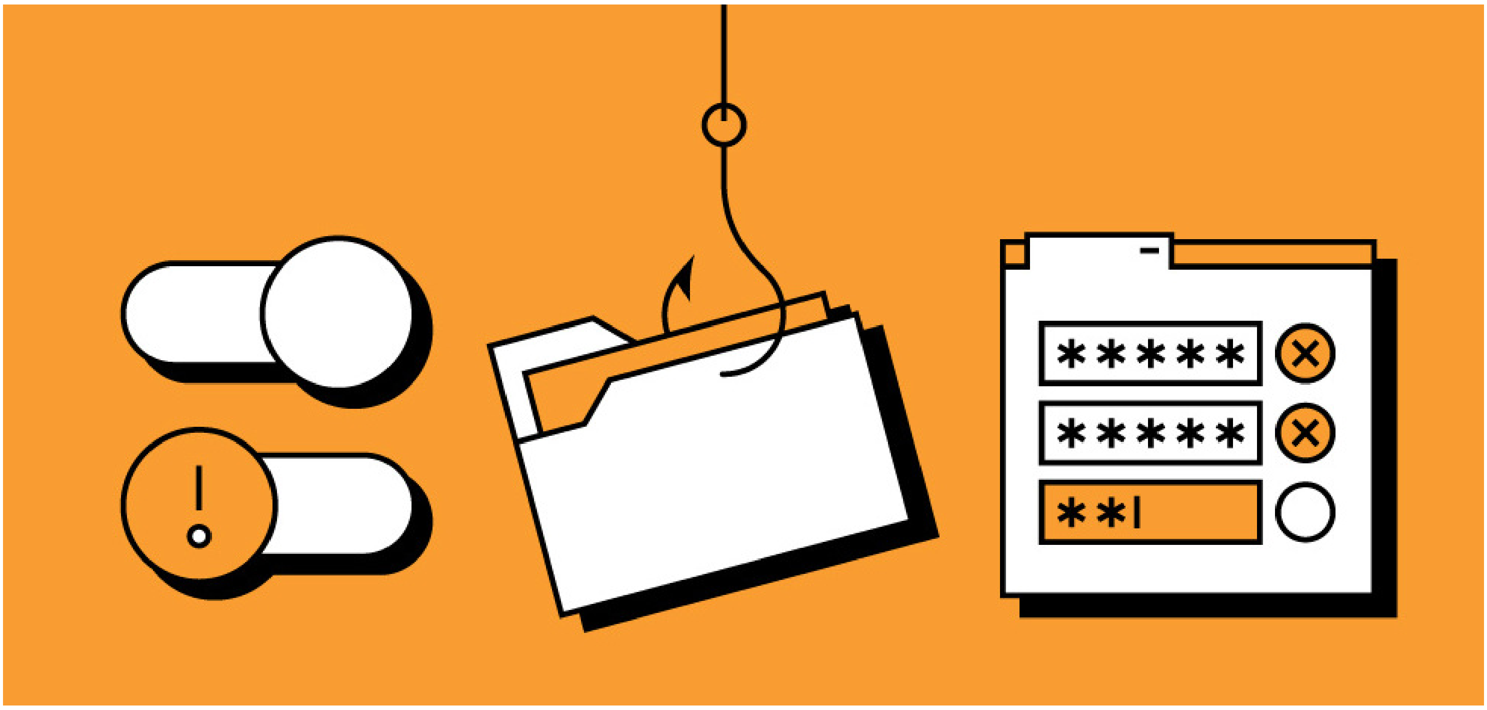
Introduction

In 2014, we published the "Protecting personal data in online services: learning from mistakes of others" paper. Over the last decade more of our personal information has moved into the digital world and we have continued to empower people and organisations to improve their security by issuing up-to-date guidance and advice.



The General Data Protection Regulation (GDPR), updated Data Protection Act 2018 (DPA), and the proposed Data Protection and Digital Information (DPDI) Bill are still based around the same eight principles of "good information handling". These provide an overview of people's specific rights about their personal information and organisations' obligations when they are processing it. The Network and Information Systems (NIS) Regulations also require Operators of essential services (OES) and relevant digital service providers (RDSPs) to implement security measures.

There is a large amount of guidance from different sources around security and this can sometimes make it difficult to know which guidance to rely on. We recognise that the National Cyber Security Centre (NCSC) is the technical authority on cyber security in the UK. We have drawn upon their existing resources to highlight the most significant threats to securing information and safeguarding of people.

Cyber security is a crucial part of protecting information and it is important to note that security breaches frequently lead to information breaches. If personal information is at risk, you may need to report the breach to us within 72 hours.

Ten years on from our original publication, our security incident trend information shows cyber threats not only continue to exist but increase year-on-year. We aim to 'empower and inform' organisations, and this review intends to support you in improving your knowledge of common security pitfalls. We believe that better transparency benefits not only specific organisations but society. So with that in mind, we want organisations to learn from the mistakes of others by understanding what common security control failures led to breaches. This should help you to put mitigating controls in place or take preventative measures before you experience your own breach.

We have summarised several case studies from our regulatory activities to illustrate some commonly encountered issues and highlight where lessons might be learnt. These are not a full representation of the case and we have linked to the relevant monetary penalty notice or reprimand for further information.

Whilst ransomware remains one of the top incident type categories, we have already provided comprehensive guidance for it. Therefore, this review will focus on other main causes of security breaches:

- Phishing
- Brute force attacks
- Denial of service
- Errors
- Supply chain attacks

This guide summarises:

- what each of these attack types are;
- how they take place;
- some key principles to consider when trying to mitigate or reduce the level of harm from a security breach, based on our review; and
- possible developments that might impact these categories in the future.

There are no silver bullets for information security. You should consider the nature of your activities when deciding what is appropriate for your organisation, Getting the correct foundational controls in place is key, as well as ensuring that you take a layered approach to your security. Therefore, if one control fails, there is another mitigating control in place.

Further reading

Further reading:

- The eight principles of ‘good information handling’

An overview of the main legal provisions and relevant guidance:

- UK GDPR guidance and resources
- The Guide to NIS

Who is this aimed at?

This review might help you gain insights but is not intended as guidance. It is aimed at someone who is responsible for compliance with data protection legislation, or for managing information security, or both. It is primarily focused on organisational security. However, where applicable, we do also mention what we found in our review about steps which people might take for their own security. This review assumes a basic level of knowledge, it does not replace any of our existing guidance or technical guidance from the

NCSC, which is referred to throughout.

Malware and ransomware

We recognise that we have already said a lot about ransomware, so this section is a very brief overview with signposts to new developments, where appropriate.

Malware (malicious software) is any software that is used with malicious intent to harm systems. It is deliberately damaging to computer systems. Although the motives can be varied, many criminals are looking to disrupt operations and benefit financially. Malware attacks are rising year-on-year.

Ransomware is the most common malware, and often the most harmful. Typically, ransomware involves criminals encrypting an organisation’s files to make them inaccessible. They then demand money in exchange for providing access to the information. More recently, ransomware is being used to describe different types of cyber extortion, including information theft.

Ransomware is still a persistent and significant online threat to the UK economy and people. If you become a victim of ransomware, you should assume the information has been exfiltrated (extracted).

Jointly with the NCSC, we have developed our position about ransom payments. Specifically, that paying a ransom to unlock your information does not reduce the risk to people and it does not safeguard the information. Attackers are known to publish information on the dark web. Some criminals have exfiltrated (extracted) information before encrypting targeted networks, subsequently threatening to leak the information unless a ransom is paid (known as double extortion ransomware). Leaked information is vulnerable to criminal misuse and leads to financial losses. But more importantly, it increases the risk to people who need extra support to protect themselves.

Most ransomware incidents are usually the result of poor cyber hygiene rather than sophisticated attack techniques. Ransomware attacks are frequently enabled by phishing emails or by exploiting remote services, for example remote desktop protocol (RDP) which is often used by administrators to remotely connect to servers on their organisation's network. If these remote services are not secured appropriately, they can provide an easily exploitable access point into a corporate network.

In some cases, attackers will join forums which steal and sell remote access credentials to the highest bidder. These are often referred to as access brokers. They could also sell valid session cookies and other credentials that could be exploited to gain access to an organisation’s internal systems.

Example: Malware leads to loss of access controls and a fine

Facts

An attacker had compromised a retailer's infrastructure and gained control of multiple domain administrator accounts.

Malware installed by the attacker was running on 5,390 Point of Sale (POS) terminals in stores which take in-store payment. Therefore, the attacker was able to collect payment card details for any transactions that used the POS terminals during that period.

What could have been done differently?

- Use network segregation - sufficient internal network segmentation could have contained the compromise to a particular section of the network.
- Put effective local firewalls in place.
- Implement more timely patch management.
- Undertake adequate vulnerability scanning.
- Apply allowlisting consistently and appropriately.
- Implement an effective system of logging and monitoring.
- Update software promptly.
- Implement point-to-point encryption.
- Secure the domain administrator account with appropriate controls.
- Implement standard builds for all system components based on industry standard hardening guidance.

What might help to reduce the risk of malware?

In practice, there are several key security principles you should consider:

- Follow good cyber hygiene; refer to NCSC's 10 steps to cyber security as a helpful guide.
- Use multi-factor authentication (MFA /2FA), protect user credentials and information used in credential verification, and utilise the principle of 'least privilege' for accounts. Be mindful of new attack techniques that seek to bypass MFA and deploy appropriate controls to mitigate those, in line with your risk assessment.
- Have appropriate, secure, and tested back-ups.
- Provide appropriate security training for staff.
- Actively manage and monitor systems to detect issues early.
- Test response and recovery plans.
- Sign up to the NCSC's Early Warning service, where appropriate, and keep up-to-date with security issues.

Example: Unavailable systems due to ransomware lead to a fine

Facts

A legal firm determined that it had been subjected to a ransomware attack after parts of its IT system became unavailable and they discovered a ransomware note.

The attack encrypted civil and criminal legal case bundles stored on an archive server and the encryption of backups. This resulted in personal information being unavailable (via encryption) and a loss of confidentiality (via access to, and exfiltration of, the personal information).

The attack

The legal firm could not determine conclusively how the attacker was able to access the network. However, it did find evidence of a known system vulnerability that could have been used to either access the network or further exploit areas of the firm, once inside the network.

Once inside the network, the attacker installed various tools to enable them to create their own user account to execute the attack. The attacker then encrypted 972,191 individual files and 24,711 court bundles. The attacked then exfiltrated 60 of these bundles and published them on an underground market site (the "dark web").

What could have been done differently?

- Use multi-factor authentication (MFA) for the remote access solution.
- Implement more timely patch management.
- Use encryption for the archived documents.

Further reading

- 10 steps to cyber security - NCSC
- Ransomware guidance - ICO
- Joint ICO and NCSC letter re: ransom payments
- Ransomware, extortion, and the cyber crime ecosystem white paper - NCSC
- Multi-factor authentication - NCSC
- NCSC Annual Review 2022
- RUSI Ransomware: a perfect storm
- "What's happened to my data?" blog - NCSC

Phishing

56% of businesses and 62% of charities that reported having had breaches or attacks in the past 12 months, felt phishing attacks were the most disruptive types of attack that organisations face. This is according to the most recent UK government cyber security breaches survey. It also showed that the percentage of phishing attacks was on the rise. 79% of businesses identified having had a phishing attack in the last 12 months, compared to 72% in 2017.

Proofpoint's State of the phish report revealed a higher percentage still. 91% of UK companies responding to their survey stated they had experienced at least one successful email-based phishing attack in 2022. More than a quarter of those (26%), also reported direct financial losses as result.

During the COVID-19 pandemic, the UK's National Cyber Security Centre (NCSC), the United States Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) published a joint advisory statement. They warned of malicious cyber actors exploiting the pandemic with related scams and phishing emails. The levels of attacks have not returned to pre-pandemic levels. The Office of National Statistics (ONS) also reported that fraudsters were targeting people by taking advantage of behavioural habits since the pandemic, such as increased online shopping.

Defending against phishing requires using technological mechanisms (such as filtering, firewalls and blocklists) in conjunction with human-centric approaches (such as cyber security awareness training around phishing).

Further reading

- The effects of human behaviours in phishing - IEEE research
- Phishing attacks – who is most at risk? - ONS
- NCSC and DHS joint advisory statement

What is phishing and how does it happen?

Phishing is when criminals use scam messages to trick people into sending sensitive information, pay money, or click on a link which contains a virus or takes you to a fraudulent website. Phishing threats affect organisations of all sizes and sectors. 34% of users did something that put themselves or their organisation at risk, such as clicking on a malicious link, according to a report from Proofpoint.

Phishing is a type of social engineering. It relies on the person believing the message originates from someone they know or an organisation they trust. Proofpoint's report also highlighted that 44% of people think an email is safe when it contains familiar branding. However, criminals used Microsoft branding or products in over 30 million malicious messages sent in 2022.

Phishing may happen by various means, most commonly by email, text (smishing) or voice call (vishing). Most phishing attackers send high numbers of messages and expect success in relatively few cases.

Some attackers are much more targeted and use a method known as spear phishing. These attacks aim to target a specific person or organisation. These attacks are tailored to use information such as names, job roles or social media profiles to make the messages seem more relevant and believable. This is why it is important to be aware of the information you disclose online and how attackers may use it.

Business email compromise (BEC) is a scam which compromises legitimate business email accounts through social engineering, spoofing, or hacking, to conduct unauthorised transfers of funds. In more recent times, attackers have targeted savings accounts held by financial institutions, such as banks or stockbrokers, for cryptocurrency exchanges. The FBI’s 2022 Internet crime report showed BEC still accounts for 75% of attacks and $2.7 billion in losses.

Typically, the attacker sends a message designed to frighten or panic the person opening it into acting immediately. This is so they don’t have time to judge whether the message is real.

Common topics are about health scares, the threat of money losses, advising another account is compromised or time-limited ‘too good to be true’ offers. If the person takes the bait, they will download malware or be asked to provide further information, such as their banking details, usernames, and passwords.

Phishing attacks can put all your information at risk. A successful phishing attack can have serious consequences, including:

- theft of money;
- lost, or compromised information;
- damage to reputation or trustworthiness;
- identity theft; and
- disruption to business functions.

Attackers often rely on phishing emails to get people to download the malware needed to start the attack or get access to the credentials needed to gain a foothold into the target organisation’s systems.

Usually, attackers will try and find a weak point in the target organisation’s defences. They will launch an initial attack on a regular user account. Inadequate security controls, or failure to follow the principle of least privilege, can inadvertently provide criminals with much wider access once compromised. Criminals may escalate privileges, either laterally, by taking control of additional systems, or by looking to gain administrative permissions or root access to control the entire estate.

Whilst anyone can be the victim of phishing, attackers are looking for high value returns. The FBI’s Internet crime report shows phishing has the highest number of victims, with 300,497 recorded victims in 2022. This is a year-on-year increase from 2020. Phishing is also recorded as one of the top initial infection vectors for ransomware.

Example: Phishing compromise leads to loss of personal information and a monetary penalty notice

Facts

An attacker compromised a construction company's servers including four HR databases and File Director System. The systems contained the personal information, including special category information, of up to 113,000 people. This was encrypted and rendered unavailable to the company by the attacker.

The attack

A phishing email was sent to the company's accounts team mailbox which was designed to appear as though the document required urgent review. One employee then forwarded it to another employee responsible for paying invoices. This employee opened the email, downloaded, and extracted the ZIP file linked in the email, and opened the script file. This installed malware onto their workstation and gave the cyber-attacker access to the employee's workstation.

The employee was working from home and had access to the company's systems via a split tunnelling method. As a result, the employee who clicked on the link in the email did not go through the company's Internet Gateway system which was designed to restrict access to malicious sites.

The company's System Centre Endpoint Protection tool attempted to remove some of the files and subsequently reported that the removal of malware files had been successful. No further action was taken by the company at this time to verify that all malware had been removed. In fact, the attacker retained access to the employee's workstation.

Following this initial access, the attacker compromised a server. This was used to move laterally to other systems and resulted in the:

- compromise of 283 systems and 16 accounts (including 12 privileged accounts) across four domains;
- execution of a script to uninstall the company's Anti-Virus solution; and
- encryption of personal information on four HR databases and File Director System, which together contained personal information of up to 113,000 people, including special category information.

What could have been done differently?

- Implement supported operating systems (operating systems no longer the subject of security updates to fix known vulnerabilities can be exploited by malicious actors.)
- Implement appropriate end-point protection.
- Undertake adequate vulnerability scanning and penetration testing.
- Provide appropriate staff training.
- Update protocols.
- Conduct an effective and timely investigation.
- Give domain privileges only where strictly necessary and to the minimum number of users.

Further reading:

- The FBI’s Internet crime report

- Data breaches: guidance for individuals and families - NCSC
- Security outcomes guidance – NCSC

What might help reduce the risks from phishing?

Phishing attacks are common and there is no single security solution. You should put in place multiple layers of protection, so that if one fails, the others can mitigate against further damage:

- Refer to the 'Basic security principles' in the previous section.
- Be aware of how phishing attacks work and provide training to all staff to help them recognise and respond to potential attacks.
- Foster a 'no blame' culture for staff to encourage reporting. The more you know, the more you can do to limit any impact and remember that your staff are your first line of defence in these instances.
- Have a clear reporting mechanism so you are made aware of any concerns promptly. All staff need to know when and how to report, with robust processes in place to respond to potential phishing reports.
- Enable multi-factor authentication.
- Have clear contracts and service level agreements with any IT providers you might have outsourced specific operational or security services to, which cover expected security measures.
- Train staff to be wary of opening emails from senders they don't recognise, and to contact known senders by alternative methods if you are concerned.
- Advise staff not to click on password resets in an email unless they have recently requested them. Instead, tell them to login in the usual way and change passwords from inside the system.
- Set up anti-spoofing controls to prevent attackers being able to pretend to be from a particular organisational domain.
- Review information in the public domain, on your websites, in news articles and across social media channels, so it doesn't provide information which can help trick your staff or make you an easier target.

What are the likely future developments?

Phishing emails are getting increasingly sophisticated and more of them are getting through traditional perimeter detection, according to the Egress phishing report. They report a 29% rise in phishing emails getting through secure email gateways (SEGs).

Attack frameworks, such as Evilginx and phishing kits, that mirror legitimate websites, are also being sold to potential criminals. It is likely that defender's capabilities will also develop to better identify and block these attacks. However, the speed attackers develop their own capabilities means it's difficult for defenders to stay one step ahead.

Phishing kits incorporating anti-bot protection and QR generation will make security more difficult. The real-time ability to decide which fake page someone sees depending on their actions, will also make it hard for potential victims to spot them. Novel attacks also seek to exploit MFA fatigue to bypass current controls, or capture session cookies that render existing controls futile.

As artificial intelligence (AI) continues to develop, criminals are increasingly using large language models (LLMs), such as ChatGPT, to create phishing campaigns. The use of AI makes it less likely phishing emails will have poor grammar, bad spelling or requests which don’t make sense. This makes it virtually impossible for people to distinguish between malicious social engineering attempts and legitimate messages.

Generative AI can create faster, more effective, and larger scale cyber attacks through tailored phishing that can intelligently adapt to bypass firewalls. Artificial intelligence can also replace a person in a video for someone else (known as a deepfake video) and voice cloning. The increasing use of text-to-speech in phone calls and chatbots capable of evading existing bot detection techniques will inevitably lead to security challenges.

The ease with which artificial intelligence can be used to generate content means far fewer skills are required. This lowers the entry barrier for would-be cyber criminals to carry out effective attacks.

However, despite these issues, AI-powered security protection is also being developed to improve detection and disrupt criminals. This is due to the positive developments in effective analysis of user behaviours and email content. The general advice remains, and you should assess the risks and opportunities that these emerging technologies pose to your organisation, considering the organisational context, and deploying proportionate and layered controls and mitigations.

Relevant links

- Report scams to:
  - National Cyber Security Centre (for anything suspicious)
  - Action Fraud (if you've suffered a loss or been a victim of a crime) - the national reporting centre for fraud and cybercrime via the reporting fraud and cyber crime online form or by telephoning 0330 123 2040

Further reading

- Introduction to phishing - NCSC
- Phishing guidance - NCSC
- Password administrator for system owners - NCSC
- Egress phishing report 2023

Brute force attacks

Password attacks spiked in 2023, according to Microsoft's recent digital defence report. It stated that after a notable increase in the number of password-based attacks per month in October 2022, that number increased ten-fold in 2023 compared to the same time the previous year. It showed 11,000 attacks per second in April 2023.

In 2020, the internet security company Malwarebytes noticed a rise in compromised servers used to run brute force tools. This corresponded to a rise in the number of RDP ports exposed to the internet. This grew from about 3 million in January 2020 to over 4.5 million in March of the same year, due to the COVID-19 pandemic. Microsoft responded to this threat by adding default protection against RDP brute force attacks in Windows 11.

Most online login forms have lockout mechanisms incorporated to prevent too many login attempts being made. However, some applications may require lockouts to be set manually, including systems running versions of Windows prior to 11. This also does not prevent attackers from downloading an offline copy of a password database and running password cracking attempts against it until the password is revealed. They can then use this to access the target system.

Machine learning-based AI password cracking tools, such as PassGAN, are also being increasingly developed to remove the manual efforts in password analysis and cracking passwords.

What is a brute force attack and how does it happen?

A brute force attack is where criminals use trial and error to guess username and password combinations (credentials) or encryption keys. The success rate of an attack increases when credentials are simple and easy to guess.

A brute force attack requires trial and error to guess the credentials, by testing every possible combination. The need to try numerous variations means that this type of attack is normally automated, relying on software tools. It increasingly uses artificial intelligence to rapidly try huge numbers of combinations in the fastest time.

Brute force attacks are a common and historic way for criminals to attempt to gain access to user information, devices, and systems, but attacks are becoming increasingly sophisticated.

The simplest form of attack involves the criminal attempting to logically guess the password, often by using easily researched information. For example, children's or pet names and birthdays. Common passwords such as '123456' or 'password' are easily breached by this method. A **hybrid attack** combines common words and random characters, such as 'United123!' in the same way.

Attackers often use tools to test huge lists of login credentials, frequently with a **dictionary attack** method. They combine a traditional dictionary of words with common phrases or known passwords, systematically trying them to gain unauthorised access to systems.

A rainbow search builds a table of all possible values and then uses these to try to find a suitable match against the original value. The rainbow table works like a large dictionary, but it is optimised for hashes and passwords to ensure fast look-up speeds. Attackers steal password hashes (the scrambled, unreadable version of the actual password) which they then compare to the rainbow table. If successful, the table will provide the string relating to the hash.

When a criminal has successfully identified the password, they may use or sell these credentials on to other criminals. They will test them on multiple sites in a **credential stuffing** attack. This is surprisingly effective, as it is estimated that up to 65% of people reuse the same password on multiple sites.

If the victim is a person, rather than an organisation, the criminal may go as far as stealing their identity. This may then allow them to access bank accounts or commit other acts of fraud.

Fraud and monetary gain are still the primary motivators for attacking organisations. The sale of stolen personal information is common. If a hacker also accesses the organisation's website, they may place spam ads to gain commission, reroute internet traffic or place malicious software on a site to commit further cybercrime offences.

What might help reduce risks from brute force attacks?

The general good practice guidance applies, but since brute force attacks specifically target access credentials, you should also take the following actions to protect yourself from these types of attacks:

- Use two-step or multi-factor authentication. Note that some options are more resilient to attacks than others (eg SMS based ones are exposed to SIM swap attacks), so consider carefully which option to choose. Depending on the risk, you may decide to use hardware-based tokens.
- Use strong passwords, ideally using the 'three random words' approach.
- Avoid passwords which contain information about you which is easy to guess.
- Use unique passwords for different accounts and do not reuse passwords.
- Protect passwords at rest, eg by hashing and salting (adding extra random characters to the plaintext password, before hashing it) them, and in transit by using secure transport mechanisms.
- Consider the use of a password manager.
- Reduce reliance on passwords by considering single sign-on (SSO), hardware tokens and biometric options.
- Disable unused accounts.
- Limit logon attempts and set accounts to lock if too many wrong guesses are made of a password. NCSC recommend between five and 10 attempts.
- Consider configuring systems to have increased delays between successive login attempts (throttling).
- Consider using a CAPTCHA, a test to determine if a user is human rather than a bot, to mitigate against automated password guessing attempts.

Monitor for unusual or unexpected activity either from disabled or dormant accounts, or legitimate ones.

Further reading:

- Two-step authentication - NCSC
- Password managers - NCSC

- Three random words blog ↗ - NCSC
- Updated approach to passwords ↗ - NCSC

What are the likely future developments?

A low-cost attack tool which can crack the authentication fingerprint used on device lock screens has been developed.

To unlock a device with a password, an exact match to what is stored in the database is required for authentication. However, fingerprint authentication matching uses a reference threshold, so authentication only depends on an approximation of an image in the fingerprint database within the threshold parameters. Known as BrutePrint, it **does** require the criminal to have physical access to the device and set up additional hardware, including a microcontroller board. BrutePrint manipulates the false acceptance rate (FAR) to increase the threshold so fewer approximate images are accepted.

This attack type exploits zero-day vulnerabilities in the smartphone fingerprint authentication (SFA) framework. Using a database of fingerprints like leaked password databases, the time it took researchers to access the device was dependent on the number of authorised prints. The time varied between 40 minutes to 14 hours.

This type of attack raises questions about the implications of brute force attacks on underlying technology relied on for multi-factor authentication (MFA).

All brute force attacks require powerful computers to run a huge range of potential combinations as quickly as possible. As quantum computers are faster than conventional machines at this task, cyber security professionals and researchers have been considering how the future of quantum computing could pose a significant threat to cyber security.

Based on quantum physics, rather than standard electronics, quantum computers can lessen the time used to decrypt encrypted information. They could theoretically crack most current cryptographic methods used to transmit information over the internet. You should continue to keep your mitigation measures under review and consider what measures might be appropriate to future-proof your operations, considering technological developments.

Denial of service

Just as other areas of the digital ecosystem have moved to as-a-service models, cyber criminals are making use of the same business model, offering services and tools as a service for financial gain.

Cybercrime-as-a-service (CaaS) and related tools (booters, stressers, or ddosers) are increasingly available to launch distributed denial of service (DDoS) attacks at scale, to those without any technical knowledge at all.

The Financial Conduct Authority (FCA) has published information about cyber security incidents. DDoS attacks accounted for 25% of all hacking incidents reported to the FCA in the first half of 2022, compared to just 4% in 2021. Hackers are increasingly launching DDoS attacks against the UK's financial sector, as they move away from using phishing and ransomware, which was down 63% against the same period in the previous year.

According to the most recent UK government cyber security breaches survey, 15% of businesses identified having a denial-of-service (DoS) attack in the last year. Microsoft's Digital defense report 2023 showed DDoS attacks are continuing to rise, with an average of 1,700 attacks per day in the last year. Criminals are increasingly exploiting cloud computing resources, such as virtual machines, to launch DDoS attacks. Those same cloud resources provide our best defence against such large-scale attacks.

What is a denial-of-service (DoS) attack and how does it happen?

A DoS attack aims to stop the normal functioning of a website or computer network by overloading it and creating a virtual 'traffic jam'. Overloading the system makes it unusable and causes disruption. DoS attacks cause a machine to consume all available hard disk space, memory, or processing time.

A more complex version of this type of attack is a distributed denial of service (DDoS) attack. The attack still overloads systems, but the hacker uses a network of connected devices to flood the target from multiple points, 'distributing' the attack and making it much harder to stop.

DoS attacks either flood web services or crash them. They target organisations and exploit how computer networks connect. Flooding attacks overwhelm systems by sending large amounts of traffic which servers can't handle, commonly by sending 'spoof' information to every computer on a network.

Spoof information is information that the system is tricked into believing is from a legitimate source but is actually from the attacker. This false information overloads the system, causing it to come to a stop.

Alternatively, the criminals transmit software bugs that target the system to crash it.

DoS attacks take advantage of the way computer networks function and the way devices communicate. Misconfiguration or system vulnerabilities make a successful attack more likely.

In some cases, attackers aim to disrupt services for social or political reasons, but profit is usually a key driver.

Network connectivity errors and a heavy bandwidth use can affect performance, but indications of a DoS attack include:

- exceptionally slow network speeds, with very long load times for files or websites, or a failure to load at all;
- a sudden loss of connectivity across devices on the same network;
- being unable to load a particular website; and
- a sudden and noticeable increase in spam emails (known as an email bomb).

These issues may not be limited to the targeted computer as the available bandwidth is reduced and taken up by the attack.

Why is NIS relevant to denial of service?

The Network and Information Systems Regulations 2018 (NIS) concern systems that process ‘digital data’ for operation, use, protection, and maintenance purposes. NIS requires specific security requirements and incident reporting thresholds for Operators of essential services (OES) and Relevant digital service providers (RDSPs).

Clearly, a denial-of-service attack could significantly impact the availability of services and information. Therefore, for RDSPs, there may be additional reporting requirements. The magnitude, frequency and impact of security incidents is increasing, and network and information systems may become a target for harmful actions.

What might help reduce risks from denial-of-service attacks?

Our review of cases indicates that it might be helpful for you to take the following actions:

- Consider purchasing services which help defend and recognise legitimate increases in network traffic from possible attacks, as prompt detection makes an attack easier to contain.
- Check your firewalls and routers are correctly configured and updated with the latest security patches and consider a router that has in-built DDoS protection.
- Consider using hardware to help classify information before traffic reaches the server.
- Consider leveraging third party DoS protection services.
- Have a tested business continuity and disaster recovery plan.

In cases of DDoS attack, there may be another surge in traffic before recovery is complete, so on-going monitoring is essential.

Further reading:

- Network and Information Systems Regulations 2018 (NIS)
- Vulnerability scanning tools and services - NCSC
- Denial of Service (DoS) guidance - NCSC

What are the likely future developments?

The number of DDoS-for-hire platforms continues to rise, with 20% having emerged in the past year alone, according to Microsoft’s Digital defence report 2023.

In 2023, the cyber warfare associated with the Ukrainian conflict saw DDoS used as a key weapon to paralyse essential services. DDoS attack numbers reportedly rose following the Russian invasion in February. Just prior to the start of the conflict there had been a rise in carpet bomb attacks, a DDoS attack type that targets a range of addresses or subnets.

These are designed to attack multiple small targets, rather than a single, main target. These attacks expand to a range of IP addresses that share the same network provider or data centre. They can bypass traditional DDoS detection methods and alerts, going undetected. This invalidates the use of black hole or null route techniques and overloads reporting systems.

It is likely that machine learning will play a part in future mitigation strategies, but also attack techniques, just as with other aspects of cyber security. Machine-learning based algorithms can learn normal (and therefore expected) traffic patterns. This allows them to subsequently detect anomalies and detect a likely DDoS attack automatically.

Errors

According to Verizon's Data breach investigation report 2023, "74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering." Verizon categorises error as "anything done (or left undone) incorrectly, or inadvertently."

Breaches due to misconfiguration accounted for 21% of error related breaches within Verizon's dataset. The information they analysed showed that most errors that lead to breaches were committed by developers (over 40%) and system administrators. This is unsurprising as they are the ones with the responsibility for configuring environments.

According to Gartner cloud security research, cloud misconfiguration is a significant cause of cloud security breaches, with 36% of companies suffering a serious cloud security leak. Furthermore, 99% of all firewall breaches are caused by misconfigurations.

Error is a wide spanning topic, and for the purposes of this review we focus on misconfiguration as a specific type of error.

Security misconfiguration refers to security settings that are:

- poorly put in place (implemented);
- not setup at all during the configuration process; or
- are not maintained.

Misconfiguration also happens when systems are put in to use (deployed) with default settings, leaving them open to attacks.

Security controls that are not correctly configured and maintained put at risk your systems, information, and ultimately people. Misconfiguration can happen at any layer, through any application, through any platform, and across your network or in the cloud. Misconfigurations may seem completely avoidable, but to date we see them as one of the most significant risks.

A number of configuration errors happen because system administrators fail to change the default ("out of the box") settings. But typical misconfiguration vulnerabilities occur with any of the following inadequate security measures:

- Default passwords and certificates.
- Outdated (deprecated) protocols, ineffective and insufficient encryption.
- Application programming interface (API) security misconfiguration, which allows unrestricted access to endpoints and leaves files unprotected.
- Unused pages and unnecessary services.
- Open or dormant ports or other access points.
- Unrestricted permissions or inherited excessive permissions.
- Incorrectly implemented IT changes.

Often when software is provided in the form of software as a service (SaaS), the cloud provider takes on most of the security responsibilities. But with any type of cloud service (SaaS/PaaS/IaaS), cloud security is a shared responsibility.

A high number of cloud security incidents can be traced back to preventable misconfigurations made by end-users. Cloud services are any services that are made available by the internet. You should configure cloud services correctly and share the responsibility between you and your cloud provider.

Errors may be from misconfiguration, human error or simply a lack of checks and balances leading to insufficient controls that can leave systems vulnerable. You should never rely on one person or one control for security. Always take a layered approach, informed by the nature of any processing and an assessment of risk.

Further reading

- Shared responsibility in the cloud - Microsoft
- Shared responsibility model - Amazon Web Services (AWS)
- Shared responsibilities - Google Cloud | Architecture Framework
- Top ten cybersecurity misconfigurations – NSA and CISA
- Cloud security principles - NCSC

Configuration errors create security vulnerabilities that criminals can use to gain unauthorised access to systems, services, or personal information.

Misconfigurations, including unused open administration ports, can allow attackers to access servers remotely and disable the security controls you already have in place (eg firewalls and VPNs).

Example: Development error leads to a reprimand

Facts

A health service allowed integration of untested development code for a future liver scheme into its live environment. This integration error led to a number of prospective transplant patients being excluded from the service's liver-matching run.

What could have been done differently?

- Implement appropriate branch or version control so developers could not unknowingly introduce untested code into a live environment.
- Implement appropriate peer reviewing of developers' work to reduce the likelihood of inadvertent coding errors being introduced.
- Scope testing requirements prior to the launch of new schemes and implement testing prior to going live.
- Provide appropriate training for staff about code testing, branch control and the use of peer review.

What might help reduce risks of error?

You should:

- embed security from conception through to implementation and initialisation;
- contain development functions and not introduce them into live environments without suitable testing;
- have security as a core component (eg ‘security by design’ and ‘security by default’ principles);
- establish baseline configurations and guardrails and monitor for any unauthorised changes to those;
- educate your staff on how mistakes occur and why controls are important;
- consider automating repetitive processes to reduce the chance of error;
- change all default accounts, usernames, and passwords;
- remove all unnecessary features;
- undertake ‘Four Eyes’ (two person) quality control checks, requiring activities to be approved by two people;
- uninstall any unused applications or programs; and
- not ignore warnings or errors and plan time for security updates and bug fixes.

It’s never too late to look for security misconfigurations that already exist in your systems. This is just as important as preventing them.

Further reading

- Data protection by design and default - ICO
- Configuration management - NCSC
- Cloud security principles - NCSC
- Top cyber security misconfigurations – NSA and CISA
- Secure-by-design – CISA
- OWASP top ten – OWASP Foundation

What are the likely future developments?

No matter what security controls you put in place, there will always be a human element. Avoiding misconfiguration becomes ever more vital as more information is democratised and big data (high volume information which is complex or very varied in nature) is increasingly harnessed to inform decision-making. Open Web Security Application Project (OWASP) stated misconfiguration was one of the top 10 security issues, with default credential use and misconfigured storage being key factors.

Security relies on the analysis of security event information. Generative AI, with the ability to self-learn and backed by consistent data-driven algorithms, can provide a faster response to potential threats. Artificial intelligence may help reduce some of the issues human error creates, but it also creates new challenges, as understanding of new technologies often lags significantly behind implementation.

As emerging technologies, especially the development of products and tools which use AI increase, there is an ongoing need for privacy and security by design and default. Due to the large volumes of information needed to inform AI processes, misconfiguration at any level could lead to serious implications for people. An ever-expanding digital estate will continue to lead to more points of potential vulnerability and an increasing chance of error or misconfiguration.

However, technology also presents a great opportunity for more automated and streamlined development approaches. For example, infrastructure-as-code and continuous integration/ continuous deployment (CI/CD) pipelines having security controls and policies embedded from the start.

Human-centric security design is also set to increase, with more organisations focusing on employee experience, rather than relying on technical controls alone. Gartner predicts that by 2027, 50% of large enterprise Chief Information Security Officers (CISOs) will have adopted human-centric security design.

Further reading

- Secure development principles - NCSC

Supply chain attacks

Many third parties are now processing more sensitive information on behalf of other organisations than ever before. You can no longer just rely on your own internal cyber security controls to secure information. Although many businesses have effectively enacted internal cybersecurity protections, The Marsh State of Cyber Resilience Report 2022, ↗ found that less than half have conducted risk assessments of their supply chain.

The increased use of cloud and an expanding digital landscape have caused some organisations to rush into new implementations, without the due diligence needed to manage the associated risks. Following on from the COVID-19 pandemic, Argon's security review ↗ found supply chain attacks grew by over 300%.

The threat from a supply chain is directly linked to the number of suppliers, and hence the number of potential attack entry points. As digital estates expand, the risks from the supply chain also increase. Vendors with poor security controls can leave themselves, and the wider supply chain, open to attack.

The ability to attack many targets simultaneously through supply chain vulnerabilities has meant supply chains are an attractive target for criminals. Well publicised attacks, such as SolarWinds, log4j, Kaseya, and Spring4Shell, have alerted more people to the importance of vendor management.

What is a supply chain attack and how does it happen?

A supply chain attack is when products, services, or technology you are supplied with have been breached or compromised and are in turn used to infiltrate and further compromise your own systems.

This type of attack targets one or more elements you need to provide the products or services that you rely on. It could include software, hardware, or third-party vendors. This combination of people, processes and technological elements is your 'supply chain' and the risk to your organisation and those you interact with, will vary.

This means that when you use third-parties or IT service providers to process information on your behalf, you should be satisfied that:

- they have appropriate security and are complying with data protection legislation; and
- you have some form of assurance, usually via a contract.

Attackers search for unsafe code, unsafe infrastructure practices, and unsafe network procedures that allow them to insert or exploit the third party's systems with the intent to cause harm.

Recently, Russian actor Nobelium has been attacking organisations which are seen as integral to the global IT supply chain. Microsoft reports that these attacks are against resellers. Attackers have not attempted to exploit software vulnerabilities, but used techniques, such as phishing, to steal legitimate credentials, gain privileged access and exploit this to gain entry to their client's systems.

In a **software supply chain attack** the attackers insert their own code into a system or product known as malicious code injection. A criminal software developer could change code to perform malicious actions within the application. This enables fraud and information theft, or leaves a backdoor for an attacker to remotely access a corporate system. Applications with these undetected vulnerabilities could cause numerous attacks on many organisations and systems.

Further reading:

- The SolarWinds supply-chain attack – SANS Institute
- Supply chain panel session recording – Data Protection Practitioner's Conference

Digital supply chain attacks occur when developers use commonly used libraries to enable a function in their application. If the attacker inserts the malicious code into the programming library, any software developer that incorporates the infected library into their product will leave the product vulnerable.

In a **hardware supply chain attack**, the criminal supplies hardware products with installed components (eg microchips on a circuit board) which are used to build servers and other network components. The attacker can then search or extract information or obtain remote access to the corporate infrastructure.

The reason supply chain attacks are so difficult to mitigate is because you not only have to trust all the vendors you work with, but all the vendors who supply them.

An attacker, or a group of attackers, can target any part of the supply chain.

Example: Insecure supply chain leads to infiltration and a penalty notice

Facts

The IT systems of a hotel company were compromised by an unknown attacker using an unknown attack vector. The company was later acquired by another organisation. During the post-acquisition period, the attacker continued to travel through the company's systems and gained access to the system containing cardholder information.

This access allowed the attacker to export the personal information of many customers to "dmp" files on the company's systems, potentially with a view to taking a copy of the information, which included card payment information.

The attack

The attacker installed a web shell on a device within the company's network. This device was used to support an Accolade software application used by employees to request changes to any content of the company's website. The installation gave the attacker the ability to remotely access the system, allowing them to edit the contents of that system and, in this case, install Remote Access Trojans (RATs). The trojan malware enabled remote administrative control of the system, giving the attacker more access than a normal user account and unrestricted access to the relevant device.

The attacker then installed and executed a post-exploitation tool, 'Mimikatz'. This tool allows the harvesting of login credentials temporarily stored in the system memory, scanning the server for all the usernames and passwords stored. This allowed the attacker to continue to compromise user accounts which were secured using a mixture of single and multi-factor authentication.

The attacker then used these accounts to perform further reconnaissance and to run commands on the reservation database, including creating files which may have been intended for exfiltrating information. Additional malware, known as memory-scraping malware, was installed on multiple devices which searched them for payment card data.

What could have been done differently?

- Use multi-factor authentication (MFA) without gaps.
- Carry out more thorough due diligence where possible.

Note: the acquiring organisation was only able to carry out limited due diligence on the company's information processing systems and databases, including due diligence in relation to MFA. For the avoidance of any doubt, there was no finding of infringement in relation to MFA or due diligence aspects.

They could have implemented:

- appropriate monitoring of privileged accounts - appropriate and adequate measures are in place to allow for the identification of the breach and to prevent further unauthorised activity e.g. appropriate ongoing monitoring of user activity, particularly activity by privileged accounts;
- appropriate monitoring of databases including sufficient logging of key activities such as user activity or actions taken on a database and server logging of the creation of files;
- a form of server hardening as a preventative measure e.g. allowlisting; and
- encryption across more information categories.

What might help reduce risks from supply chain attacks?

Detecting attacks is an increasing challenge, due to ever more advanced tactics, new techniques and tools, as with all types of cyber-attacks Supply chains expand the scope beyond what is under your direct control, as they can come from any third-party vendors, including:

- website or software suppliers;
- development and testing platforms; or
- information storage solutions.

A supply chain attack targets systems and services you assess and trust. In each case, the attacker uses this trust to attempt to access critical aspects of your infrastructure and carry out malicious activity.

Supply chain attacks are more complicated than many other types of attacks and your recovery may depend much more heavily on your third-party supplier. To reduce the risk you should:

- have a robust supply chain risk management programme in place and apply a process for monitoring, managing, and reviewing systems, processes and access throughout your supply chain;

- document, evaluate, mitigate, and regularly review risks in your supply chain (recital 87), including who you share the information with and where and how it is processed;
- conduct thorough due diligence with any potential supplier prior to commissioning their service;
- verify any connections you have, ensuring that the principles of least privilege and segregation of duties are enforced throughout;
- perform tests over systems developed for you by third parties, where possible;
- have assurances from your processors before sharing any information with them and have documented service level and security agreements;
- review your contractual relationship with your suppliers and understand the responsibility each has, especially about an incident that stems from the supplier's network; and
- be aware when procuring software as a service (SaaS) that you rely on the vendor supplying you with relevant logs if the system is compromised and logging may be limited.

Incident response for supply chain attacks is like any incident response, but supply chain attacks rely on trust. You should demonstrate you understand all your third-party connections and, with the use of appropriate tools, be able to detect unexpected actions, discover malicious code, and deny access to possible threats.

Further reading:

- Supply chain security resources - NCSC
- Introduction to zero trust - NCSC
- How to assess your supply chain - NCSC
- Guidance on supply contracts - ICO
- Training to manage supply chain risk - NCSC
- Supply chain mapping guidance - NCSC

What are the likely future developments?

Research by Gartner showed attackers are targeting software development systems and open-source artifacts to compromise software supply chains. Gartner predicts that, "…by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021." The research demonstrated an escalating threat to software supply chains with attackers targeting build pipelines. This increased risk requires robust DevOps (development and operations) security controls.

Inserting malicious code into open libraries means that every other project that uses the code will be susceptible to the vulnerability created. In a market which is focused on innovation at speed, code sharing and insecure ad-hoc tooling is a potential area of vulnerability.

You must develop systems and all their components with security in mind from the outset. Positive developments are taking place with an increased focus on security-by-design, with DevOPs moving to a DevSecOps model. This aims to integrate security into the software development lifecycle in order to prevent security vulnerabilities becoming apparent in production and save the resource required to fix post-release flaws.

Conclusion

There is no single solution to security. The principles that are embedded in our guidance, and guidance from the NCSC, can help reduce the probability of an attack occurring or reduce its severity. However, there is no guarantee that systems and people won't be affected. You should still document and test your plans for incident response, business continuity, and disaster recovery.

As set out in the guidance referenced within this document, if your security is breached, you must consider the nature of the information (the level of sensitivity) and the risk of harm. You must balance security against the nature of any processing, to determine if your proposed or current security measures are enough to minimise harm to people.

This review examines several case studies, but of course different organisations will have different challenges. You may need to implement different measures to those of other organisations, depending on the level of risk.

You should not benchmark yourself against other organisations, even if they appear to have a similar structure or provide similar services. You will have your own mission and objectives. You should assess your current state against your target state. The best baseline for measuring your performance is your own.

During our review, we observed that is also important to appreciate the importance of governance and ensure that resources with appropriate skills are available. The NCSC encourages boards to take a more proactive approach to overseeing cyber risks within their organisations. Bodies, such as the UK Cyber Security Council, set standards for practitioners across the sector in support of the UK Government's National Cyber Security Strategy, to make the UK the safest place to live and work online. You must have organisational controls, in addition to physical and technical measures.

Key take aways

Our enforcement information has shown that we investigate cyber related data breaches which are often entirely avoidable.

If you have large volumes of personal information, then you must consider how to remedy or mitigate potential threats to security in your risk assessment.

We have taken enforcement action against organisations who have failed to:

- secure external connections without multi-factor authentication (MFA);
- log and monitor systems, and act when there is unexpected exfiltration or there are unexpected RDP connections from the internet;
- act on alerts from endpoint protection, such as anti-malware or anti-virus. This includes when there has been successful removal of malware, as the possibility of advanced persistent threat (APT) exists;
- use strong passwords on internal accounts or use unique passwords across multiple accounts, or both. In particular, for privileged, administrator or service accounts; and

- mitigate against known vulnerabilities, applying critical patches within 14 days, where possible. Our information evidences breaches where organisations have failed to address known vulnerabilities for more than a year, in some cases, many years.

Further reading

- Our guide to data security
- Our security outcomes guidance and resources
- NCSC’s cyber security toolkit for Boards

Further support

The NCSC provide a free check service for UK organisations. It carries out a range of simple online checks to identify common vulnerabilities in your public-facing IT. All checks are remote, do not require you to install software, and use the same kind of publicly available information as criminals use to find easy targets.

- Check your cyber security
- UK Cyber Security Council