PUT SIMPLY

Jersey Finance
Delivering Insight • Driving Innovation

Cyber and Data Security

Cyber and data security are commonly used terms in an area that can be complex to understand. In this Put Simply, we aim to provide clarity on the subject, define the most commonly used terms, and explain how businesses can protect themselves from risks.

What is cyber and data security?

Cyber security relates to computers and technology and preventing these systems from unauthorised access or misuse. It includes designing, implementing, and maintaining policies, controls, and safeguards which may include IT solutions to protect people and organisations from attack.

Data security is an area which focuses specifically on the standards, policies, and technologies which seek to protect all forms of data that an organisation has collected. This could include information about clients, staff and business operations. Data security is not just about information held on computer systems but also includes paper records and files. Data security and information security are often commonly used interchangeable terms. Both terms mean protecting information in a responsible manner.

Glossary

anti-virus software - security software designed to monitor computers. When malicious activity is detected, the software will attempt to identify and remove the offending item from the system or may isolate the file for further analysis.

audit trail - a record showing who has accessed a system and the activity they undertook.

authentication - verifying that someone is who they claim to be when they access a computer or online service.

back-ups - making a duplicate copy of data onto a separate device or online/cloud storage solution which allows for damaged or lost data to be restored from the back-up.

bot - programs which perform automated tasks, this could include repeated activity as part of a cyberattack.

bug - an error or mistake in software or hardware which causes things to perform in an unexpected way. A bug represents a flaw or weakness which is discoverable by attackers and can be used as point of attack.

How do organisations protect themselves and their employees?

Each organisation's businesses, systems and people are different and there is no set way of ensuring total protection. Organisations will implement a combination of cyber and data security measures that align to the areas which are most important for them to protect. In addition to technology solutions, some of the best forms of protection are through policies and people.

Policies

Dedicated Information Security Policies are written accounts of security plans which organisations implement. Internal policy and procedure documents are those designed to inform employees and contractors of the legal, regulatory, or internal company standards and acceptable behaviours that must be met to ensure the organisation protects itself from cyber and data security risks. Examples of internal policies include acceptable use, IT systems access including remote access, application of patches and bug fixes, classification of types of data, confidentiality, data storage and back-ups.

People

Protecting employees from causing actual or unintended action against the organisations policies is key to helping an organisation protect itself. This can include staff training and accreditation, testing staff and acting on the results to improve awareness, ensuring robust building access controls are in place and challenging strangers, plus monitoring or even blocking access to external websites known to have weaknesses. It is crucial that employees are aware of what to look out for and that they can report anything that appears suspicious.

Organisations and software providers can also publish external policies such as those defining their use of client data in either dedicated policies or as part of their terms and conditions.

Chief Information Security Officer (CISO) – a senior person in an organisation responsible for maintaining adequate information security protection.

cyberattack — an attack initiated using software or hardware weaknesses such as bugs. Cyberattacks are focused on gathering information, damaging business processes, exploiting flaws, discreetly monitoring targets, or interrupting business tasks.

cybercrime – organised criminal activity which has the intent to conduct illegal activity to cause disruption, harm, or exploitation.

DDoS – a distributed denial of service attack is an attempt to disrupt normal IT operations by using bots or infected computers to flood a system with so much traffic it fails e.g. multiple website visits beyond normal tolerances which case the website supporting systems to crash.

disaster recovery plan – a plan of policies, actions, and responsibilities to be followed which will allow an organisation to resume normal operations following a disaster or occurrence which has impacted operations.

dumpster diving – searching through rubbish and discarded information or media in an attempt to find information.

firewall – a system that monitors network traffic and blocks undesirable network traffic based on a set of defined rules.

Are there any recognised standards?

Yes, to support organisations in protecting themselves, their people, and the information held, frameworks and standards have been created. The most common of these are:

- **ISO 27001** – published by the International Standards Organisation, ISO 27001 is an information security standard which provides a management and control specification along with mandatory control documents which organisations can follow to identify and then act upon to reduce risk. Organisations can choose to be assessed by an external body to formally be recognised as an ISO 27001 accredited entity. Further reading is available on the ISO Information Security Management website.

- **NIST Cybersecurity Framework** – a voluntary framework which consists of standards, guidelines and best practices from the US National Institute of Standards and Technology. NIST provides a structure to help organisations manage and reduce risk. Although originating from the US companies from around the world have embraced the use of the framework, including JP Morgan Chase, Microsoft, Boeing, Intel, and the Bank of England. To learn more please visit the NIST Cybersecurity Framework website.

- **Cyber Essentials** – Cyber Essentials is a UK Government backed scheme that helps firms guard against common threats and show a commitment to cyber security by undertaking self and then independent assessment of cyber security risks to their organisation. Cyber Essentials is becoming increasing popular in Jersey across all sectors not just finance, more information can be found on the Government of Jersey's Cyber Essentials page.

hacker - someone who can analyse weaknesses in systems or controls to gain access to virtual or physical information, to cause damage, or to disrupt services generally for personal gain or as part of criminal activity.

insider threat – a threat arising from an individual within an organisation undertaking unauthorised activity.

malware - the shortened version of 'malicious software' which is written for the specific purpose of causing harm, disclosing information or causing disruption. Malware includes a wide range of types of malicious programs including virus, worm, Trojan horse, logic bomb, backdoor, rootkit, ransomware and spyware/adware.

network – interconnected IT systems of more than two computers that can share resources and applications.

patch – a software update released by a software company which repairs bugs and vulnerabilities discovered after the product has been released. Ensuring patches are applied to repair the vulnerabilities is one of the strongest ways of reducing the threat or impact of a cyberattack.

These standards are recognised around the world. Accredited organisations can provide reassurance to their clients by demonstrating that they are following a recognised standard.

How do people work together?

The cyber security professionals and information security community actively collaborate to share ideas and best practice. Cyber criminals and organised crime often work in isolation and working together is a key way of fighting back.

The Government of Jersey lead a Cyber Security Task Force where key bodies and agencies including Jersey Finance work together to undertake activities which help protect Islanders, Jersey's key infrastructure, and the economy.

The UK National Cyber Security Centre recognise that working together is vital and they operate a Cyber Security Information Sharing Partnership (CiSP). There is a dedicated Channel Islands CiSP portal where approved professionals can exchange cyber threat information in real time, in a secure, confidential and dynamic environment, this increases situational awareness and helps reduce the impact on businesses.

What are Jersey firms required to do?

The Jersey Financial Services Commission (JFSC) and the Jersey Office of the Information Commissioner have detailed information available to support people wishing to find out more information. Please see their websites for the latest guidance and information.

phishing - an attack that attempts to collect information from victims often by mimicking communications from legitimate parties. Phishing attacks can take place over email, text messages, through social networks or via smart phone apps. The goal of a phishing attack may be to learn logon credentials, credit card information, system configuration details or network, computer or personal identity information.

ransomware - a form of malware that holds a victim's data hostage on their computer, typically by locking the system or files using encryption. This is followed by a demand for payment in order to release control of the captured data back to the user.

RBAC - role based access controls, a set of authorisations and access permissions based on a specific role and the work needed to be undertaken.

social engineering - an attack focusing on people rather than technology. This type of attack aims to manipulate people to either gain access to information or to a location. Examples of social engineering attacks are by tricking a worker into assisting with building access by holding open a door to a restricted area, or by gaining access to information or a computer network by tricking a user into revealing their account details or passwords.

spam – emails sent to a large number of individuals typically for the purposes of advertising, phishing, or spreading malware and other viruses.

What is a data breach?

The Jersey Office of the Information Commissioner (JOIC) defines a data breach as:

"A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data."

Data could include information such as names, addresses, contact information, credit card or bank details, location or even biometric data.

There is no standard way in which an organisation can suffer a data breach making policies, procedures, and training of employees crucial. Examples of causes of breaches are where an employee could case an accidental data breach by losing a laptop or client file, by sending an email to the wrong person, or they could deliberately cause a data breach by leaking, email or copying data to an unauthorised source. An organisation could also be breached from an external source that breaks into their premises to access information, uses a malicious cyber-attack, or ticks an employee into revealing data via social engineering.

Under the Data Protection (Jersey) Law 2018, organisations who have incurred a data breach must notify the JOIC within 72 hours of becoming aware of the breach.

Additionally, organisations regulated by the JFSC are bound by the relevant laws and Codes of Practice to disclose information that is relevant to the JFSC's supervisory role, that might affect the person's registration, and that may be of interest of its clients or investors to disclose.

trojan – named after the Greek Trojan Horse legend, a Trojan is a type of virus or malware that is disguised as a legitimate file to trick users into opening it at which point it installs malicious code intended to cause damage.

unauthorised access - any access or use of a computer system, network, or resource which is against company security policy or when the person was not explicitly granted access authorisation.

virus - malicious software designed to cause damage or disruption which is installed on a computer without the user's knowledge. Viruses can be installed in many ways, the most common are through accessing or downloading infected files. Once installed the virus can spread to other computers in a network.

vishing – similar to phishing but specifically uses voice systems such as telephone scams to trick users into revealing key sensitive or personal information.

vulnerability - any weakness which would allow for a threat to cause harm. It may be a flaw in coding, a mistake in configuration, or a clever abuse of valid systems and their functions.

zero day – generally defined as attacks that target known bugs or system vulnerabilities that have yet to have fixes made available.

Where can I find more information?

For more information on cyber and data security or fintech visit our dedicated Jersey Finance fintech page.

Government of Jersey – the Government of Jersey's Be Safe Online pages contain cyber and data security tips and best practice for businesses and Islanders.

Jersey Office of the Information Commissioner – the JOIC provides comprehensive information on data protection for organisations and individuals on all aspects of privacy and information rights of individuals in or with data held in Jersey on their website.

Jersey Financial Services Commission – further information on how firms can understand their cybersecurity regulatory obligations can be found here.

National Cyber Security Centre – the UK National Cyber Security Centre has a guidance page which provides 10 steps to cyber security.