COMMERCIAL BANKING

CYBER SECURITY GUIDANCE

LLOYDS BANK

The threat from cyber on all businesses is constantly growing. This guidance provides some steps that can help you safeguard your business, employees and assets from these attacks.

Contents

Cyber threats

Protecting your business

68%

of large firms have experienced a breach or attack in the last year (Department for Culture, Media and Sport, 2017).

$450 billion

the cost of cyber-attacks to businesses globally in 2016 (Lloyd's of London/Cyence).

This guide offers insight to assist in building your awareness of and protecting your business from the increasing number and sophistication of cyber threats.

It highlights commonplace cyber attacks and offers suggestions to help safeguard your business, employees and assets from these threats.

> Cyber crime is a dynamic threat that can have a major impact on an organisation of any size. Business leaders are having to rapidly adapt to prepare their businesses to protect, respond and recover from cyber attacks. It is crucial to give consideration to operational, media, legal and financial planning in addition to 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 Data and Cyber Security, Lloyds Commercial Bank

Protecting your business

What are cyber threats?

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

The range of cyber threats is constantly evolving, but most of them involve attacking the **confidentiality, integrity or availability** of data or systems.

Consequences of cyber attacks are often much wider than a local IT or fraud issue, they can have a significant impact on a business, including reputational damage to the brand, for instance through the loss of customer confidence.

Other consequences can include legal or regulatory sanctions, particularly if large quantities of customer data is stolen and regulators find that business controls are not sufficient from a data privacy perspective.

Case study: Reputational impact of cyber attack

A major internet service company reported two data breaches during the second half of 2016 affecting over 500 million and 1 billion customers. The company is now facing several lawsuits as well as government scrutiny and it has reportedly impacted the acquisition by another company, with the price of the deal reducing by $350m.

Who are the culprits?

Attackers are generally grouped into categories, based on their motivations and capabilities, collectively known as 'Threat Actors', including:

1. **Hacktivists:** Politically or ethically motivated groups and individuals using cyber attacks to get a political message across. These groups tend to be loosely organised and target websites in order to deface them or take them offline.
2. **Criminals and Organised Criminal Groups (OCGs):** This category can range from a few individuals operating on their own to large OCGs. They are financially motivated and often use phishing and malware to obtain log-on credentials to online banking services or accountancy systems in order to steal money. They are responsible for stealing billions of pounds from consumers and businesses each year.
3. **Nation States/State Sponsored:** Government-funded and guided attackers, primarily focused on the theft of intellectual property or confidential government information. These attackers are often well-funded, and well-resourced and attract high level talent in order to create and deliver the most sophisticated threats.

Whilst cyber attacks are often perceived as an external threat, **insiders** are often involved in an element of the attack, sometimes maliciously, but often by being manipulated by criminals to divulge information or perform a specific task.

Vulnerabilities

How the attackers get in

What are vulnerabilities?

Attackers seek to gain access to systems through vulnerabilities in a business' systems, their processes or their people. Vulnerabilities occur through **flaws, features** or **user error**, and attackers will exploit any combination of these to succeed.

Flaws: Flaws or unintended functionality are typically found in software, a vulnerability exploited regularly in cyber attacks. Fixing known flaws is a process known as 'patching'. However, flaws can often go undetected for significant periods, until a fix or patch is released by the vendor.

Features: Functionality intended to automate or simplify the use of computers or mobile devices can be misused by an attacker in order to breach a system.

For example, the macro feature in spreadsheet and word processing applications enables a user to automate frequently performed tasks or perform complex calculations. This functionality can also be used by attackers 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 via a secure build, a significant vulnerability can remain through user error (i.e. a systems administrator who enables vulnerable features by mistake or fails to fix a known flaw.) Protected information can be divulged, either intentionally or not, by users' actions.

Why are they so valuable?

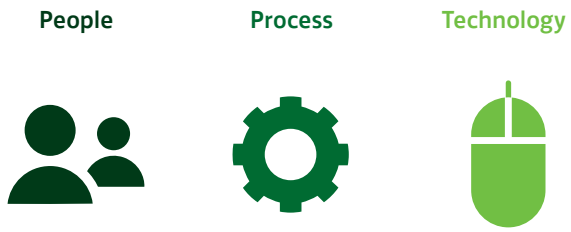
The lifecycle of a vulnerability has changed significantly over the years and they are now actively pursued and exploited by the full range of attackers.

There is now an active criminal market that buys software flaws, with 'zero-day' vulnerabilities (i.e. recently discovered vulnerabilities that are not yet publicly known) fetching hundreds of thousands of pounds.

Having a proactive vulnerability management process is therefore a critical element of defence against cyber attacks.

It is important to ensure that cyber threats and vulnerabilities are addressed through your people and processes, as well as by using technology.

Protecting your business from cyber threats



Cyber threat management

User Education and Awareness

Produce policies covering acceptable and secure use of the organisation's systems. Establish a training programme. Maintain user awareness of the cyber threats.

Network Security

Protect your networks against external and internal attack. Manage the 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 and ensure that the secure configuration of all IT systems is maintained.

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.

Malware Protection

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

Social Media

Implement a social media policy for employees. Educate users to consider what they post online, particularly due to the risks from discussing work-related topics on social media, which could result in being targeted by (spear) phishing attacks.

Incident Management

Establish 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

Establish 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

Establish 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.

> "Establish 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?

An email scam when fraudsters masquerade as a bank or other trusted organisation to obtain confidential information such as personal information, bank details or passwords. The message typically highlights the need for urgent action, suggesting for example that online access will be blocked unless a link is followed. The email will typically link through to a fake website which looks almost identical to the real one. This website will then entice the victim to enter log-on credentials or download malware.

What is spear phishing?

Spear phishing is a targeted form of a phishing attack. Spear phishers generally disguise themselves as a legitimate, familiar sender, often from within the same organisation, to increase the chance the recipient will carry out the intended action.

This could include opening the attached file or visiting a website which would typically download malware, divulging sensitive personal or commercial information or being duped into completing a transaction e.g. making a payment.

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

Case study: Simple but effective

Over the period 2015-2017, phishing techniques were used to influence two major US-based multinational companies to transfer in excess of $100million to accounts controlled by a fraudster. A Lithuanian man was arrested in early 2017 and has subsequently been charged by the US Department of Justice.

How to protect your business?

Employee education and awareness – Educate users of the risks associated with opening files or visiting websites via links in emails – even when the email appears to originate from a colleague. Also 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, ensuring privileges are limited to those required to perform their role. Restrict privileged accounts and the ability to run executable files*, especially if not required for their role.

Secure configuration – Known as 'hardening', minimise the potential attack surface on users' devices by having a secure 'build', ensuring (amongst other things) that unnecessary software and default user accounts are removed.

Software patch management – Ensure patches are applied 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 relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Consider having a separate device to undertake online banking activities that does not 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.

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

Distributed Denial of Service attack

Attacking your online availability

What is a Distributed Denial of Service attack?

A Denial of Service (DoS) attack is an attempt to make an online resource, such as a website, unavailable to its intended users by overloading it with internet traffic.

A Distributed Denial of Service (DDoS) attack is a specific class of DoS where the attack originates from multiple sources, often using a huge network of computers infected with malware, known as a 'botnet'. This allows the attacker to create a much larger volume of internet traffic against the target and helps to hide its origin.

Historically, only a skilled individual was able to conduct a DDoS attack as it required a keen understanding of internet and system infrastructure. However in recent years, tools have been made available on the Dark Net* which, for a relatively modest fee, allow an unskilled individual to hire a botnet and conduct an attack on the target of their choice. The strength and ease of administering a DDoS attack has also increased, partly in thanks to competition amongst hackers, the cheap cost to launch (just $25 per hour) but also via powering attacks through internet of things (IoT) devices.

As well as undertaking DDoS attacks for political or ideological reasons, cyber criminals have also been known to threaten companies with DDoS attacks unless a ransom demand is paid.

The victim company will usually receive extortion emails demanding payment (usually in the cryptocurrency Bitcoin), otherwise they will carry out a DDoS attack against the victim's network. DDoS attacks can also be used as a smokescreen to distract defences from other attacks such as a data breach or unauthorised access to a network.

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 and what controls they have in place. There are various mitigation techniques that could be combined in an attempt to counter the effectiveness of these attacks including:

- **Buying excess bandwidth** from your Internet Service Provider.
- **Configure routers and firewalls** to stop simple attacks by filtering non-essential traffic and blocking invalid IP addresses. However, these are typically ineffective against more sophisticated attacks.
- **Intrusion-detection systems** can be used in conjunction with firewalls but this is not an automated process; requiring manual tuning by security experts, they often generate false positives.

However, given the increasing threat of DDoS, even the most technically proficient companies are beginning to employ external mitigation services to counter DDoS attacks. These are dedicated to monitoring your internet traffic and when necessary, instigating numerous technical controls to mitigate the attack.

Case study: The tools: big, and getting bigger

An internet company that provides domain name system (DNS) registration and other services, suffered a series of massive DDoS attacks on 21 October 2016. The reported size of the attacks (up to 1.2Tbps) was unprecedented as was the impact this attack had on other companies. A large number of well-known internet-based businesses in the US and Europe, who relied on the DNS company for essential 'upstream' services, were taken offline for most of the day.

*refer to glossary

Cyber attacks will continue to evolve, which is why the public and private sectors must continue to work at pace to deliver real-world outcomes and ground-breaking innovation to reduce the threat to critical services and to deter would-be attackers.

Ciaran Martin
CEO National Cyber Security Centre

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

A demand is then displayed informing the user that it will not be unlocked until a sum of money is paid. A time limit is usually imposed for the ransom to be paid, or the code to decrypt the data will be deleted and the data will not be recoverable. Ransomware usually infects single machines but some recent attacks have also incorporated exploits that allow the malware to move laterally within a network and spread to other devices.

How are users infected?

The most common ways ransomware infects a computer are via:

- **Email** – Clicking on a malicious link in an email, or opening a malicious attachment;
- **Websites** – Visiting a social networking site or other website which is hosting ransomware;
- **Removable media** – Inserting or connecting an infected USB or other removable media device (e.g. memory sticks, external hard drive).

Case study: A global ransomware outbreak

A massive ransomware outbreak occurred in May 2017, when a ransomware variant named WannaCry spread rapidly infecting more than 200,000 computers in over 150 countries within a day. WannaCry had the ability to propagate within networks without user intervention, and many large organisations were significantly affected, including healthcare providers in the UK who had to reduce the services they could provide until they could restore the infected machines.

How to protect your business?

Employee education and awareness – Ensure users are aware of the risks associated with allowing malware onto a system. Additionally educate them about the typical ways malware can get onto a device – via email, internet (websites) and removable media.

The following controls (detailed on the Phishing page 5) will help to reduce the chance of being infected with ransomware – **user access controls, secure configuration, patch management, malware protection** and **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 and scan all media for malware before importing onto any of the organisation's systems.

Back-ups – Establish a programme of taking regular back-ups, ensuring that your most important files are copied most frequently – potentially also off-site. This will enable machines and systems to be restored in the event of infection, without a significant impact.

- The site 'Get Safe Online', partner of Lloyds Banking Group, has advice on how to decrease the chance of being infected by ransomware: **www.getsafeonline.org**
- If any of your systems are compromised by ransomware and the computer or data sources have been locked, seek professional advice. Attacks should also be reported to the police by visiting: **www.actionfraud.police.uk**

Website attacks

Protecting your online presence

What is a website attack?

Whilst websites are often described as the shop window to your business, they can also be attacked by a range of actors and for a variety of reasons.

These include defacement of the website (changing the visual appearance or content), the addition of content (a phishing page or malware), or the loss or compromise of customer or company data. It could also facilitate a denial of service attack to take the site offline, or an intrusion into the back end IT systems potentially launching malicious code.

Case study: European Central Bank (ECB) hacked

The details of around 20,000 people who had registered on the ECB's website were compromised by a website attack. The ECB was unaware of the breach until it was contacted anonymously by the perpetrators who then sought to extort cash in return for the stolen data.

How to protect your business?

Education and awareness – Ensure staff involved in designing and developing websites understand that security is part of their role and are trained 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 controls and ensure updates and patches are applied swiftly. Establish a process to run frequent back-ups and monitor the site regularly for suspicious activity including any unauthorised or unscheduled changes to the content of the website.

Website governance – Ensure clear policies exist, particularly around the ownership of websites and the accountabilities 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 – Software testing tools and/or code analysis could be incorporated into the software development lifecycle to search for vulnerabilities written into software or code.

Penetration testing – Should be completed to evaluate the security of the system or application by simulating an attack. Undertaken by skilled personnel, ideally it should be completed before a website is launched and also after any significant code change.

Vulnerability scanning – Regularly scan any internet-facing networks for vulnerabilities. This is a mainly automated test and helps to identify any vulnerabilities that are discovered between penetration tests.

Vulnerability management – Vulnerabilities identified during any testing should be assessed and where necessary remediated on a prioritised basis.

Web application firewall (WAF) – A WAF will help to mitigate common attacks (cross-site scripting (XSS) and SQL injection) and could be customised to identify and block other attacks.

3rd party service providers – Ensure 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)?

An APT is a sophisticated targeted attack which typically uses a wide variety of carefully planned and designed attack techniques to achieve its objective. 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 obtain the information required 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. The early stage of an APT will be conducted stealthily to avoid detection, and it is increasingly common for some material to be gathered from employees' social media posts.

Case study: Central Bank of Bangladesh loses $81m

In early 2016 arguably the largest cyber heist ever took place targeting the Central Bank of Bangladesh. The attackers utilised custom malware that interacted with payment systems software to steal funds. Those funds were then moved quickly through casinos in the Philippines. The attack was timed over a Bangladeshi Bank Holiday when response was slow, and the Chinese New Year when large transfers are normal across Asia. $81m remains unaccounted for. The attack was intended to net $951m and was only stopped by a counterparty querying a spelling error. The sophistication and amount of planning indicates this was the work of a nation state.

Who conducts APTs and why?

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

Nation-state actors are also believed to have orchestrated APT attacks against commercial organisations, notably those involved with scarce natural resources (i.e. 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 any business with valuable technology, high-value processes, or intellectual property could be targeted.

A small subset of nation state actors are also motivated by financial gain. As these nation states also appear to be using more 'open source' attack tools it is harder to differentiate them from organised criminals making it ever more challenging to identify the culprits.

Advanced Persistent Threats

Prevent, detect & respond

Case study: Ukraine power outage

In December 2016 a cyber attack was launched against the Ukrainian energy grid cutting power to around a fifth of the capital Kiev; this followed an attack in 2015 which cut power to 225,000 people.

The attackers gained a foothold through spear-phishing before accessing the organisation's Supervisory Control and Data Acquisition (SCADA) systems and turning off services. It is suspected that the actors were on the Energy company's network for up to six months undetected before mounting the attack.

Many researchers believe that the group responsible could have conducted more extensive attacks but did not, suggesting this particular attack was a demonstration of capabilities and intent. This echoes the commonly held belief that there are groups with the intent and ability to launch attacks on the critical national infrastructure of every country in the world.

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. However, taken individually, those techniques are typically well-known, so can be defended against.

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 also help to protect against APTs, along with a risk based approach – ensuring available resources are directed towards the assets most likely to be targeted.

An essential layer of protection involves employee education, as staff will often be targeted via spear phishing attacks 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 but the most popular example is one called the 'Cyber Kill Chain®' which was produced by Lockheed Martin.

Key considerations for your business

What next?

What do you do from here?

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 a number of factors including who might be attacking you, what they want to achieve and how vulnerable are your assets or services – think **means, motive** and **opportunity**.

Whilst you have no control over the capabilities or motives of attackers, it is possible to make things more difficult for them by reducing your business vulnerabilities.

The following questions may assist your company in becoming more aware of and protected against cyber threats:

1. Have we identified and understood the company's critical information, assets and services? Where are they stored, who has access to them and have we considered suppliers, contractors etc. (**confidentiality, integrity** and **availability**)?
2. Have we considered who might want to attack us, why and what the impact of a successful attack might be?
3. Do we have a risk appetite for different types of cyber events impacting our business?
4. Do we know what vulnerabilities we have and do we have an efficient vulnerability management process (**people, process** and **technology**)?
5. Have we risk assessed how well our critical assets are protected and produced a gap analysis?
6. Do we have a prioritised action plan to enhance our capability to protect our business against cyber attacks (10 Steps to Cyber Security)?
7. Have we ensured our colleagues (and if appropriate, our clients) are aware of the cyber threats, especially the risks associated with social engineering and phishing attacks?
8. How do we know our defences work – have we tested them or sought external assurance?
9. Do we have a process to regularly review our key information, data assets and the cyber threat to our business?
10. Do we have a plan (is our incident response and disaster recovery prepared) in the event of a successful cyber attack (Reducing The Impact)?
11. Have we considered taking out adequate cyber insurance cover?
12. Have we considered the disruption to working capital position, revenues and capital position of the firm and made appropriate provisions?

How should you report a cyber attack?

If your business is the victim of a cybercrime, you should contact Action Fraud.

WHERE TO FIND OUT MORE?

Action Fraud
Cyber Aware
Cyber Essentials
Get Safe Online
Stay Safe Online
10 steps – Board Responsibilities
How to Protect Small Firms in the Digital Economy

If you would like any further information please contact your Relationship Manager.

Cyber glossary

Access Control

Access controls allow a system administrator to set restrictions and approve access to files and programs within a network.

Advanced Persistent Threat (APT)

An advanced persistent threat is a type of targeted attack. Typically, APTs are carried out by attackers who have the time and resources to plan a sophisticated infiltration into a network. These attacks usually seek proprietary information, rather than simple financial data. APT attackers may obtain access to a network through spear phishing or by exploiting a vulnerability in a system's software. They may remain on a network for some time while they map out systems and move through the network until they are able to extract the required information.

Bitcoin/Virtual Currencies

Bitcoin is essentially an online currency that enables payments without the use of interim organisations such as banks. Bitcoin legitimacy is often disputed because it is unregulated and is frequently associated with illegal activities, for instance in dark web black markets.

Bot

Abbreviation from web ro**bot**. A bot is a device, such as a computer or smartphone, that has been compromised and is capable of performing tasks on behalf of its master, typically a cyber-criminal, who would often control a multitude of bots; collectively known as a botnet. Bots and botnets are controlled via command and control (C&C) servers, and are often used to send spam email, spread malware or generate specific traffic as part of a DDoS attack. These machines are also frequently known as 'zombies'.

Botnet

A botnet is a collection of bots or zombie devices. This could range from a few hundred to many thousand compromised computers or devices, often geographically spread, that are controlled to serve particular purposes. Botnets are commonly associated with DDoS attacks, in which they collaborate (via C&C servers) together to direct traffic towards the victim site, with the aim of rendering the site unusable.

Command and Control

A command and control centre (C&C or C2) is a computer that controls a botnet (a network of compromised computers). Some botnets use distributed command and control systems, making them more resilient. From the command and control centre, hackers can instruct multiple computers to perform their desired activities. Command and control centres are often used to launch DDoS attacks because they can instruct a vast number of computers to perform the same action at the same time.

Crimeware-as-a-Service (CaaS)

The provision of cyber criminal activities or attacks as a service for hire. Availability of these services is increasing which allows a wider range of threat actors to launch attacks, where they don't have the technical ability or toolset to do so themselves. This includes the ability to launch DDoS attacks, steal financial information and deliver malware.

Dark Web/Dark Net

The 'Deep Web' refers to the large portion of the internet that is hidden from search engines. These are often associated with academic, scientific or financial organisations. The 'Dark Web' specifically refers to a subset of the Deep Web which hides the IP address of the servers that run them, making it very difficult to establish who is behind them. Dark Web sites are generally only accessible by using anonymising software such as TOR (The Onion Router). Whilst many of these sites are used for legitimate purposes, the Dark Web is most famous for hosting criminal sites such as 'Alphabay' and 'The Silk Road' offering the sale of many illegal items such as malware kits, weapons and drugs.

Denial of Service (DoS) Attack

A DoS attack prevents users from accessing a computer or website. In a DoS attack, a hacker attempts to overload or shut down a service so that legitimate users can no longer access it. Typical DoS attacks target web servers and aim to make websites unavailable. No data is stolen or compromised, but the interruption to the service can be costly for an organisation.

Distributed Denial of Service

A DDoS attack is a Denial of Service attack that uses many (usually compromised) devices to launch the attack. These devices are typically distributed across the internet as part of a Botnet. It has the same goals as a DoS attack – disrupting systems by preventing genuine users from accessing them - but is more difficult to mitigate as the malicious traffic originates from many distributed devices.

Encryption

Encryption is the process of encoding data (i.e. messages or information) into secret code so that only authorised parties can read it. The intended recipient(s) must use the appropriate password or key to decrypt it.

Exploit

An exploit is an attack on a computer system that takes advantage of a particular vulnerability or 'bug', which exist in software or hardware. Typically a piece of software or a sequence of commands is used to 'exploit' the vulnerability to give an attacker unauthorised access to, or control over the computer system.

Firewall

A firewall prevents unauthorised access to a computer or network by acting as a barrier between networks or parts of a network, blocking malicious traffic or preventing hacking attempts. The firewall inspects all traffic, both inbound and outbound, to see if it meets certain criteria. If it does, it is allowed; if not, the firewall blocks it.

Hacktivism

The word 'Hacktivism' is derived from the terms 'hack' and 'activism', and is the act of breaking into computer systems ('hacking'), typically for politically or socially motivated purposes. This often involves defacing websites or launching DDoS attacks to disrupt services, to bring attention to political/social agendas, rather than for any financial gain.

Indicators of Compromise (IoCs)

IoCs are data items found in system log entries or in files, that can be used to identify potentially malicious activity on a system or network.

Industrial Control System

ICS is 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). Many of these are found in critical industry sectors such as electrical, gas and water industries, as well as being used to control heating and air conditioning systems in office buildings. Outside takeover can cause not only disruption to business operations, but also destruction of equipment and, potentially, injury to people.

Internet of Things (IoT)

The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data; these sorts of devices can also be known as connected or smart devices.

Malware

Malware is a collective term used to refer to a multitude of **mal**icious soft**ware**, including viruses, Trojans and ransomware. It is created for nefarious purposes, typically to damage, disrupt or exploit vulnerabilities in computers.

Patches

Patches are software add-ons designed to add new features or fix software bugs, including 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

Phishing is an attempt to obtain sensitive information from a victim by email. The sender will claim to be emailing from a trusted source, such as a colleague, the victim's bank or similar. The email will typically direct the victim to a website which will ask them to share their passwords or credit card details, or install malware on the victim's device.

Ransomware

Ransomware is a type of malware designed to coerce victims into paying a ransom, often by restricting access to a computer, device or files until the user pays a fee. Other times, messages purporting to be from law enforcement agencies are displayed claiming the user has been involved in illegal online activities, and providing instructions to pay a fine.

Remote Access Trojan

A RAT is a malware program that provides cyber-criminals with back-door access to an infected device. RATs are typically used to gather information from the infected device, such as through webcam surveillance, but can also be used to infect that device with additional malware.

Rootkit

A rootkit is a type of malware which attacks a device before the operating system has fully started up. It generally attempts to gain administrative access to the device so that it can control the device's processes or software. It may also manipulate important system files to hide its presence or inject additional information. It is often necessary to completely reinstall the operating system in order to remove a rootkit.

SCADA

Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organisations to control industrial processes locally or remotely; monitor, gather and process real time data; directly interact with devices such as sensors, valves and pumps through human-machine interface (HMI) software; and record events into a log file.

Smishing (SMiShing)

A social engineering technique which targets users of mobile phones/devices. Smishing is a type of phishing attack that uses SMS (Short Message Service) or text messages, instead of email (phishing), to obtain private and confidential information from individuals. The messages are typically designed to trick the recipient into downloading malware onto their mobile phone/device.

Social Engineering

The manipulation of people into performing actions or divulging sensitive or confidential information that can be used to gain physical access to areas or unauthorised access to computer systems, usually for fraudulent or other criminal purposes.

Spam

Spam is unsolicited bulk email, the electronic equivalent of junk mail, that comes to your inbox. Spammers often disguise their email in an attempt to evade anti-spam software. Increasingly spam arrives via legitimate email addresses whose user credentials have been compromised. Spammers can send millions of emails in a single campaign at very little cost. Spam is frequently used to distribute malware. Spammers are now also exploiting the popularity of instant messaging and social networking sites such as Facebook and Twitter to avoid spam filters and to trick users into revealing sensitive and financial information.

Spear Phishing

A carefully crafted phishing attack directed at specific individuals or companies. The email is often made to look like it has arrived 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

SQL injection is an exploit that takes advantage of database query software that doesn't thoroughly test for correct queries. SQL injection sends commands via a web server linked to an SQL database. If the server is not correctly designed and hardened, it might treat data entered in a form field (such as username) as a command to be executed on the database server. For example, an attacker might enter a command string designed to output the entire contents of the database such as customer records and payment information.

Threat Actors

A threat actor, is an individual or group that is engaged in malicious cyber activity. Threat actors are typically categorised as 'Nation State', 'Organised Crime Group' or 'Hacktivist', however there is some crossover between these groups.

Trojan

A Trojan horse or Trojan is a program that appears harmless but is, in fact, malicious software. Typically the malware would be hidden within an innocent-looking email attachment or a free computer program/application.

Virus

Viruses are malicious computer programs that can spread to other files. Viruses can have harmful effects such as displaying irritating messages, stealing data, or giving hackers control over your computer. Viruses can attach themselves to other programs or hide in code that runs automatically when you open certain types of files. Sometimes they can exploit security flaws in your computer's operating system to run and spread automatically. You might receive an infected file in a variety of ways, including via an email attachment, in a download from the Internet, or on a USB drive.

Vishing (Voice or VoIP Phishing)

Another social engineering technique that is a variant of a phishing scam. Vishing uses the telephone in an attempt to scam users into divulging private or confidential information.

Vulnerability

Vulnerabilities are bugs in software programs that hackers exploit to compromise computers. Security vulnerabilities are commonplace in software products, leaving users open to attacks. Responsible software vendors, when aware of the problem, create and issue patches to address the vulnerability. When an attack exploits a vulnerability before it has been discovered or patched by the vendor, it is known as a "zero day" attack. 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)

Web application firewalls help keep your servers safe from hackers by scanning activity and identifying probes and attacks. A web application firewall is an otherwise traditional firewall appliance that also performs typical duties handled by multiple systems, including content filtering, spam filtering, intrusion detection and antivirus. Web application firewalls are typically used to protect web servers that are accessible from the Internet.

XSS (Cross Site Scripting)

XSS is a type of attack in which an attacker inserts code into an otherwise legitimate website. This enables the attacker to bypass the security of the website in order to change user settings, hijack accounts or enable malware downloads.

Zero Day

A zero day vulnerability is a software bug that has not yet been patched by the software vendor, typically because it has not been disclosed to them but may already be known by attackers who are working to exploit it – known as a zero day attack. The term zero day refers to the number of days that the software vendor has known about the bug.

Find out more

Go to lloydsbank.com/business

Contact your Relationship Manager

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

If you have a hearing or speech impairment you can use the Next Generation Text (NGT) Service (previously Text Relay/ Typetalk) or if you would prefer to use a Textphone, please feel free to call us on 0345 601 6909 (lines open 7am-8pm, Monday-Friday and 9am-2pm Saturday).

Our service promise

If you experience a problem, we will always try to resolve it as quickly as possible. Please bring it to the attention of any member of staff. Our complaints procedures are published at lloydsbank.com/business/contactus

Important information

Calls may be monitored or recorded in case we need to check we have carried out your instructions correctly and to help improve our quality of service.

LLOYDS BANK

M60752 (12/18)