



Introduction to cyber security and cyber risk

What is Cyber?

Cyber – a word that, a few years ago, was new to many of us. These days, however, we are at the point of information overload.

The word cyber is put in front of other words often without context or meaning. For example, cyber security, cybercrime, cyber threat, cyberattack and so on. But what really is cyber?

Cyber, by its dictionary definition, denotes information technology (IT) devices and all tasks and actions completed. This includes collecting, storing, processing, transmitting, accessing, and linking data. Cyber by itself describes all actions we complete on our business and personal electronic devices.

In its simplest form, it is anything we do on a device that is connected to the internet. This is something we all do a lot at home and at work.

Cyber security is defined as precautions taken to protect against crime that involves the internet, especially unauthorised access to computer systems and data connected to the internet.

Newer to the industry is the concept of resilience, specifically **cyber resilience**.

The government definition describes 'cyber resilience' as the ability for organisations to prepare for, respond to and recover from cyberattacks and security breaches. Cyber resilience is key to operational resilience and business continuity, as well as the growth and flourishing of the UK economy.

With so much information available, it can be difficult to know where to look and which solution is best for your business. At Net-Defence, we are striving to simplify cyber security, making it affordable, attainable, and available to all.

The **core principle**? Prevent, detect, and respond to potential and actual threats and incidents to your IT infrastructure, systems, and data.

This is where our Business Resilience as a Service comes in. Designed to be fully flexible to suit your organisation's vulnerabilities and challenges, it allows you to create a custom package made up of core and supplementary services.

What is a cyberattack?

A cyberattack is a malicious attempt to access your business or personal computers, mobile phones, gaming systems and any other device that is connected to the internet or Bluetooth-connected devices.

Types of attack:

- **Malware:** A file or code that infects your infrastructure to perform any action the attacker wants.
- **Phishing:** A social engineering attack to steal data (e.g. log-in credentials, financial information).
- **Spear phishing:** Like phishing, this is a socially engineered attack targeted to one individual.
- **SQL injection attack:** Used to gain unauthorised access to web application databases by adding malicious code.
- **Cross-site scripting (XSS):** Injects malicious executable scripts into the code of a trusted application or website to steal data such as credentials and financial information.
- **Denial of service (DoS):** An attack to shut down a machine, network, or website, making it inaccessible.
- **Business email compromise (BEC):** An attacker has control or access to a genuine email account and uses this maliciously.
- **Credential reuse:** The attacker is able to obtain valid credentials for one system and then tries to use the same credentials to compromise other accounts or systems.

Cyber risk

Now that we have clearly established what cyber is, we can explore cyber risk and what this means.

What is a risk?

- Exposure to the chance of injury or a loss.
- A situation involving exposure of a chance of danger or hazard.

Cyber risk

Cyber risk is the chance of exposing business information and communication systems to an unauthorised person or circumstances that could lead to loss or damage.

Risk implies the likelihood or probability of an event occurring.

Therefore, this is the risk-based probability of a bad event happening to your business information systems, leading to the loss of confidentiality, integrity, or availability of your system.

Risk can originate from anywhere, including an attack, a 3rd party vendor or supplier with weak security, or internally from a rogue employee, by accident or from failure to adopt security best practices.

Risk assessment:

The industry standard for assessing IT systems and applications is known globally as the CIA Triad. This is made up of 3 key concepts: Confidentiality, Integrity & Availability.

This is also part of Business Continuity Planning (BCP) and Disaster Recovery (DR) processes.

- **Confidentiality** (access control): Confidentiality means ensuring that information is accessible only to those authorised to have access.
- **Integrity** (accuracy): Integrity means safeguarding the accuracy and completeness of the information.
- **Availability** (accessibility): Availability means ensuring that authorised users have access to information and associated systems when required.

Risk can either be **accepted**, **mitigated** or **transferred**.

We all manage risk like this in our everyday life, most likely subconsciously.

We do this by protecting our homes with everything from door locks and alarms to CCTV and 24/7 security. We decide what we need based on risk and how much we can live with so that we can enjoy life without worry.

To protect our children, we teach them from day one about safe behaviours, such as how to cross the road and so on. Again, we decide this based on risk factors.

Every organisation also operates with risk; some are more familiar than others, such as health and safety and financial risk. In a world where data is king, and protecting it is critical to your ability to continue to operate, IT and information security risk cannot be ignored

Net-Defence

Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 ONF • Ogilvie House, 200 Glasgow Road, Stirling FK7 SES
Tel: 03300 241 666 • Web: net-defence.com

Probability & who is at risk?

As I meet with customers, suppliers, and peers this is a question that is becoming the most asked: "Who is at risk and why?"

In the cyber security sector, the world has moved on from the thought process of "if" an attack will happen to "when" it happens. So, which sector has the greatest target on its back?

Before I get into more detail, you need to get a little into the mindset of the cybercriminal. Who are they, why are they attacking and what is the aim of their attack?

Who are they?

- **State-sponsored threat actors:** these are often funded by hostile foreign governments.
- **Hacktivists:** their purpose is to further social or political objectives.
- Individual or teams of cybercriminals out for their own gain.

Why are they attacking?

- Financial gain
- Data theft
- Large-scale service interruption
- Raise awareness of social and political issues
- Individual kudos

Mostly, they want to access:

- Businesses' or customers' financial information
- Sensitive personal data
- Customers' or staff members' email addresses and login credentials
- Customer databases and clients lists
- IT infrastructure
- IT services (e.g. the ability to accept online payments)
- Intellectual property (e.g. trade secrets or product designs)

According to current reporting, the sectors at greatest risk are:

- Health (17%) 5,520
- Education and childcare (16%) 5,477
- Manufacturing and retail (12%) 3,871
- Local government (10%) 3,361
- Charitable and voluntary (8%) 2,777

UK Statistics (2024 Proofpoint State of the Phish report & UK Cyber Breaches Survey)

- 73% of organisations experienced a Business Email Compromise (BEC) attack in 2023, yet only 29% train users specifically on BEC threats.
- 69% of organisations suffered a ransomware attack, with almost 60% reporting four or more incidents in the year.
- Email remains the most common delivery method for attacks, with phishing the most prevalent type across global data sets.

Net-Defence

Top three threats by prevalence in 2023 (with high likelihood to continue in 2024 and beyond):

- BEC (Business Email Compromise) – detected in 66 million attacks per month
- Ransomware – affected 69% of organisations globally
- Supply Chain Attacks – seen by 67% of respondents

Email impersonation/spoofing and social engineering tactics remain major issues:

- 58% of users who took a risky action said it made them vulnerable to phishing or impersonation.

Threat actor tactics are evolving:

- A rise in TOAD (telephone-oriented attack delivery), MFA bypass attacks, and QR code-based phishing.
- Generative AI is being leveraged to craft more convincing BEC emails, especially in non-English-speaking countries.

Risky behaviour is widespread:

- 71% of users admitted to taking risky actions, and 96% of them knew it was risky when doing so.
- Common risky actions include reusing passwords (26%), clicking unknown links (19%), and using work devices for personal use (29%).

In summary, **no sector is safe**. Even charities and not-for-profit organisations are targets!

But the good news is that cyber and information security is not complex or expensive, despite what you might have heard. Preparation and prevention are your best allies in this battle.

Prepare: Preparing a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRC), will ensure you will be ready to act if you suffer from an attack.

Prevent: Risk assessments and action plans are the best way to identify and mitigate risk. This can be done through the Cyber Essentials Scheme and IASME Governance Certifications. These are government, GCHQ, and NCSC-backed schemes to protect organisations from the most common cyber threats and loss of IT.

What can you do to avoid becoming another statistic in the next report?

- **Cyber Security Awareness Training:** Your employees are your best line of defence if your IT systems don't stop the threat.
- Simulated phishing and other email-based attacks to test and educate your employees.
- Information security incident response protocols can be put in place for reporting and issue handling.

There are some simple steps you can take today to ensure you are better protected under the current heightened threat, and any new threats that may emerge:

- Check your systems for patching and updates.
- Review and verify access controls, particularly for admin and privileged users.
- Test and review your current defences.
- Review your monitoring.
- Review and test your backups and recovery.
- Information security and phishing training for all employees.

Net-Defence

These steps and others are included in the Cyber Essentials scheme. This is an effective, government-backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyberattacks.

1. Acceptance: The cost of doing nothing

With any risk you have 3 decisions to make: **accept**, **mitigate**, or **transfer**.

If you choose to accept risk without assessment, what is the cost of doing nothing if the worst happens?

- **Loss of ability to operate:** Average downtime after an attack or hack is reported to be around 21 hours. If this is a result of ransomware, it is more likely to be days rather than hours. The average global lifecycle of a breach from attack through to recovery and reporting is 277 days.
- **Loss of reputation:** Something that can be lost in seconds with the click of a button, and can be potentially unrecoverable, is your reputation. 85% of data breaches involve a human element.
- **Financial penalties:** The average ICO fine is now around £258K, with public-sector penalties climbing up to £750K and corporate fines in the tens of thousands. These regulatory penalties frequently pave the way for private data protection claims.
- **Failure to win new business:** More and more organisations are required to hold accreditations and certifications and, without these, can be excluded entirely for tendering and bidding.
- **Wasted effort:** Digitise the process to be 50% more efficient and in full control.

If you didn't prepare for an attack, how do you respond? What do you do first?

Identification and **resolution** are the 2 priority tasks.

Indications that an issue could be occurring include:

- Computers running slowly
- Users being locked out of their accounts
- Users being unable to access documents
- Messages demanding a ransom for the release of your files
- People informing you of strange emails coming out of your domain
- Redirected internet searches
- Requests for unauthorised payments
- Unusual account activity

Identification: What is actually happening? Information gathering needs to happen as soon as an issue is suspected. This needs to be collated and/or shared with your IT team.

10 crucial questions:

1. What problem has been reported, and by whom?
2. What services, programmes and/or hardware aren't working?
3. Are there any signs that data has been lost? For example, have you received ransom requests, or has your data been posted on the internet?
4. What information (if any) has been disclosed to unauthorised parties, deleted, or corrupted?
5. Have your customers noticed any problems? Can they use your services?
6. Who designed the affected system, and who maintains it?

7. When did the problem occur or first come to your attention?
8. What is the scope of the problem? What areas of the organisation are affected?
9. Have there been any signs as to whether the problem has occurred internally within your organisation or externally through your supply chain?
10. What is the potential business impact of the incident?

Stop the incident from getting any worse

Take a look at your security software such as antivirus alerts and server/audit logs. Can you identify attack specifics and the potential cause?

If you know which device has been affected, take this offline and run your antivirus programme to complete a full scan⁹, and take notes of the results it gives you.

Use the information you have gathered to look for advice online from trusted sources such as police or security websites.

In the case of internet outage, contact your ISP in the first instance; most will have pages that relate to service availability.

Resolution:

Use the information you have gathered to look for advice online from trusted sources such as police or security websites. Take extra care that any advice is from a verified and trusted source only!

If your IT is managed externally, share information you have identified and work with them to resolve the issue where possible. Check your support contract to understand what they are responsible to action and in what time frame.

Working to resolve the issue can include:

- Replacing infected hardware
- Restoring service through backups
- Patching software
- Cleaning infected machines
- Changing passwords

If you lack the internal expertise for complex incidents, consider using the services of a Cyber Security Practitioner. Make sure they are from a reputable organisation and hold appropriate credentials.

2. Mitigation: The cost for doing something?

Mitigation covers how you reduce your risk to prevent attacks. The secret to surviving an attack is to prepare for it. This is not as complex as you might think it is.

First, you should prepare a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP), as this will ensure you are ready to act if you suffer from an attack.

Secondly, prevention is the best form of defence. Completing risk assessments and action plans is the best way to identify and mitigate risk. This can be done through the Cyber Essentials Scheme and IASME Governance Certifications.

Preparation

This falls into two areas:

Business Continuity Planning (BCP) is about having a plan to deal with difficult situations, so your organisation can continue to function with as little disruption as possible. This plan needs to account for people, locations and processes based on criticality.

Disaster Recovery (DR) is a plan designed to recover your IT and infrastructure after a disaster. A DR plan comprises recognising crucial IT systems and networks, categorising the RTO, and reporting the activities required to resume, reconstruct, and recover IT systems and networks.

DR is part of the overall BCP.

Business Continuity: People and locations

Input required is to understand the critical employees, critical time periods and your dependency on your offices.

The definition of critical in this instance: Would causes severe operation problems.

1. People

Employees in your organisation that you would classify as critical every day or at certain times in the month?

2. Critical time period/task

Which critical processes and tasks do you have within the month?

3. Locations

Does your business rely on being able to physically access your current office?

Business continuity – IT systems

- **Recovery Point Objective (RPO)** is the tolerable amount of data the organisation is prepared to lose.
- **Recovery Time Objective (RTO)** is the amount of time needed to recover the critical systems and applications.

Prevention

Cyber Essentials Certification gives you peace of mind that your defences will protect you from the vast majority of common cyberattacks, simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place.

Cyber Essentials Plus gives you the added reassurance of an independent assessment.

Scope/controls:

- Firewalls
- Secure configuration
- User access control

Net-Defence

Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 0NF • Ogilvie House, 200 Glasgow Road, Stirling FK7 5ES
Tel: 03300 241 666 • Web: net-defence.com

- Malware protection
- Security update management

The **IASME Cyber Assurance** was developed over several years during a government-funded project to create a cyber security standard which would be an affordable and achievable alternative to the international standard, ISO 27001.

The IASME Cyber Assurance standard allows small companies in a supply chain to demonstrate their level of cyber security for a realistic cost and indicates that they are taking good steps to properly protect their customers' information.

The IASME Cyber Assurance Level 2 gives the added reassurance of an independent assessment.

Scope/controls

- Risk assessment
- Backup
- Policies
- Incident management
- Data protection
- Operation management

3. Transference: cyber insurance

With the changes to the UK Data Protection Act in 2018, the ability to transfer risk is now limited to insurance.

It has been widely publicised that 2020 & 2021 were very turbulent for insurers; they were significantly unprofitable across the globe. This forced carriers to slow down and, in some cases, halt underwriting new businesses, reducing limits and coverage for renewals.

In the last 2 years, this have gone through another evolution. The market has stabilised and competition in the providers has resulted in more favourable terms for the buyers. Despite this, overall claims continue to increase in volume and value.

Changes during 2024 include:

- Gallagher, a global insurance, risk management, and consulting firm, reports that cyber insurance rates have continued to stabilise, with rates remaining flat or declining across much of the market due to increased competition among carriers and improved cyber risk hygiene among insurers.
- Claims frequency has increased, largely driven by a resurgence in ransomware activity, which spiked by 95% in Q3 2023 compared to the prior year. However, while claim frequency rose, claim severity remained somewhat contained, thanks to improved security controls by organisations and more disciplined underwriting.
- Coverage limits and capacity continued to expand in 2024, as insurers regained confidence in the market. Reinsurers played a critical role in this expansion, supported by innovative use of cyber catastrophe bonds and insurance-linked securities.

Looking forward:

- **Underwriting:** Due diligence and focus on IT controls will continue, with increased reliance on advanced modelling tools to predict cyber events.
- **Limits:** While not explicitly stated as continued reductions, carriers are expanding war exclusions and imposing sub-limits for systemic events.

Net-Defence

- **Price:** Despite 2023's flat or declining rates due to competition, carriers face challenges maintaining profitability as the average cost of a data breach reached an all-time high of \$4.35 million in July 2023.
- **Coverage:** Exclusions are expected to increase, particularly for war and systemic risk, regulatory issues, and wrongful data collection claims.
- **State of the market:** The cyber insurance market is expected to continue its expansion in 2024 and beyond. While it has matured, underlying concerns about systemic cyber risk and catastrophic events persist.

Cyber insurance is designed to cover against a cyber event – this is a malicious action or an accidental event on an organisation's digital systems, data, or technology.

Impact of an event:

- **Non-physical:** Compromise of the confidentiality, integrity and/or the availability of digital systems, data and or technology.
- **Physical:** Property damage and/or bodily harm and injury.

Consequence of an event:

- Loss of income
- Extortion/ransom demands
- Fines and penalties
- Negligence
- Shareholder litigation
- 1st party costs (insurance)
- 3rd party liability (if the organisation is sued)

The **due diligence** process includes a review of your cyber resilience. These are 12 key information security controls. While they have been established for several years and considered best practices, many organisations have not adopted them.

The 12 controls:

- **Multifactor authentication:**
 - Additional electronic identity authentication
- **End Point Detection & Response (EDR):**
 - Solution to detect and respond to attacks on end point devices (e.g. anti-virus).
- **Backups:**
 - Secure, encrypted backups, stored in a separate and secure location.
 - Tested (monthly) for recovery.
- **Privileged Access Management (PAM):**
 - Information security mechanism that safeguards identities with special access or capabilities beyond regular users.
- **Network protection:**
 - Network security protects your network and data from breaches, intrusions, and other threats.
- **Email filtering & web security:**
 - Email scanning to for undesired content, categorising (e.g. spam, junk, virus, and malware) and taking specific actions

(e.g. block, move to junk).

- Web filtering is restricting access to certain websites or those that have malicious content.

- **Patch & vulnerability management:**

- Vulnerability management refers to the process of discovering, identifying, cataloguing, remediating, and mitigating vulnerabilities found in software or hardware.

- Patch management refers to the process of identifying, testing, deploying, and verifying patches for operating systems and applications found on devices

- **Cyber incident response planning & testing:**

- Incident response is a term used to describe the process by which an organisation handles a data breach or cyberattack, including the way the organisation attempts to manage the consequences of the attack or breach.

- **Cyber security awareness training and phishing testing:**

- Information Security Awareness Training: Your employees are your best line of defence if your IT systems don't stop the threat.

- Simulated phishing and other email-based attacks test and educate your employees.

- **Hardening techniques including Remote Desktop Protocol (RDP):**

- Hardening refers to processes that reduce means of attack by taking specific actions (e.g. turning off non-essential services).

- Remote Desktop Protocol (RDP) is a secure connection that enables IT support to remotely diagnose problems that individual users encounter and gives users remote access to their physical work desktop computers.

- **End of life management:**

- Protocols and processes to ensure that when hardware and software that is no longer maintained or supported, it is removed/replaced.

- **Vendor/digital supply chain risk management:**

- Processes to identify, assess and mitigate risk in your end-to-end supply chain with the intended to prevent issues and loss mitigation if issues do occur.

The 12 controls are assessed as part of risk assessments completed through Cyber Essentials Scheme and IASME Cyber Assurance Certifications, designed to protect organisations from the most common cyber threats and loss of IT.

What is not covered by cyber insurance?

Cyber insurance does not transfer all risk, and it is not a substitute for having robust cyber risk management in place.

It will allow some costs from an incident to be recovered, it can provide specialist to manage the immediate crisis, and it can sometimes allow a ransom payment to be made.

There are several issues that may not be resolved by having insurance in place. These include:

- The cost of time lost in resolving the issue.
- The cost of loss of ability to operate (fee earners being unable to work)
- Loss of reputation
- Impact of explaining to clients that their data has been breached

- Time lost in reporting the incident to the Information Commissioner's Office (ICO), the Solicitors Regulation Authority (SRA) and law enforcement agencies

The National Cyber Security Centre (NCSC) notes: "Cyber insurance will not instantly solve all of your cyber security issues, and it will not prevent a cyber breach/attack. Just as homeowners with household insurance are expected to have adequate security measures in place, organisations must continue to put measures in place to protect what they care about."

Whether you need insurance or not, ensuring your organisation has the 12 controls in place is the best way to improve your information security posture and resilience.

Cyber Essentials Plus and IASME Cyber Assurance certifications address these controls and more through self-assessment.