Fraud
- Cyber Aware
- Cyber Essentials
- Get Safe Online
- Stay Safe Online
- Global Cyber Alliance
- NCSC Board Toolkit

Cyber glossary

Access Control

Allows system administrators to set restrictions and approve access to files and programs within a network.

Advanced Persistent Threat (APT)

A targeted attack carried out by sophisticated attackers who infiltrate a network over time, seeking proprietary information.

Bitcoin/Virtual Currencies

An online currency enabling payments without intermediaries like banks. Bitcoin's legitimacy is disputed due to lack of regulation and associations with illegal activities.

Bot/Botnet

A Bot is a compromised device, like a computer or smartphone, controlled by a cybercriminal to perform tasks such as sending spam, spreading malware, or participating in DDoS attacks. These devices are also called "zombies."

A Botnet is a network of these compromised devices, controlled via Command and Control (C&C) servers. Botnets, which can include hundreds to thousands of devices, are often used in DDoS attacks to overwhelm and disable target sites.

Command and Control

A Command and Control (C&C or C2) centre is a computer that manages a Botnet, a network of compromised devices. Some Botnets use distributed C&C systems for increased resilience. Hackers use C&C centres to direct multiple devices to perform tasks, often launching DDoS attacks by instructing many computers to act simultaneously.

Crimeware-as-a-Service (CaaS)

Cyber-criminal services offered for hire, including launching DDoS attacks, stealing financial information, and delivering malware.

Cryptocurrency

Decentralised digital currency, like Bitcoin, Litecoin and Ethereum, using cryptography for transactions, making it difficult to trace payers and payees. This makes it an attractive option for cyber criminals to evade law enforcement.

Dark Web/Dark Net

A hidden portion of the Internet not indexed by search engines. The Dark Web, a subset of the Deep Web, conceals server IP addresses and is accessible through anonymising software like TOR. It hosts both criminal and legitimate sites.

Denial of Service (DoS) Attack

Prevents users from accessing a computer or website by overloading or shutting down a service. While disruptive, it doesn't result in data theft.

Distributed Denial of Service

Uses many compromised devices (Botnet) to launch an attack, disrupting systems by preventing genuine users from accessing them. DDoS attacks are harder to mitigate due to distributed traffic.

Encryption

Encoding data into secret code to ensure only authorised parties can read it. Decryption requires the appropriate password or key.

Exploit

An attack on a computer system that exploits a vulnerability or bug in software or hardware, granting unauthorised access or control.

Firewall

Prevents unauthorised access to a computer or network by acting as a barrier. It blocks malicious activity and hacking attempts.

The Firewall inspects all traffic, both inbound and outbound, to see if it meets certain criteria. If it does, it's allowed; if not, the Firewall blocks it.

Hacktivism

Breaking into computer systems for politically or socially motivated purposes, often involving defacing websites or launching DDoS attacks.

Indicators of Compromise (IoCs)

Used to identify potentially malicious activity on a system or network. IoCs are data items found in system log entries or files.

Cyber glossary

Industrial Control System (ICS)

A general term that includes various types of command and control systems primarily used in industrial production.

These include Supervisory Control and Data Acquisition (SCADA) systems and Digital Control Systems (DCS).

Outside takeover can cause not only disruption to business operations, but also destruction of equipment and potentially injury to people.

Internet of Things (IoT)

Interconnected computing devices embedded in everyday objects, enabling data exchange.

Malware

Collective term for malicious software viruses, like Trojans and ransomware, created to damage, disrupt, or exploit computer vulnerabilities.

Patches

Software add-ons that fix bugs and security vulnerabilities in operating systems or applications.

Patching for new security vulnerabilities is critical to protect against malware. Many high-profile threats take advantage of security vulnerabilities.

Phishing

An attempt to obtain sensitive information from victims via email. The sender poses as a trusted source, such as a colleague or bank, and directs victims to a website. It asks for passwords, credit card details, or installs malware on their devices.

Ransomware

Malware that restricts access to a computer, device, or files until the user pays a fee. Fraudulent messages may falsely claim to be from law enforcement agencies, alleging illegal online activities.

Remote Access Trojan (RAT)

A malware program providing cybercriminals back-door access to infected devices. RATs collect information, including webcam surveillance, and can introduce additional malware.

Rootkit

A type of malware attacking a device before the operating system fully starts up. It gains administrative access to control processes or software, often needing Operating System reinstallation to remove it.

SCADA

A system allowing industrial organisations to control processes, monitor real-time data, and interact with sensors and valves through Human Machine Interface (HMI) software.

Smishing (SMiShing)

A social engineering technique targeting mobile phone users through text messages. Smishing tricks recipients into downloading malware onto their devices to get private and confidential information.

Social Engineering

Manipulating people to share sensitive information or perform actions. Cybercriminals use this for unauthorised access to systems or fraudulent purposes.

Spam

Unsolicited bulk email (junk mail) arriving in inboxes. Spammers disguise emails to evade anti-spam software and may distribute malware. Instant messaging and social networking sites are also exploited for spam.

Spear Phishing

A carefully crafted phishing attack directed at specific individuals or companies.

It appears to come from a recognised source, to lull the recipient into a sense of trust.

Although often intended to steal data for malicious purposes, cyber criminals may also intend to install malware on a targeted user's computer.

SQL Injection

An exploit that takes advantage of database query software lacking thorough testing for correct queries. It sends commands via a web server linked to an SQL database. Improperly designed servers may execute unintended commands, potentially revealing sensitive information.

Threat Actors

Individuals or groups engaged in malicious cyber activity. They can be categorised as "Nation State," "Organised Crime Group," or "Hacktivist," with some overlap between these groups.

Trojan

A program that appears harmless but contains hidden malicious software. Trojans often disguise themselves as innocent email attachments or free applications.

Virus

Malicious computer programs that can spread to other files, causing harmful effects such as displaying messages, stealing data, or giving hackers control over your computer. Viruses can exploit security flaws in your operating system and may arrive via email attachments, Internet downloads, or USB drives.

Cyber glossary

Vishing (Voice or VoIP Phishing)

A social engineering technique using telephone calls to scam users into divulging private or confidential information.

Vulnerability

Bugs in software programs that hackers exploit to compromise computers. Responsible vendors issue patches to address vulnerabilities. A "zero-day" attack exploits a vulnerability before it's patched.

To reduce vulnerabilities, you should apply the latest available patches and/or enable the auto update feature on your operating system and any installed applications.

Web Application Firewall (WAF)

Protects web servers accessible from the Internet by scanning activity, identifying probes, and blocking attacks. It performs content filtering, spam filtering, intrusion detection, and antivirus functions.

XSS (Cross Site Scripting)

Where an attacker injects code into a legitimate website, bypassing security to change user settings, hijack accounts, or allow malware downloads.

Zero Day

A vulnerability that remains unpatched by the vendor. Attackers may exploit it even before the vendor is aware, resulting in a zero-day attack.

Find out more

bankofscotland.co.uk/business

Contact your Relationship Manager

Please let us know if you have a problem – we're here to help. See our complaints process on our 'Help & Support' page at: **business.bankofscotland.co.uk/complaint**

Please contact us if you would like this information in an alternative format such as Braille, large print or audio.

Important information

Bank of Scotland plc. Registered Office: The Mound, Edinburgh EH1 1YZ. Registered in Scotland no. SC327000. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under Registration Number 169628.

Eligible deposits with us are protected by the Financial Services Compensation Scheme (FSCS). We are covered by the Financial Ombudsman Service (FOS). Please note that due to FSCS and FOS eligibility criteria not all business customers will be covered.

Lloyds Banking Group is a financial services group that incorporates a number of brands including Bank of Scotland. More information on Lloyds Banking Group can be found at **lloydsbankinggroup.com**

While all reasonable care has been taken to ensure that the information provided is correct, no liability is accepted by Bank of Scotland for any loss or damage caused to any person relying on any statement or omission. This is for information only and should not be relied upon as offering advice for any set of circumstances. Specific advice should always be sought in each instance.

BANK OF SCOTLAND

By the side of business