National Cyber Security Centre
a part of GCHQ

Cyber threat report: UK charity sector

January 2023

Scope

The purpose of this report is to help charities understand current cyber security threats, the extent to which the sector is affected and whether it is being targeted, and where charities can go for help. This report is an update to NCSC's February 2018 "Cyber threat assessment: UK charity sector".

This report draws on consultation with experts within the National Cyber Security Centre (NCSC), other government departments and open sources, and was written with the support of The Charity Commission for England and Wales.

The National Cyber Security Centre (NCSC), a part of GCHQ, is the UK's technical authority for cyber security. Since the NCSC was created in 2016 as part of the Government's National Cyber Security Strategy, it has worked to make the UK the safest place to live and work online.

The Charity Commission for England and Wales registers and regulates charities in England and Wales, to ensure that the public can support charities with confidence. It works in partnership with the NCSC to enhance the cyber resilience of charities.

Contents

4 Foreword

6 The charity sector

7 Why is the charity sector particularly vulnerable?

8 Who might target the charity sector?

11 The main methods of cyber attack

13 How to improve your charity's cyber security

18 All links

Foreword: Lindy Cameron

As a charity trustee and international development professional, keeping charities, their donors and beneficiaries secure online matters a lot to me personally. I am very pleased to introduce this updated threat report for the charity sector, which has been developed to respond to the needs of the sector so we can all focus our efforts as effectively as possible.

The charity sector plays a vital role in supporting the most vulnerable people in our society. The sector's services were essential during the COVID-19 pandemic and continue to be during the cost of living crisis; and their efforts internationally have been vital during periods of conflict and crisis. Charities work tirelessly and innovatively to maintain their support to beneficiaries, despite facing enormous challenges.

More charities are now offering online services and fundraising online, meaning reliable, trusted digital services are more important than ever. During the Ukraine crisis, we saw more criminals taking advantage of the generosity of the public, masquerading as charities for their own financial gain.

Cyber attacks affecting services, funds or compromising sensitive data can be devastating financially and reputationally, potentially putting vulnerable people at risk. The NCSC continues to support this vital sector and encourages all readers of this report to implement the guidance within it.

Lindy Cameron - Chief Executive Officer, NCSC

Foreword: Helen Stephenson

Charities play a crucial role in our society and in every community. They save lives, and they provide many of the services that make life worth living.

All charities ultimately rely on public trust and continued public generosity. So the impact of any cyber attack on a charity can therefore be devastating, not just for the organisation and those who rely on its services, but also in undermining public confidence and support.

Taking steps to stay secure online is not an optional extra for trustees, but a core part of good governance. We welcome this report and urge trustees to take early action to protect their charities from cyber harm.

Helen Stephenson – Chief Executive, Charity Commission for England and Wales

The charity sector

Charities in the UK range from large, internationally recognised organisations to small, local community ones. The range of activity by UK charities is diverse, benefitting many sections of society, both here and overseas. All charities with an annual income of over £5,000 are required to register with a UK charity regulator.

There are 200,000 charities registered in the UK with a combined annual income of £100 bn. In England and Wales alone over a million people are employed in the charity sector with over 5 million volunteers.

DCMS Cyber Security Breaches Survey

The DCMS Cyber Security Breaches Survey measures the policies and processes organisations have for cyber security, and the impact of breaches and attacks. In the 2022 survey 30% of UK charities identified a cyber attack in the last 12 months. Of those attacks, 38% had an impact on the service with 19% "*resulting in a negative outcome*".

Charity Commission for England and Wales

169,029

registered charities

with a combined annual income of

£83.8 bn

Scottish Charity Regulator

24,020

registered charities

with a combined annual income of

£13.7bn

Charity Commission for Northern Ireland

6,691

registered charities

with a combined annual income of

£2.3bn

Why is the charity sector particularly vulnerable?

The charity sector faces the same cyber risks as private sector and government organisations but there are some reasons why charities could be particularly vulnerable to cyber attack:

Charities are attractive targets for many hostile actors seeking financial gain, access to sensitive or valuable information, or to disrupt charities' activities

Charities may feel reluctant to spend resources, money, oversight and staff effort on enhancing cyber security rather than on front line charitable work

Charities are less likely than businesses to employ technical cyber security controls.
(DCMS Cyber Security Breaches Survey 2022 4.4)

Charities have a high volume of staff who work part time, including volunteers, and so might have less capacity to absorb security procedures

Charities are more likely to rely on staff using personal IT (Bring Your Own Device) which is less easy to secure and manage then centrally issued IT

64% of charities report their staff regularly using their own devices, vs 45% of businesses.
(DCMS Cyber Security Breaches Survey 2022 2.3)

And finally, the impact of any cyber attack on a charity might be particularly high as charities often have limited funds, minimal insurance coverage and, by their very nature, are a supplier of last resort providing services where there is insufficient government or affordable private sector alternatives

22% of charities have cyber security insurance as part of a wider insurance policy; 5% have a specific cyber security insurance policy.
The lower the charity's income, the less likely they are to have cyber security insurance.
(DCMS Cyber Security Breaches Survey 2022 4.3)

Who might target the charity sector?

Like any other organisation, charities are increasingly reliant on IT, and cyber criminals make no distinction between charities and business. They often rely on supplier organisations to handle financial transactions, or to provide technical support. Even if a charity is not targeted, these organisations in their supply chain may be.

Cyber criminals

Cyber criminals are motivated by financial gain. They may seek to directly steal funds held by charities or seek to capitalise indirectly through fraud, extortion or data theft.

Cyber criminals vary from advanced, professional groups to small-scale fraudsters. The technical skill required to commit cyber offences varies depending on the goal of the attacker and some of the tools required are available through online criminal forums.

There is growing availability of criminal services for hire; the offender can buy 'off the shelf' services from another criminal group and so do not need to have advanced technical skills themselves.

This change has led to an increase in the scale of cyber crime and a less targeted approach to victims - criminals will indiscriminately target *all* organisations.

This means cyber criminals, rather than targeting organisations specifically, will attack thousands of organisations using largely automated tools that require little technical knowledge. A charity with few resources could be devastated if caught up by (for example) a ransomware attack. They are more vulnerable to attack, perhaps via unpatched vulnerabilities on unmanaged devices, or due to untrained volunteers and staff. Once attacked, a relatively small financial or reputational loss may be disastrous.

Nation states

Nation states conduct cyber activities to further their own national agenda and prosperity, or to disrupt professionals working on issues the state disagrees with, including human rights or those wanting regime change.

Russia, Iran and North Korea have all been identified as using criminal actors for state ends, operating to raise funds and cause disruption using criminal malware techniques. While they are unlikely to specifically target charities as a sector the range of hostile activity is so broad that UK charities will have been victims.

UK and allies expose Iranian state agency for exploiting cyber vulnerabilities for ransomware operations

"Iranian-state actors have been observed actively targeting known vulnerabilities on unprotected networks, including in critical national infrastructure (CNI) organisations." - UK and Allies advisory September 2022

The UK charities most at risk from nation state attacks are those that operate either directly, or through local partner organisations, overseas. Others that could be at risk are those which play a role in helping formulate and deliver UK domestic and foreign policy.

State actors, for example from China, have also used cyber techniques against UK institutions for Intellectual Property theft which is a risk for charities working on science or technology.

ICRC cyber attack in January 2022

"The attack compromised personal data and confidential ICRC information of more than 515,000 vulnerable people, including those separated from their families due to conflict, migration and disaster, missing persons and their families, and people in detention. The attackers used a very specific set of advanced hacking tools designed for offensive security. These tools are primarily used by advanced persistent threat groups, are not available publicly."

The Citizen Lab, a Canadian Academic research lab, has been working for a number of years to expose the use of private sector surveillance technology, sold to governments and then used *"against human rights and civil society actors."*

Hacktivists

Hacktivist is a term used to describe computer hackers motivated by a specific cause, for example to further political or personal agendas or in reaction to events or actions they perceive as unjust. Hacktivists have successfully used distributed denial of service (DDoS) attacks to disrupt websites, or have exploited weak security to deface them.

The charity sector is not a priority target for hacktivists, but even a limited website takedown or defacement could have financial, operational or reputational implications. There are examples of hacktivist groups launching cyber attacks against government and private sector websites so charities that support contentious issues could be at risk of attack.

SiegedSec turns hacktivist to target 'pro-life' US government entities after Roe v Wade ruling

"Hacking gang SiegedSec says it has leaked eight gigabytes of data stolen from two US state governments online in protest at the overturning of the decision in the Roe v Wade case. The group says it will embark on a hacktivist campaign against "pro-life entities" in the US following last week's decision by the US Supreme Court."

Insider threat

Insider threat is the deliberate or accidental threat to an organisation's security from someone who has authorised access such as an employee, volunteer, contractor or supplier.

Malicious insiders can pass on credentials to attackers or conduct activities such as stealing data. They may be motivated by a variety of reasons such as a grievance against the organisation, ethical concerns about its activity or have financial pressures leaving them vulnerable to coercion. However, insider threats are not always malicious. Employee breaches of security can stem from unclear or onerous processes, lack of training or simply mistakes.

Insiders are a risk to any organisation but charities may be more vulnerable due to a high turnover of staff, for example if a lot of volunteers are involved, and if there is limited staff training or security monitoring.

Supply chain attacks

(suppliers and third parties)

Cyber threats may not come from direct attacks on charities but they could still be affected. It is common, especially for smaller charities, to outsource the responsibilities for running, maintaining and securing their IT and data to specialist support companies.

... only 12% and 4% of micro businesses and charities take action to address supply chain cyber risks, giving cause for concern as smaller organisations compose a high proportion of the UK population and are often more reliant on outsourced IT providers.
Cyber Security Breaches Survey 2022 (4.9)

Charities may also share data with external organisations such as marketing companies. Cyber criminals and other groups may be able to gain access to charities' networks and/or information through these companies.

Blackbaud: Bank details and passwords at risk in giant charities hack

In October 2020 it was reported that "*Bank account information and users' passwords are among details feared stolen by hackers in a security breach at a service used to raise donations from millions of people. Many UK universities and charities, as well as hundreds of other organisations worldwide, use the software involved. Its developer Blackbaud made the admission in a regulatory filing*".

The main methods of cyber attack

Phishing

'Phishing' is when criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer, or steal bank details or other personal information.

Phishing is often untargeted, in the form of a mass email, text or cold calling campaign. However an attacker may use more targeted information to make their messages more persuasive and realistic (sometimes known as 'spear phishing').

The outward facing nature of charities, culture of trust in the sector, reliance on volunteers, staff members using personal IT, and reluctance to spend limited funding on cyber security training and measures could make them particularly vulnerable to criminality.

Fake organisations and websites

Criminals can exploit the credibility and appeal of charities to trick donors into giving money to what appears to be a legitimate charity, or they can set up fake charities or impersonate well-known charity names to add credibility in phishing campaigns. Although not directly targeting charities by cyber means, this activity has potential financial and reputational ramifications for genuine charities.

Public urged to donate safely this Christmas as it's revealed £1.5m was lost to online charity fraud over the past year.

In November 2021 the Fundraising Regulator, the Charity Commission for England and Wales, National Trading Standards and Action Fraud ran a joint publicity campaign to call on the public to give safely when donating online.

Business Email Compromise

Business Email Compromise (BEC) is a form of phishing attack where a criminal attempts to trick someone into transferring funds, or revealing sensitive information. In BEC a cyber criminal initially compromises a business email account through social engineering or computer intrusion techniques. After using this access to check out the organisation, the criminal then pretends to be the account owner over email or phone conversations to redirect payments to fraudulent bank accounts. BEC actors can create auto-forwarding rules within email to decrease the victim's ability to observe fraudulent communications.

This attack route took advantage of the shift to remote working during the pandemic, with staff working in isolation at home and their IT less able to be monitored for unusual activity.

Hospice case study

In 2019, a member of staff at a small hospice in the West Midlands received an email purportedly from Microsoft, asking them to change their email password, which they did. A few hours later, a second email arrived stating the password update was unsuccessful, and they should re-enter their original password (which they also did).

The next day, a donor rang the hospice, querying a suspicious email they'd purportedly received from the same member of staff. After receiving similar calls from 5 different people, hospice staff raised their concerns with a hospice director and their outsourced IT provider. On investigating the (by now quarantined) computer, the provider discovered criminals had taken control of the email account, and had changed the 'email forwarding rules', so the user could not see any emails being sent from their account.

Further investigations found credit card details of 35,000 users stored on the computer, which could have been accessed by the criminals.

The hospice reported the incident to Action Fraud, the ICO and Charity Commission, all of whom were supportive. Fortunately, the criminal made no ransom demands, and there was no evidence the card details were used. The hospice wrote to all donors to inform them what had happened, and although numbers on their mailing list reduced, donation levels remained the same. In addition to reputational damage, the cost of dealing with (and recovering from) the cyber attack was £17,000.

Since the incident, the hospice has:

- focussed on cyber security training for all staff
- started using NCSC's Web Check and Mail Check tools
- achieved Cyber Essentials Plus certification
- implemented two step verification (2SV)

"Even though we have to accept no organisation will ever be 100% secure, we can confidently tell all of our supporters, and those that we care for, that we take the security of their personal data very seriously and have taken every possible step to make our hospice as digitally secure as possible. The reputational damage would have been far worse had we not been honest about a mistake made by a member of staff."

Hospice Director of Operations

"Business Email Compromise (BEC) continues to be a significant issue facilitated by phishing and sophisticated social engineering. BEC is unlikely to be identified unless a customer/ client informs the company of the potential discrepancy in their email correspondence, at which point significant funds have been extracted" - NFIB

Ransomware

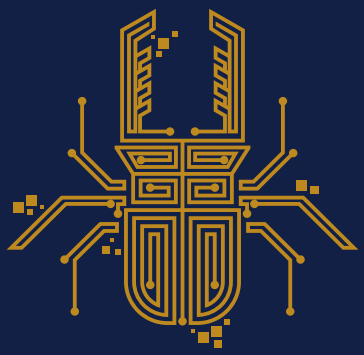
Ransomware is the most harmful cyber crime threat to the UK today. It is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption, while threatening to delete or leak the data they have stolen. The technique is now so evolved that criminal groups offer Ransomware as a Service (RaaS), whereby ransomware variants and commodity listings are available off the shelf for a one-off payment or a share of the profits.

Edinburgh Festival Fringe Society case study

The Edinburgh Festival Fringe Society (a charity that underpins the Festival) was victim of a ransomware attack in January 2022. They informed their staff straightaway and arranged for disaster recovery help from a cyber security company.

Although their system segmentation rules had helped minimise the number of systems the cyber criminals had managed to infiltrate, historic staff information was at risk. Recovering from the attack cost £95k, of which only £25k was covered by insurance so the Society had to fund the difference from their charity reserves.

"Ransomware continues to be a successful cyber attack and although the extent of the harm is underreported by most victims, ransomware remains hugely profitable for individuals and group offenders and equally disruptive for victims." - National Fraud Intelligence Bureau (NFIB) Action Fraud



How to improve your charity's cyber security

We strongly recommend that all charities:

Read and implement the NCSC's guidance that has been especially created for charities

Improve your staff (and volunteers') cyber awareness by using the NCSC's staff training resources

Consider using the NCSC's Active Cyber Defence services, which can provide a range of automated protections, free of charge to charities

Make sure the charity's board understands its responsibility regarding cyber security, and knows what questions to ask

Use Cyber Essentials, a government-backed scheme that will help protect your organisation from cyber attacks (and convince potential donors that you take cyber security seriously)

Guidance

All charities

If your charity's brand is being exploited online via a fake website, you can find out how to remove this in the NCSC's takedown guidance.

You can also protect your communications with your service users, donors and partners by following the NCSC's Business Communications guidance.

Smaller charities

The Small Charity Guide contains everything you need to build a firm foundation of cyber defence for your small charity. Additional resources are available including links to webinars produced by Charity Digital in partnership with the NCSC.

Larger charities

Larger charities with more complex IT will benefit from our more technical guidance. You can find out which areas you need to improve by applying for Cyber Essentials certification, or by running the Cyber Essentials readiness tool (see below).

Key guidance:

- 10 Steps to Cyber Security: designed for security professionals and technical staff as a summary of NCSC advice, and provides links to more detailed guidance where applicable
- Mitigating malware and ransomware hub: all the guidance relevant to defending your charity against these key threats
- Cyber insurance guidance: what to consider when thinking about cyber insurance
- Bring your own device: developing a policy and approach to BYOD

Training

Smaller charities

Smaller charities in particular may benefit from staff working through the NCSC's e-learning package Top Tips for Staff. This package has been designed for a non-technical audience with little or no knowledge of cyber security. It can be used in conjunction with your existing policies and procedures, and can be modified to reflect your own branding and/or built into your own learning platform.

Larger charities

While larger charities may also want to use the e-learning package, they also have the option to engage a NCSC Certified Training provider.

You may also want to utilise the NCSC's Board Toolkit to encourage essential cyber security discussions between your Trustees and your technical experts.

NCSC services

The NCSC's Active Cyber Defence (ACD) programme provides services aimed at protecting most people from most harms caused by cyber attacks, most of the time. Speak to your IT staff about considering the following, which can significantly improve your cyber security, and are free for charities.

All charities

- Early Warning: helps organisations investigate cyber attacks on their network by notifying them of malicious activity that has been detected in information feeds
- Exercise in a Box: a toolkit of realistic scenarios that helps organisations practise and refine their response to cyber security incidents in a safe and private environment

Larger charities

- Web Check: helps you find and fix common security vulnerabilities in the websites that you manage
- Mail Check: helps organisations assess their email security compliance and adopt secure email standards which prevent criminals from spoofing your email domains

Smaller charities

The NCSC is launching a new 'Check Your Cyber Security' service in March 2023. This will help non-technical users find and fix some of the most important cyber security issues.

Governance

The Board is responsible for making sure a charity is taking appropriate measures to protect itself from a cyber attack - not the IT department, or third party provider.

The Cyber Security Toolkit for Boards is a set of resources designed to encourage essential cyber security discussions between the Board and their technical experts. For charities, these questions can be asked by the charity board, the trustees, or both. Trustees of small charities may find that questions aimed at school governors and trustees are at the right level.

Assurance scheme - Cyber Essentials

NCSC's Cyber Essentials Scheme, provided through the IASME Consortium, assesses organisations' ability to protect themselves from the most common cyber threats, and reassures their stakeholders that cyber security is taken seriously.

UK organisations with a turnover under £20m that achieve whole-organisation Cyber Essentials certification are eligible for free Cyber Liability Insurance.

Case study: Sara Ward, the CEO of Black Country Women's Aid, discusses her organisation's experience of gaining Cyber Essentials Plus certification.

As well as paid certification routes, IASME runs a free Cyber Essentials readiness tool that will create a personal action plan to help you move towards meeting the Cyber Essentials requirements. Data from 2021 and 2022 use of the tool highlights some of the easy, low or no cost wins charities can implement to make their systems more secure, such as:

- implement multi-factor authentication on cloud services
- disable autorun/autoplay of new software installations (action 3)
- have a policy for creating good passwords
- have a process for tracking the user accounts of people who leave or join

All links

The charity sector

- **DCMS Cyber Security Breaches Survey:** https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022
- **UK Charity Commission for England and Wales in 2022:** https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1090647/Charity_Commission_Annual_Report_and_Accounts_published.pdf
- **Scottish Charity Regulator:** https://www.oscr.org.uk/media/4280/599187_sct0421394204-001_oscr_sector-overview-report_final.pdf
- **The Charity Commission for Northern Ireland:** https://www.charitycommissionni.org.uk/

Why is the charity sector particularly vulnerable?

- **DCMS Cyber Security Breaches Survey 2022 4.4:** https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#technical-cyber-security-controls
- **DCMS Cyber Security Breaches Survey 2022 2.3:** https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#use-of-personal-devices
- **DCMS Cyber Security Breaches Survey 2022 4.3:** https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#insurance-against-cyber-security-breaches

Who might target the charity sector?

- **NCSC - UK and allies expose Iranian state agency for exploiting cyber vulnerabilities for ransomware operations:** https://www.ncsc.gov.uk/news/uk-and-allies-expose-iranian-state-agency-for-exploiting-cyber-vulnerabilities-for-ransom-operations
- **UK and Allies advisory September 2022:** https://www.cisa.gov/uscert/ncas/alerts/aa22-257a
- **IRC cyber attack in January 2022:** https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know
- **The Citizen Lab:** https://citizenlab.ca/
- **Against human rights and civil society actors:** https://citizenlab.ca/wp-content/uploads/2019/02/Submission-to-the-UN-Special-Rapporteur-on-the-promotion-and-protection-of-the-right-to-freedom-of-opinion-and-expression-on-the-surveillance-industry-and-human-rights-2.pdf
- **SiegedSec turns hacktivist to target 'pro-life' US government entities after Roe v Wade ruling:** https://techmonitor.ai/technology/cybersecurity/roe-v-wade-hacktivist-siegedsec-abortion
- **DCMS Cyber Security Breaches Survey 2022 (4.9):** https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#cyber-accreditations-and-government-initiatives
- **Blackbaud: Bank details and passwords at risk in giant charities hack:** https://www.bbc.co.uk/news/technology-54370568

The main methods of cyber attack

- **National Fraud Intelligence Bureau (NFIB) Action Fraud:** https://www.actionfraud.police.uk/
- **Public urgent to donate safely this Christmas as it's revealed £1.6m was lost to online charity fraud over the past year:** https://www.actionfraud.police.uk/alert/public-urged-to-donate-safely-this-christmas-as-its-revealed-1-6m-was-lost-to-online-charity-fraud-over-the-past-year

How to improve your charity's cyber security

- **NCSC's guidance:** report page 14
- **Staff training resources:** report page 14
- **Active Cyber Defence services:** report page 15
- **What questions to ask:** report page 15
- **Cyber Essentials:** report page 16

Guidance

- **Small Charity Guide:** https://www.ncsc.gov.uk/collection/charity
- **Additional resources are available:** https://www.ncsc.gov.uk/collection/charity/resources
- **10 Steps to Cyber Security:** https://www.ncsc.gov.uk/collection/10-steps
- **Mitigating malware:** https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- **Ransomware hub:** https://www.ncsc.gov.uk/ransomware/home
- **Cyber insurance guidance:** https://www.ncsc.gov.uk/guidance/cyber-insurance-guidance
- **Bring your own device:** https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device
- **NCSC's takedown guidance:** https://www.ncsc.gov.uk/guidance/takedown-removing-malicious-content-to-protect-your-brand
- **NCSC's Business Communications guidance:** https://www.ncsc.gov.uk/guidance/business-communications-sms-and-telephone-best-practice

Training

- **Top Tips for Staff:** https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available
- **NCSC Certified Training:** https://www.ncsc.gov.uk/information/certified-training
- **NCSC's Board Toolkit**: https://www.ncsc.gov.uk/collection/board-toolkit

Assurance scheme - Cyber Essentials

- **Cyber Essentials Scheme:** https://www.ncsc.gov.uk/cyberessentials/overview
- **Free Cyber Liability Insurance:** https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/
- **Case study:** https://www.ncsc.gov.uk/blog-post/cyber-essentials-plus-is-for-charities-too
- **Cyber Essentials readiness tool:** https://getreadyforcyberessentials.iasme.co.uk/questions/
- **Implement multi-factor authentication on cloud services:** https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services
- **Disable autorun/autoplay of new software installations (action 3):** https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- **Have a policy for creating good passwords:** https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words
- **Have a process for tracking the user accounts of people who leave or join:** https://www.ncsc.gov.uk/collection/10-steps/identity-and-access-management

NCSC services

- **Active Cyber Defence (ACD):** https://www.ncsc.gov.uk/section/active-cyber-defence/introduction
- **Early Warning:** https://www.ncsc.gov.uk/information/early-warning-service
- **Mail Check:** https://www.ncsc.gov.uk/information/mailcheck
- **Exercise in a Box:** https://www.ncsc.gov.uk/information/exercise-in-a-box
- **Web Check:** https://www.ncsc.gov.uk/information/web-check

Governance

- **Cyber Security Toolkit for Boards:** https://www.ncsc.gov.uk/section/board-toolkit/home
- **Questions aimed at school governors and trustees:** https://www.ncsc.gov.uk/information/school-governor-questions