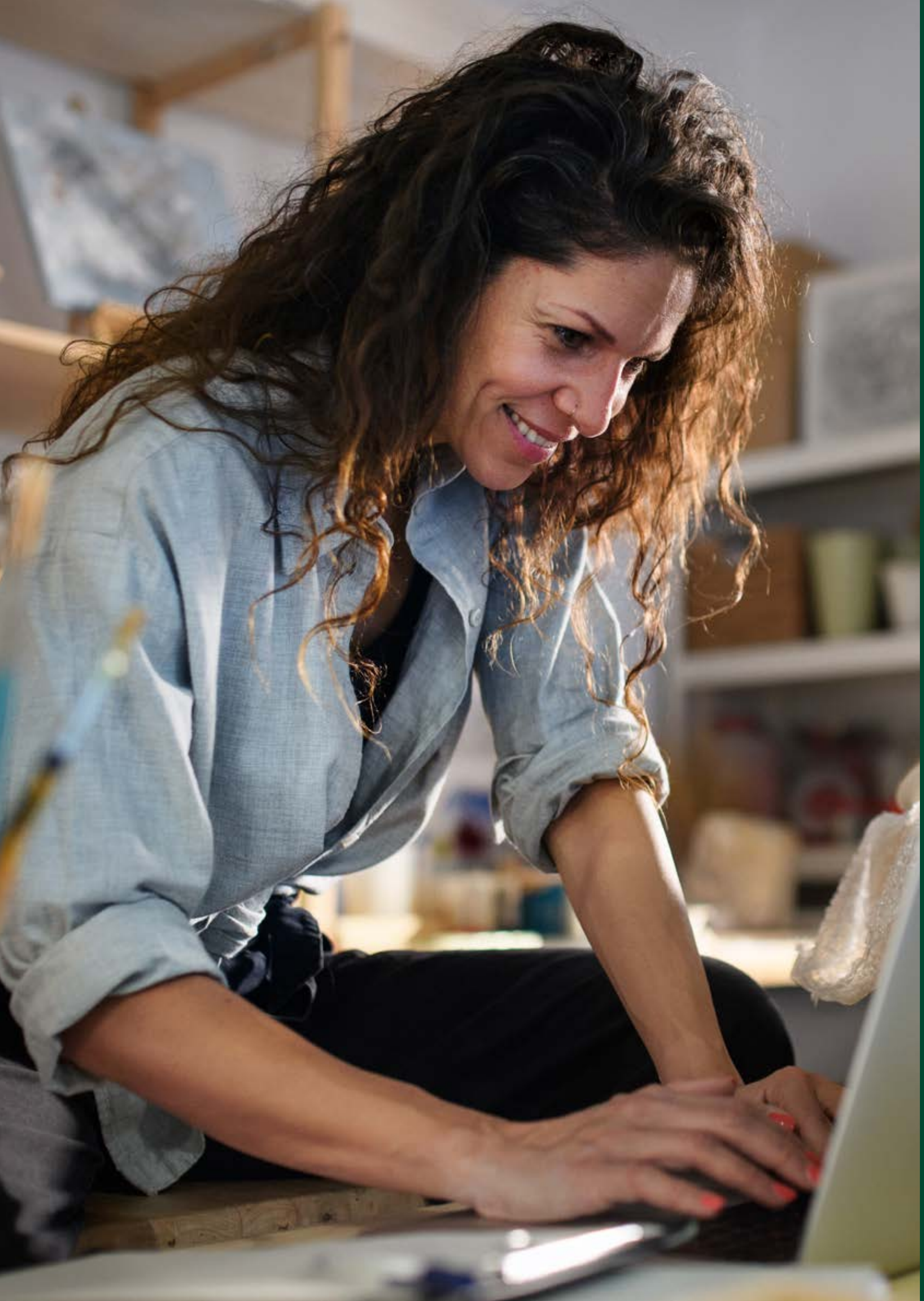


BUSINESS & COMMERCIAL

Cyber risk guidance

LLOYDS

Cyber risk guidance

Cyber threats to businesses are increasing and becoming more sophisticated.

This guide offers clear, practical steps to help you manage and reduce these risks.

Learn how to protect your business, safeguard your employees and secure your assets.

43%

UK businesses reported a cyber breach.

(Department for Science, Innovation and Technology, 2025).

$9.5 trillion

(£7.14 trillion)

The cost of cybercrime globally in 2024.

(Cybersecurity Ventures, 2024).

£12 trillion

The cost of cybercrime globally by 2029.

(Statista Market Insights, IMF, 2025).

> “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 businesses more secure and more resilient and ultimately to help Britain prosper.”

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

Contents

Select 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 can target any combination of information technology, digital assets, the data they hold and the services they deliver. These threats are constantly evolving and often focus on compromising the confidentiality, integrity or availability of data and systems.

The impact on businesses can be significant. Cyber attacks can damage brand reputation, erode customer trust and disrupt operations. They may also lead to legal or regulatory sanctions – particularly if large volumes of customer data are stolen and regulators find that business controls for data privacy are inadequate.

Threat actors: Who are the attackers?

Cyber attackers are often grouped by their motivations and capabilities. Common categories include:

Hacktivists

- Loosely organised groups or individuals driven by political or ethical causes.
- Typically, they aim to deface websites or take them offline to spread a message.

Criminals and Organised Criminal Groups (OCGs)

- Financially motivated, stealing billions from businesses and consumers each year.
- Tactics often include phishing and malware to capture login credentials for banking or accounting systems.

Nation States/State-sponsored attackers

- Government-backed groups focused on stealing intellectual property or sensitive information.
- Highly resourced and skilled, capable of delivering sophisticated attacks.

Insiders

- Threats can come from within a business. Employees or contractors may act maliciously, sometimes under pressure or manipulation from third parties.

Cyber threats and attacks
Vulnerabilities
Cyber threat management
(Spear) phishing
Distributed Denial of Service attack (DDoS)
Ransomware
Website attacks
Advanced persistent threats (APTs)
Building cyber resilience: Protect, respond, recover
Cyber glossary

Case study

Reputational impact of cyber attack

In April 2025, a leading UK retailer experienced a major ransomware attack that disrupted online sales, Click & Collect services, and inventory systems during the busy Easter shopping period. Hackers had infiltrated systems weeks earlier, deploying ransomware at a time of peak consumer demand. The incident quickly made headlines, sparking widespread criticism on social media and eroding customer trust. Surveys revealed that over two-thirds of affected customers reduced online purchases, and nearly half deleted their accounts entirely. Analysts estimated a market value drop around £500 million within days.

Although operations were restored within weeks, reputational damage lasted far longer. The brand faced increased regulatory scrutiny and ongoing challenges to rebuild consumer confidence.

This case highlights how timing and visibility can amplify reputational harm, making trust restoration a critical priority after an attack.

Source: CNBC, 2025.

Vulnerabilities

How the attackers get in

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

Features

Attackers often take advantage of features designed to make computers and mobile devices easier to use. For example, macros in spreadsheets and word processors automate tasks and calculations – but they can be also misused to download malware or record keystrokes.

Businesses can reduce this risk by disabling non-essential functions such as macros or Bluetooth on PCs and mobile devices.

Flaws

Cyber attackers often exploit flaws or unintended functionalities in software.

Fixing these issues is known as patching. However, flaws can remain undetected for long periods – until a vendor releases a patch or update.

User error

Even when vulnerabilities are patched or disabled through secure builds, risks can persist due to human error.

For example, a systems administrator might accidentally enable a vulnerable feature or fail to apply a critical fix. Actions by users – whether intentional or accidental – can expose sensitive information.

! **Attackers Exploit Vulnerabilities**

Cyber attackers actively seek out and exploit weaknesses in systems. There is a thriving criminal market for software flaws, especially those known as zero-day vulnerabilities – recently discovered issues that are not yet public. These can sell for hundreds of thousands of pounds.

Cyber threat management

How to protect your business

User education and awareness

- Create policies that set out acceptable and secure use of your business systems.
- Implement a regular training programme for all users.
- Keep awareness high by sharing updates on emerging cyber threats and best practices.

Secure configuration

- Maintain an up-to-date inventory of all IT systems and define a secure baseline build for every device.
- Apply security patches promptly to keep systems configured securely and reduce vulnerabilities.

Network security

- Protect your networks from both external and internal threats.
- Manage and secure your network perimeter.
- Block unauthorised access and filter out malicious content.
- Regularly monitor and test your security controls to ensure effectiveness.

Malware protection

- Develop a monitoring strategy supported by robust policies.
- Continuously monitor all IT systems and networks for threats.
- Analyse system logs regularly to detect unusual activity that may indicate an attack.

Removable media controls

- Establish a policy that governs all access to removable media.
- Restrict the types of media allowed and limit their use.
- Scan all removable media for malware before connecting to corporate systems.

Social media

- Implement a clear social media policy for employees.
- Educate users on the risks of posting work-related content online.
- Highlight that sharing personal or business details could make them a target for phishing or spear-phishing attacks.

Cyber threats and attacks
Vulnerabilities
Cyber threat management
(Spear) phishing
Distributed Denial of Service attack (DDoS)
Ransomware
Website attacks
Advanced persistent threats (APTs)
Building cyber resilience: Protect, respond, recover
Cyber glossary

Cyber threat management

How to protect your business

Incident management

- Establish an incident response and disaster recovery capability.
- Create and regularly test incident management plans.
- Provide specialist training for the incident management team.
- Report criminal incidents promptly to law enforcement.

Managing user privileges

- Implement account management processes to limit, control and monitor privileged accounts.
- Restrict access to activity and audit logs.

Monitoring

- Develop a monitoring strategy supported by clear policies.
- Continuously monitor all IT systems and networks.
- Review and analyse logs for unusual activity that may indicate an attack.

Home and mobile working

- Create a mobile working policy and train staff to follow it.
- Apply secure baseline builds 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 where attackers pose as trusted organisations – such as banks – to steal personal information or passwords.

They send urgent emails asking you to click a link that leads to a fake website.

On that site, victims are tricked into entering login details or downloading malware.

What is spear phishing?

Spear phishing is a more targeted form of phishing.

Attackers impersonate colleagues within your organisation to gain trust. They may trick you into opening attachments, clicking links or even making payments.

Spear phishing is often part of 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)

Building cyber resilience: Protect, respond, recover

Cyber glossary

How to protect your business

Employee education and awareness

- Train employees on the risks of opening files or clicking links in emails – even if they appear to come from a colleague.
- Implement a social media policy to limit sharing of work-related information, which attackers often use for spear-phishing.

User access controls

- Restrict user permissions to only what is needed for their role.
- Limit privileged accounts and block the ability to run executable files* if not required.
- Consider deploying technical controls to enforce these restrictions.

* 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

- Minimise the potential attack surface on user devices by applying a secure build (known as hardening).
- Remove unnecessary software and default user accounts.

Software patch management

- Apply patches as early as possible (after testing) to reduce exposure to known vulnerabilities.

Consider deploying technical controls, which could include:

Malware protection

- Deploy anti-malware tools to scan emails and attachments for malicious code.
- Create a policy that ensures anti-malware defences are applied consistently across all business areas.
- Use a dedicated device for online banking that does not have access to email systems to reduce malware infection risk.
- Regularly scan all systems and devices across the organisation for malware.

Web traffic protection

- Use web content filtering and site categorisation services to block access to risky websites.
- Enable real-time scanning of web traffic for malicious code.

Case study

Simple but effective

In May 2025, a highly targeted spear-phishing campaign hit financial executives across global banks, insurance firms and investment companies.

Attackers posed as recruiters from a well-known financial institution, sending personalised emails offering confidential leadership opportunities. Each email included a PDF attachment that redirected victims to a fake portal hosting a malicious script.

Once activated, the script installed NetBird – a legitimate remote access tool – and OpenSSH, giving attackers covert network access without triggering standard malware alerts. This straightforward yet sophisticated social engineering tactic bypassed traditional security awareness training and technical controls by exploiting trust and curiosity.

The impact was significant. Attackers gained persistent access to corporate systems, enabling data theft and potential fraudulent transactions.

This campaign proved that well-crafted spear-phishing emails – without advanced exploits – remain one of the most effective attack methods, especially when aimed at high-value targets with privileged access.

Source: Cybernews, 2025.

Distributed Denial of Service attack

Attacking your online availability

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

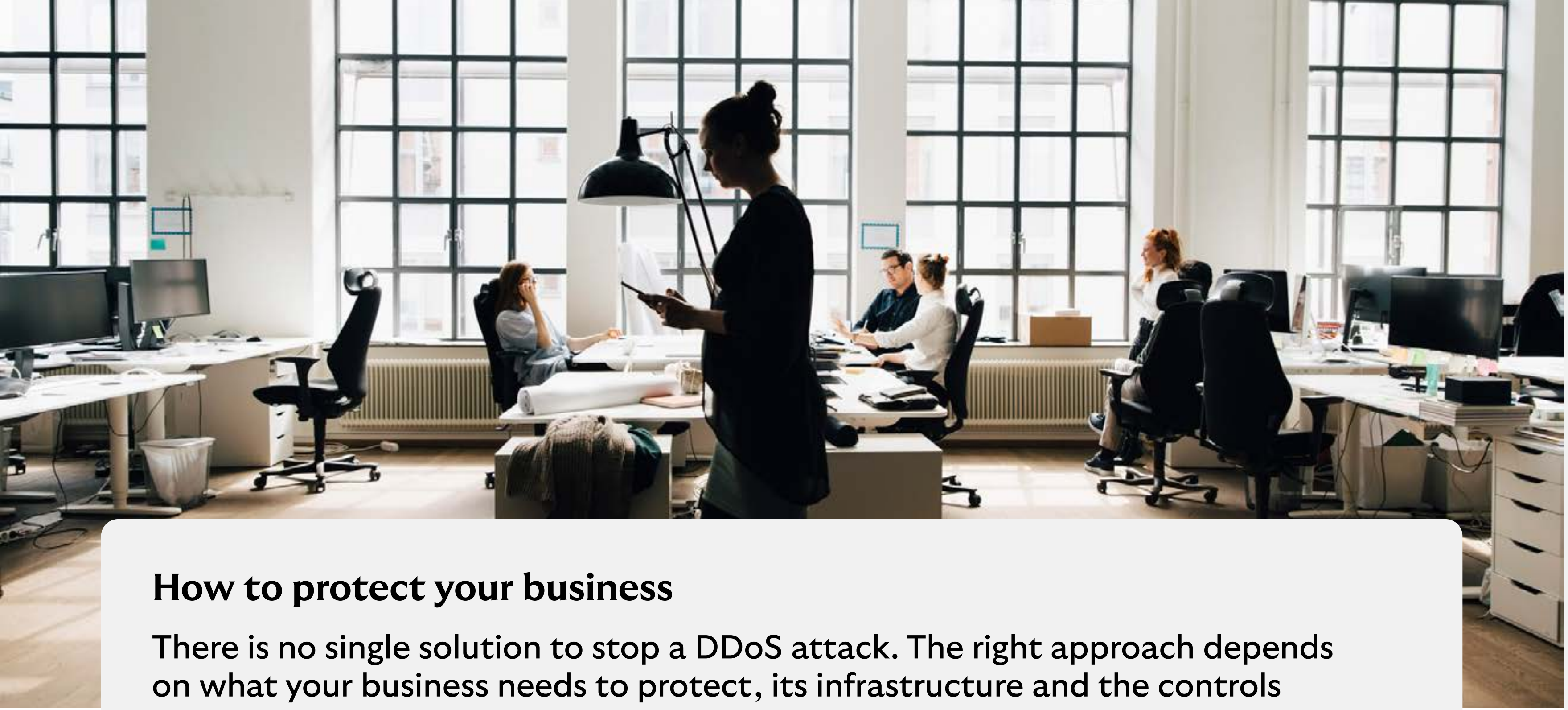
A DDoS attack is a specific class of Denial of Service. The attack will originate from multiple sources, often using a large network of malware-infected computers known as a 'botnet'. In the past, only highly skilled individuals could launch these attacks because they required deep knowledge of internet and system infrastructure.

Today, the barrier to entry is much lower. Tools are available on the Dark Net for a modest fee, allowing unskilled attackers to hire botnets and target organisations of their choice. Entry-level DDoS-for-hire plans start from as little as $10–$50 per month, with single attacks advertised at similar daily rates. High-end packages cost significantly more. These point-and-click services make launching attacks simple and cheap.

The scale and ease of DDoS attacks have grown, driven by competition among hackers and the use of Internet of Things (IoT) devices to power botnets. Hyper-volumetric attacks exceeding 1 Tbps now occur daily, with record peaks reaching 29.7 Tbps, fuelled by botnets like Aisuru that compromise millions of IoT devices.

Cyber criminals often use DDoS attacks as leverage, threatening companies with disruption unless they pay a ransom – usually in cryptocurrency such as Bitcoin. While some attacks are politically or ideologically motivated, many are financially driven. Victims typically receive extortion emails demanding payment. Most attacks last under 10 minutes but are frequently used as a smokescreen to distract defences while other intrusions, such as data theft or unauthorised access, take place.

Source: www.imperva.com/learn/ddos/booters-stressers-ddosers/



How to protect your business

There is no single solution to stop a DDoS attack. The right approach depends on what your business needs to protect, its infrastructure and the controls already in place.

Attackers use different techniques to make their attacks more effective, so businesses need layered defences. Common measures include:

- Buying extra bandwidth from your Internet Service Provider to absorb traffic spikes.
- Configuring routers and firewalls to block simple attacks by filtering non-essential traffic and invalid IP addresses. These steps help but are rarely effective against sophisticated attacks.
- Using intrusion detection systems alongside firewalls. These require manual tuning by security experts and can generate false positives, so they are not fully automated.

Given the growing threat of DDoS attacks, even highly skilled businesses often rely on external mitigation services.

These services monitor internet traffic and, when needed, apply advanced technical controls to reduce the impact of an attack.

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

In March 2024, a major European stock exchange was hit by a large-scale cyber attack that disrupted trading for two consecutive days. The attack combined Distributed Denial of Service (DDoS) techniques with application-layer floods targeting critical APIs used for trade matching and settlement.

To prevent systemic risk, the exchange suspended trading across equities, derivatives and debt markets. While core systems were not breached, the disruption caused significant delays in clearing and settlement, affecting thousands of transactions and eroding investor confidence. Regulators launched an immediate review, and the exchange implemented enhanced DDoS mitigation and zero-trust controls before restoring services.

This case shows how relatively simple attack methods, when scaled through botnets, can halt financial markets – highlighting the need for layered defences and proactive resilience planning.

Source: Infosecurity Magazine, 2025.

Ransomware

Extortion malware

What is ransomware?

Ransomware is a type of malicious software (malware) that blocks access to a computer, device or files until a ransom is paid.

It can lock a computer screen or encrypt files with a password, often using strong encryption.

When infected, the system displays a message demanding payment, warning that access will remain blocked unless the specified amount is paid.

Attackers use ransomware to encrypt data and impose strict payment deadlines. Failure to pay often results in permanent data loss. Modern ransomware doesn't stop at a single device – it spreads laterally, locking entire networks.

Double extortion is now common: criminals steal data and threaten to leak it even after payment. Increasingly, triple extortion adds pressure through DDoS attacks or harassment of customers and partners, amplifying reputational and regulatory risks.

Attacks on Industrial IoT are rising because connected devices often lack strong security. Ransomware-as-a-Service makes launching attacks easy, driving record volumes and multimillion-pound demands.

To combat these threats, the UK's Cyber Security Resilience Bill and EU's Cyber Resilience Act enforces secure-by-design principles, aiming to curb these threats.

How are users affected?

Ransomware typically infects computers through three common methods:

Email

Clicking on a malicious link or opening an infected attachment in an email.

Websites

Visiting a social networking site or other website that is hosting ransomware.

Removable media

Connecting an infected USB stick or other removable device, such as a memory stick or external hard drive.

How to protect your business

Employee education and awareness

Help your team understand the risks of malware and how it can affect your systems. Share practical tips on how malware typically enters devices, such as:

- Email attachments.
- Unsafe websites.
- Removable media (e.g., USB drives).

Controls websites

Applying the following measures can significantly reduce the risk of ransomware:

- User access controls – Limit access to what's necessary.
- Secure configuration – Ensure systems are set up securely.
- Patch management – Keep software up to date.
- Malware protection – Use trusted security tools.
- Web traffic protection – Block harmful sites and content.

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

Removable media controls

Use technical solutions to manage access to removable media devices. Always scan any media for malware before importing onto any of your business systems.

Back-ups

Create a regular back-up schedule. Copy your most important files frequently, and consider storing a copy off-site.

This ensures that if an infection occurs, you can restore machines and systems quickly without major disruption.

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**

Case study

The largest ransomware attack on emergency alert systems in U.S. history

The CodeRED emergency alert platform helps local governments, law enforcement and fire departments send geo-targeted warnings for severe weather, chemical leaks, and evacuations. Millions of U.S. residents rely on these alerts for public safety.

In November 2025, the INC Ransom group launched a ransomware attack that paralysed this critical system nationwide. Emergency alerts were disrupted across more than a dozen states, forcing officials to use social media and radio for urgent notifications. Sensitive user data was stolen and partially leaked online. The attackers demanded $950,000, later reducing it to $450,000, but negotiations failed.

The outage lasted several days, leaving millions without timely warnings and triggering federal investigations. This incident highlights how ransomware can cripple essential services – similar to the Colonial Pipeline attack in 2021 – and create cascading risks for entire communities.

How did it happen?

Attackers gained access using compromised credentials and deployed ransomware across the platform's core systems, encrypting critical servers and disabling alert distribution.

Source: SecurityWeek, 2025.

Website attacks

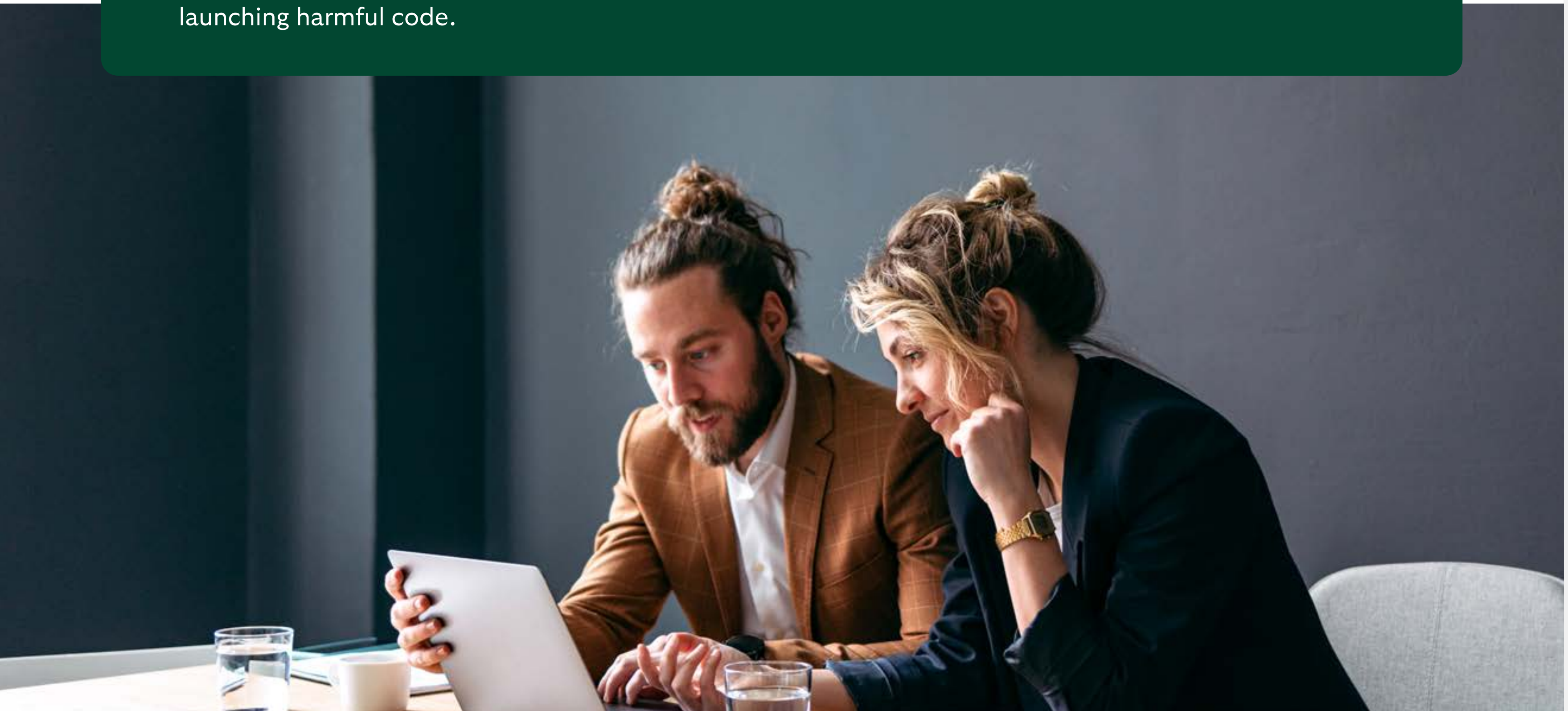
Protecting your online presence

What is a website attack?

Your website is often the shop window to your business – and attackers know it.

They may target websites for several reasons, including:

- **Defacement** – Changing the visual appearance or content.
- **Adding malicious content** – Inserting phishing pages or malware.
- **Data compromise** – Stealing customer or company information.
- **Disruption** – Using the site to support a DoS attack or gain access to back-end systems, potentially launching harmful code.



Case study

Website Attacks – Formjacking Hits Global E-Commerce

In May 2025, a sophisticated cyberattack targeted thousands of e-commerce websites worldwide. Hackers injected malicious code into checkout pages, silently capturing customers' payment card details and personal information during transactions. The attack went undetected for weeks, affecting major online retailers and small businesses alike.

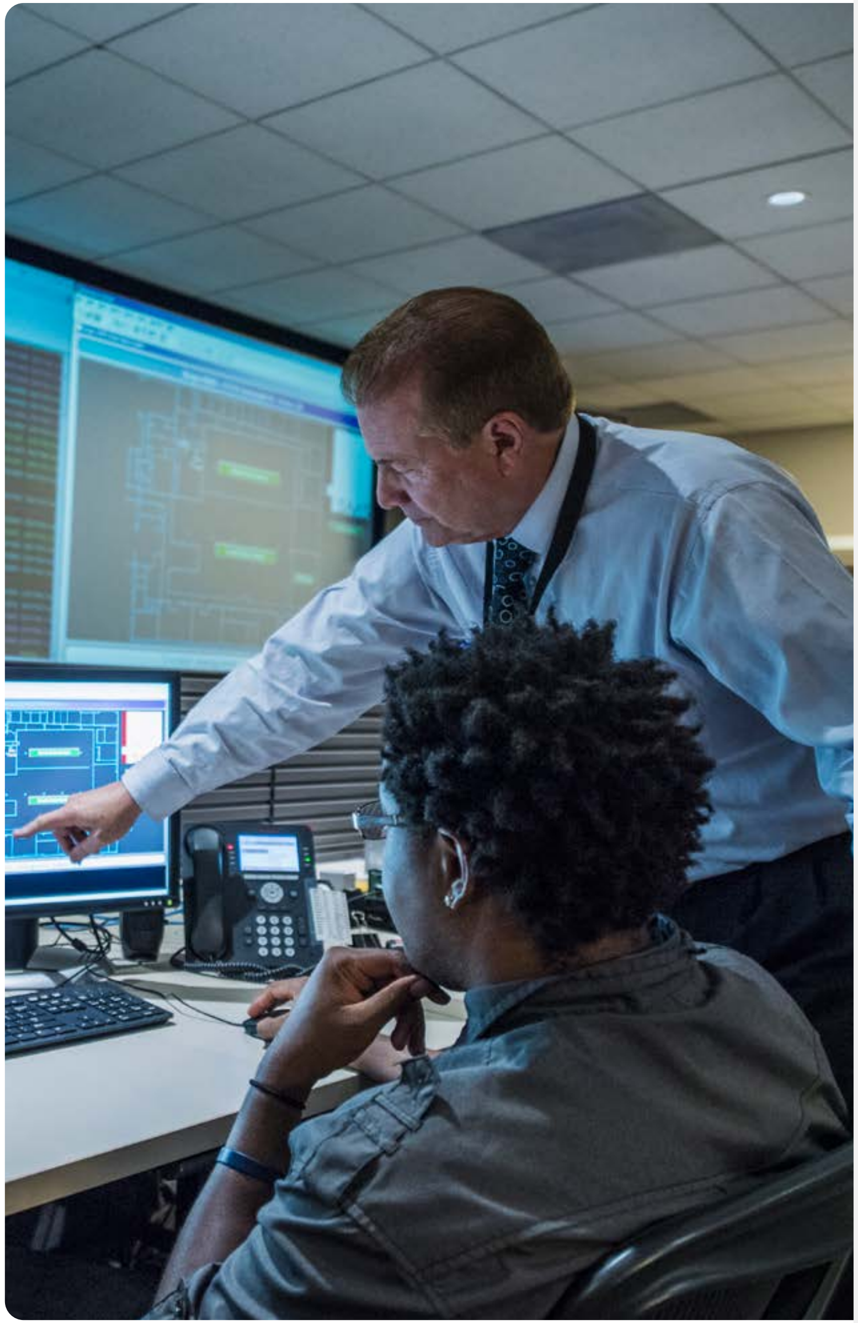
Millions of consumers were impacted, and stolen data quickly appeared on underground markets. Businesses faced severe reputational damage, regulatory investigations, and financial losses.

This incident highlights how attackers exploit weaknesses in website security and third-party scripts, making detection extremely difficult and putting both companies and customers at risk.

How did it happen?

Cybercriminals used formjacking techniques, inserting malicious scripts into payment forms via compromised third-party services. These scripts harvested sensitive data during legitimate transactions without disrupting normal site operations.

Source: Cyber Security News, 2025.



How to protect your business

Education and awareness

- Ensure staff involved in website design and development understand that security is part of their role.
- Provide training on creating secure code and building secure sites.
- Make website owners aware of the risks involved in running a site, which may extend beyond their immediate responsibilities.

Web application firewall (WAF)

- Deploy a WAF to mitigate common attacks such as cross-site scripting (XSS) and SQL injection.
- Customise the WAF to detect and block other potential threats.

Third-party service providers

- Ensure service providers comply with your security policies and allow testing before signing contracts.

Strong general IT security controls

- Enforce strict access and change controls.
- Implement a process for frequent back-ups.
- Monitor the site regularly for suspicious activity, including unauthorised or unscheduled content changes.

Software testing tools and code analysis

- Enforce strict access and change controls.
- Implement a process for frequent back-ups.
- Monitor the site regularly for suspicious activity, including unauthorised or unscheduled content changes.

Vulnerability management

- Assess vulnerabilities identified during testing.
- Remediate issues on a prioritised basis.

Vulnerability scanning

- Regularly scan internet-facing networks between penetration tests to identify vulnerabilities.

Website governance

- Establish clear policies on website ownership and accountability.
- Define minimum standards for testing and remediation of identified issues.

Penetration testing

- Conduct penetration tests to evaluate system or application security by simulating attacks.
- Ideally, perform tests before launching a website and after any significant code changes, using skilled personnel.

Advanced Persistent Threats

Cyber attacks – the next level

What is an Advanced Persistent Threat (APT)?

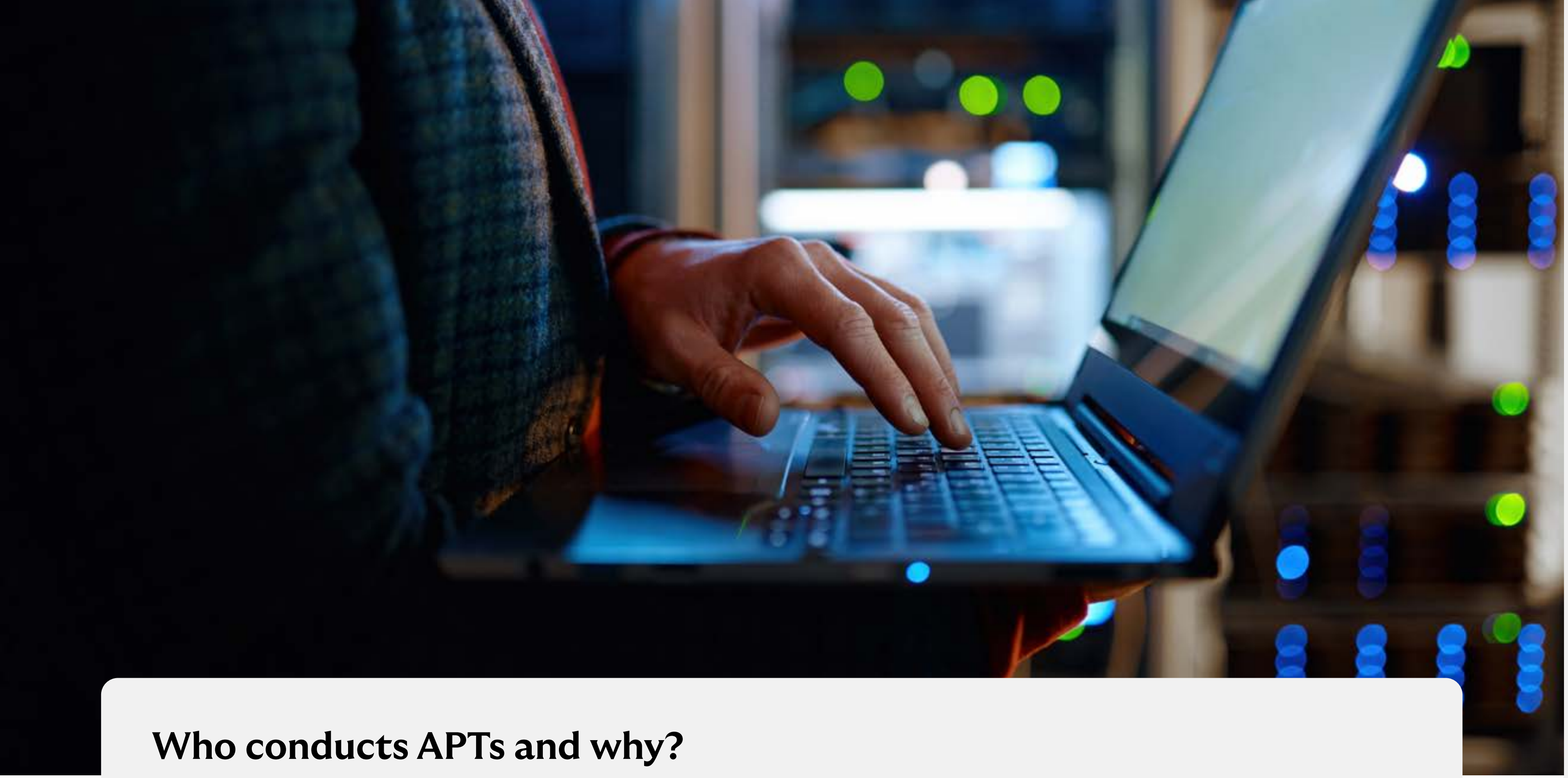
APTs are sophisticated targeted attacks that use carefully planned techniques.

These attacks often involve spear phishing and employ customised tools developed specifically for the campaign, including zero-day vulnerability exploits and rootkits.

Advanced Persistent Threats take time to prepare and execute because attackers need detailed information to customise their campaigns. This preparation often involves extensive intelligence gathering about the target business, its infrastructure, security controls, and key employees.

In the early stages, attackers operate covertly to avoid detection. They frequently collect information from sources such as employee social media posts – a practice that is becoming increasingly common as attackers exploit readily available data to launch attacks.

It's not only IT systems that are at risk. Industrial Control Systems (ICS) are also vulnerable. These systems were originally designed to operate in isolated environments, but many now connect to IT networks and the internet to enable remote operation. While this connectivity improves efficiency, it also exposes ICS to potential cyber attacks.



Who conducts APTs and why?

Advanced Persistent Threats are typically carried out by well-funded and highly organised groups. Historically, these groups often operated with the backing of military or state intelligence agencies and targeted government bodies, defence contractors, and critical national infrastructure.

Many believe nation-state actors orchestrate APT attacks against commercial organisations, particularly those involved in scarce natural resources such as minerals and fuel, as well as financial institutions.

Traditionally, APTs had three main objectives: stealing sensitive information, conducting covert surveillance, and sabotaging the target. However, organised criminal groups are increasingly adopting APT techniques for financial gain. This shift means any business with valuable technology, high-value processes, or intellectual property could be a target.

Financial gain is also a motivation for some nation-state actors. These groups are now using more open-source attack tools, making it harder to distinguish them from organised criminals and even more challenging to identify the culprits.

Case study

Nation-state threat group targeting MSP tools

In May 2025, a sophisticated cyberattack targeted ConnectWise, a major developer of remote access software widely used by Managed Service Providers (MSPs). The breach was attributed to a nation-state-affiliated advanced persistent threat (APT) group, continuing a trend of campaigns exploiting trusted IT service ecosystems.

The attackers exploited a critical vulnerability in ConnectWise's ScreenConnect platform, enabling unauthorised access to its cloud infrastructure. Although only a small number of customers were directly impacted, the attack highlighted the systemic risk posed by MSP tools as an entry point into multiple client environments.

After gaining access, the threat actors attempted to leverage compromised credentials and remote monitoring tools. While ConnectWise quickly patched the vulnerability and engaged forensic experts, the incident underscored the growing reliance on MSPs and the cascading impact of their compromise.

Industries at risk included:

- Financial services
- Healthcare
- Telecommunications
- Government and defence contractors
- Technology and cloud service providers

This case reinforces the importance of secure configuration management, real-time monitoring, and vendor risk assessments for organisations using MSP services.

Source: The Register, 2025.

Advanced Persistent Threats

Prevent, detect and respond

How to protect your business

Because APTs use multiple infiltration techniques, there is no single solution. Most businesses are familiar with these techniques individually and can defend against them, but layered protection is essential.

- Robust information security practices and systems can help prevent or detect APT attempts. This includes efficient patching and vulnerability management routines, as well as proactive monitoring for suspicious activity and Indicators of Compromise (IoCs).
- A risk-based approach is key – direct resources to the assets most likely to be targeted and build multiple layers of defence. Employee education is also critical, as spear phishing attacks often target staff to gain entry into systems.
- Understanding how APTs typically work will strengthen your ability to identify and defend against them. Several models outline the stages of an APT attack, with Lockheed Martin's **'Cyber Kill Chain®'** being one of the most widely recognised examples.

Case study

Backdoor into Critical infrastructure

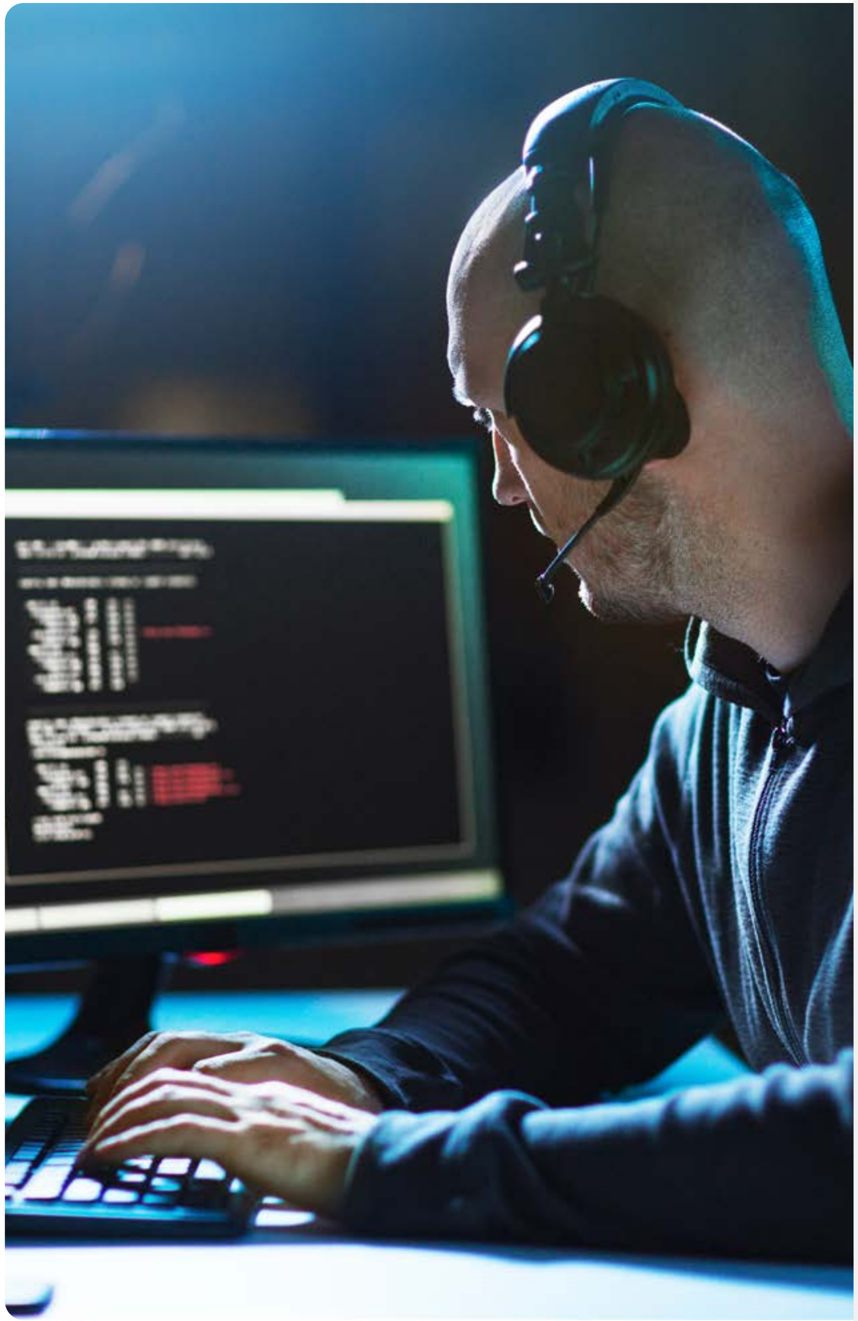
In late 2025, cybersecurity agencies revealed that a Chinese state-sponsored group deployed a sophisticated backdoor called BRICKSTORM to infiltrate critical infrastructure networks.

The malware targeted VMware vSphere and Windows environments, enabling attackers to maintain long-term persistence and stealthy access. BRICKSTORM's capabilities included lateral movement, encrypted tunnelling, and automatic reinstallation if disrupted, making it exceptionally resilient.

The campaign primarily focused on government and IT sector organisations, aiming to gather intelligence and position for potential sabotage. By compromising virtualisation platforms that underpin cloud and enterprise systems, attackers gain control over environments critical to finance, energy, and logistics.

The ability to remain undetected for extended periods means adversaries can strike at moments of maximum impact, turning routine IT dependencies into systemic vulnerabilities.

Source: Computer Weekly, 2019. Fire Eye, 2018



Building cyber resilience: Protect, respond, recover

Cyber risks vary by industry and even between businesses. Your exposure depends on:

- Who might target you and why.
- What they aim to achieve.
- How vulnerable your assets are.

You can’t control attackers – but you can make attacks harder by reducing vulnerabilities.

Cyber threats are evolving rapidly. Protecting your business means preparing for both prevention and recovery. Follow these 10 essential steps to strengthen your cyber security posture.

1. **Train your people**
   Provide tailored security education for every role – from basic phishing awareness to advanced technical and risk management skills.
2. **Identify critical resources**
   Know which systems, data, and processes are vital to your operations. Include third-party dependencies and map what’s needed to keep your business running during a crisis.
3. **Understand your risk appetite**
   Define what level of cyber risk your organisation can tolerate. This helps prioritise investments and response strategies.
4. **Know your threat landscape**
   Consider who might target your business and why. Understand the potential impact of a successful attack.
5. **Manage vulnerabilities**
   Establish an efficient process to identify and remediate weaknesses across people, processes, and technology.
6. **Plan for incidents and recovery**
   Develop and regularly test a cyber incident management strategy with clear roles, escalation paths, and hard-copy playbooks for scenarios like ransomware and supply-chain attacks.

Cyber threats and attacks
Vulnerabilities
Cyber threat management
(Spear) phishing
Distributed Denial of Service attack (DDoS)
Ransomware
Website attacks
Advanced persistent threats (APTs)
Building cyber resilience: Protect, respond, recover
Cyber glossary

7. **Test and certify**

   Consider recognised certifications such as UK Cyber Essentials and review your controls regularly to stay ahead of evolving threats. Align your security approach with established best practices, including the UK Software Code of Practice, NIST, and ISO standards.

8. **Review and update regularly**

   Set up a process to continuously monitor critical business information, data assets, and emerging threats.

9. **Manage financial resilience and risk transfer**

   Consider comprehensive cyber insurance to cover breach response, regulatory fines, and business interruption. Explore **Lloyds' solutions for cyber insurance** and working capital to maintain stability if cybercriminals strike.

   Lloyds Bank plc is an introducer to Arthur J. Gallagher Insurance Brokers Limited who arrange and administer Lloyds Bank Business Insurance Services and source products from a panel of insurers.

10. **Prepare for business impact**

    Consider the potential disruption to working capital and revenue – and make suitable provisions.

Important

If your business falls victim to cybercrime, contact Action Fraud for help.

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, hides 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 make sure only authorised parties can read it. Decryption needs 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.

Industrial Control System (ICS)

A general term that includes various types of command and control systems mainly 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 get 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 for 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 seems 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.

Vishing (Voice or VoIP phishing)

A social engineering technique using telephone calls to scam users into revealing 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

Visit **lloydsbank.com/business/help/cyber-risk**

Contact your Relationship Manager

Business help and support

We aim to provide you with a high level of service. If you have a query our Help & Support pages can help: **lloydsbank.com/business/help**

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

Important information

Lloyds and Lloyds Bank are trading names of Lloyds Bank plc. Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales no. 2065. Telephone: **020 7626 1500**.

Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under Registration Number 119278.

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 Lloyds Bank. 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 Lloyds Bank 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.

LLOYDS