Cyber Security Schools Audit 2022

National Cyber Security Centre
a part of GCHQ

LGfL

Key Findings

Foreword

NCSC

The covid pandemic saw schools rely increasingly on technology to support teaching and learning with more lessons taking place in home and online settings than ever before. Whilst teaching has largely returned to the classroom, schools should now consider their online learning options for the future. This should be enabled by considering more options for upgrading their online digital estate and keeping it resilient in the face of current and emerging cyber risks and threats.

Our schools rely so much on the myriad of data required to run efficiently, including sensitive data on students, parents, governors and staff and yet more work is still to be done to support the cyber security around these essential services. The National Cyber Security Centre has been working with schools and the education sector to provide free tools and guidance to help schools manage their cyber risks effectively and supporting them to keep this valuable information safe.

Sarah Lyons,
Deputy Director for Economy & Society, NCSC

LGfL

Since we carried out the last audit in 2019, UK schools continue to experience ransomware attacks and the subject of cyber security in education has shot up the agenda.

In the same time period, the pandemic caused a significant and sudden shift towards remote-learning technologies and an even greater reliance on system availability. A cyber incident causing even a few minutes' outage can have a massive impact on teaching and learning.

Against this background, we were delighted to partner with the NCSC again to see if this had led to increased awareness and preparedness, with policies that impact upon practice. We wanted to see if there were more schools with an effective policy, risk register and business continuity plan in place.

The risks will only continue to grow, so it is key that we have a solid research base to offer schools the support they need, when they need it.

Mark Bentley,
Safeguarding & Cybersecurity Manager, LGfL

Introduction

In 2019 LGfL (the National Grid for Learning) and the NCSC (National Cyber Security Centre, a part of GCHQ) carried out a joint audit of cyber security in schools across the UK. This produced a snapshot of schools' current systems, protections, training needs and preparedness for a cyber incident. LGfL and the NCSC have repeated this audit in 2022 to see how the cyber security landscape for schools has changed.

The findings of this report will be used to help shape the response within the education sector in the face of a growing cyber risk, and to help schools focus on educating children in their care.

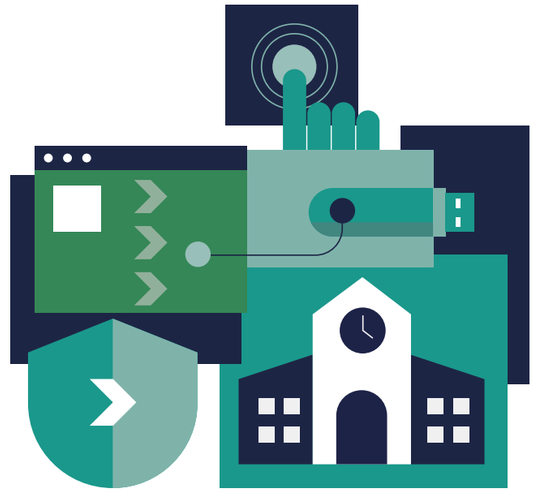
Method

The audit was open from **3 to 31 May 2022**.

805 schools took part, which was an **86%** increase from 432 schools in 2019.

Participation was particularly high in Scotland and London, but there was representation from all parts of the UK.

The statistics in this report were generated and verified by Statistical Services Centre Ltd.



Summary

Just over half of schools – **53%** - said they felt prepared for a cyber incident. This compares to **49%** in 2019

A substantial number of schools (**78%**) had experienced at least one type of cyber incident listed with **7%** experiencing significant disruption as a result.

Staff training of non-IT staff in cyber security has increased from **35%** (in 2019) to **55%**.

For example, **21%** of schools had experienced a malware and/or ransomware attack and **18%** had experienced periods with no access to important information.

Awareness of phishing in schools has increased from **69%** to **73%**.

100% of schools now have Firewall and **99%** antivirus protection.

49% of schools have included their core IT services in a risk register and/or business continuity plan showing an increase from **41%** in 2019.

Schools continue to need to focus on improvements to security with **4%** having no back-up facilities, **26%** not implementing multi-factor authentication and **25%** not limiting staff access to USB devices.

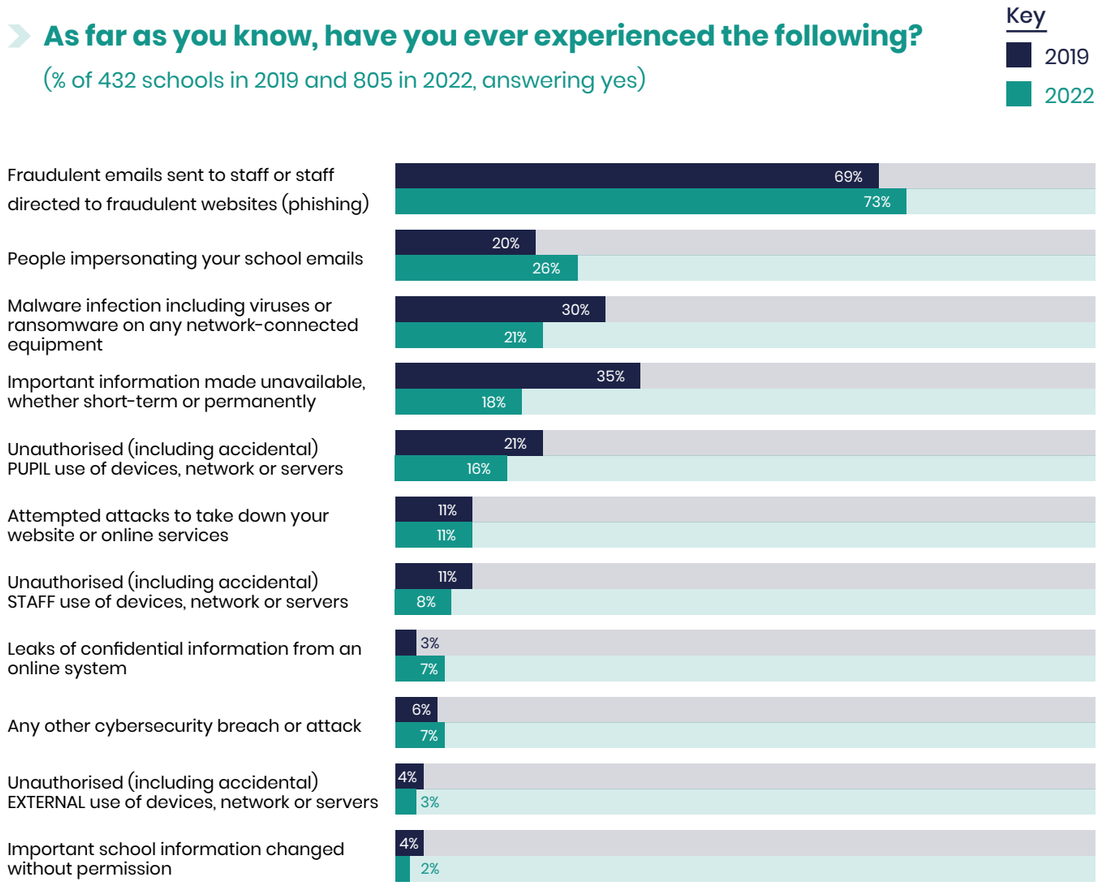
90% of schools have at least one of the following in place: a cyber security policy, a risk register or a business continuity plan. And a **third** of schools now have all three

In 2019, **no** school recorded a parent losing money due to a cyber incident, but in 2022 **six schools** reported they had.

Have you ever...?

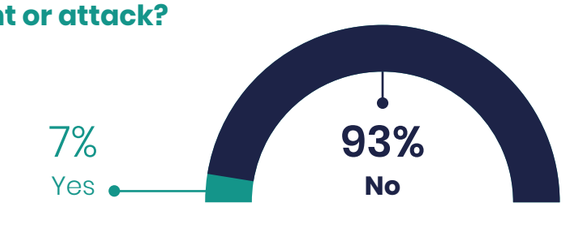
As far as you know, have you ever experienced the following?

(% of 432 schools in 2019 and 805 in 2022, answering yes)

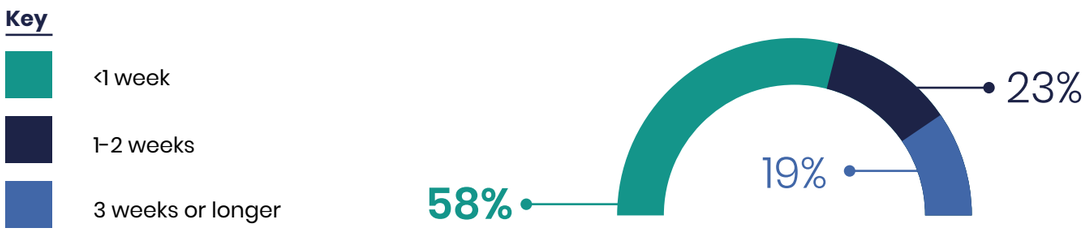


Did you experience any of the cyber incidents listed?

Has your school ever been significantly disrupted by a cyber incident or attack?



Time taken to recover from this attack



Of the schools surveyed, **22%** of schools believed they had escaped all types of incident that we asked about on page 6.

Whilst **7%** of schools reported being disrupted significantly by a cyber incident or attack, most of those schools are seemingly capable of recovering from these incidents. **81%** indicated that they recovered normal school operations in **under 3 weeks**.

Six schools knew of parents losing money due to a cyber incident or attack involving the school.

The NCSC **Response & Recovery**[1] guidance will help schools prepare their response to and plan their recovery from a cyber incident.

Breakdown of incidents

Key Changes

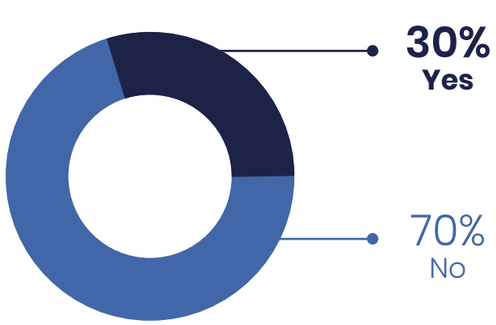
2019
(based on 432 schools)

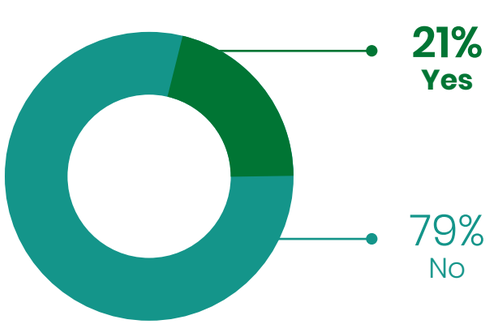
Yes No

2022
(based on 805 schools)

Yes No

Malware infection including viruses or ransomware on any network-connected equipment.





Mitigating malware/ransomware

NCSC guidance on **mitigating malware and ransomware attacks**[2] provides actions to help organisations prevent a malware infection, and steps to take if you are already infected.

Key Changes

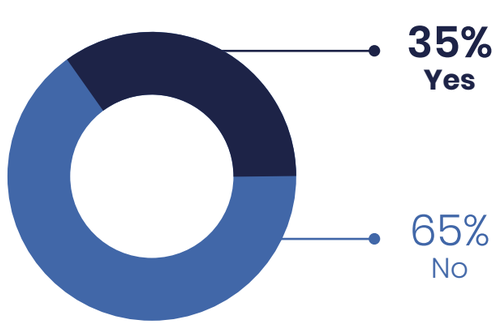
2019
(based on 432 schools)

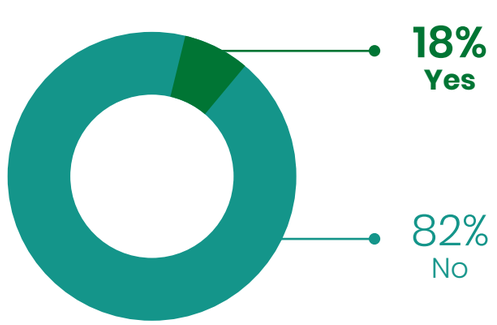
Yes No

2022
(based on 805 schools)

Yes No

Important information made unavailable, whether short-term or permanently





Important information made unavailable

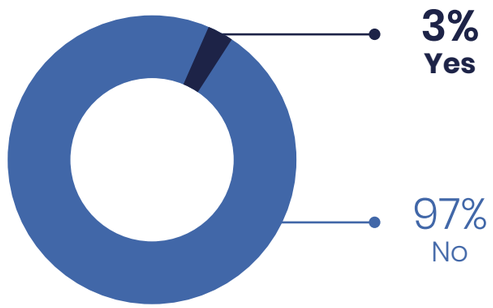
Since GDPR came into force in May 2018, schools have had new requirements places upon them regarding data access and protection. Nonetheless **18%** of schools experienced important information being made unavailable.

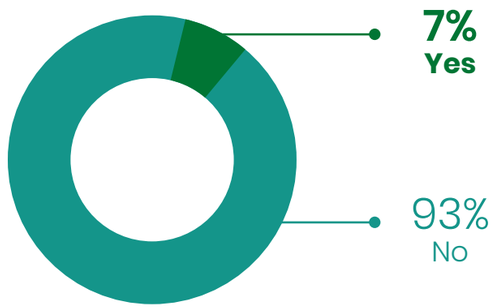
Key Changes

2019
(based on 432 schools)

2022
(based on 805 schools)

Confidential information leaked from an online system





Confidential information

Schools are obliged to publish **key information online** and safeguarding and attainment systems also need to be accurate and available at all times.

Confidential information being leaked could have serious ramifications for any school.

Schools reporting on fraudulent emails sent to staff

Key
Yes

Phishing

The NCSC's guidance on **Phishing attacks: defending your organisation**[3] provides schools with guidance for IT teams on how to defend your organisation from email phishing attacks.

Cyber security training for school staff[4] contains practical tips for how to combat phishing attacks and manage some of the key cyber threats facing schools.

School staff can learn to recognise and report **scam emails, texts, websites, adverts or phone calls**[5].

The NCSC **Small Business Guide**[6] offers helpful advice on phishing which is equally relevant for schools.

Schools reporting on people impersonating school emails

Email security and anti-spoofing

For school IT managers or administrators **Email security and anti-spoofing**[7] will support you in securing your schools email systems.

In addition, **Mail Check**[8] (which is part of the Active Cyber Defence programme), assists schools with email security configuration and reporting.

Schools reporting on a experienced attempted attack to take down their website or online services

Key
Yes

11%

Attempted take down of online services

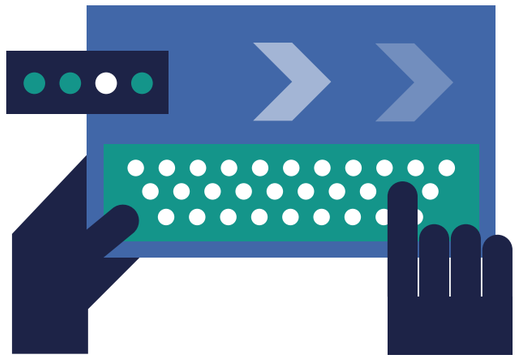
The NCSC's **Web Check**[9] tool helps you identify and fix common security issues in your websites. It is free to use for UK schools.

Schools reporting unauthorised (including accidental) use of computers, networks or servers

by pupils
16%

by staff
8%

by external
3%



Unauthorised use

Most IT accounts are protected by a password, with poor password management being one cause of unauthorised access. System owners in school can determine password policies and identity management using the NCSC's **password policy**[10] guidance.

Individual members of staff can learn about the importance of **using a strong and separate password for email**[11] and how to use **password managers**[12] safely.

Multi-factor authentication[13] or MFA (also known as two-factor authentication, 2FA; or **two-step verification**[14]) can help schools protect against password guessing and theft on online accounts.

Nonetheless, **16%** of schools had experienced unauthorised IT system use by pupils.

Exercising

Cyber incident exercising helps organisations to establish how resilient they are to cyber attack and practice their response in a safe environment.

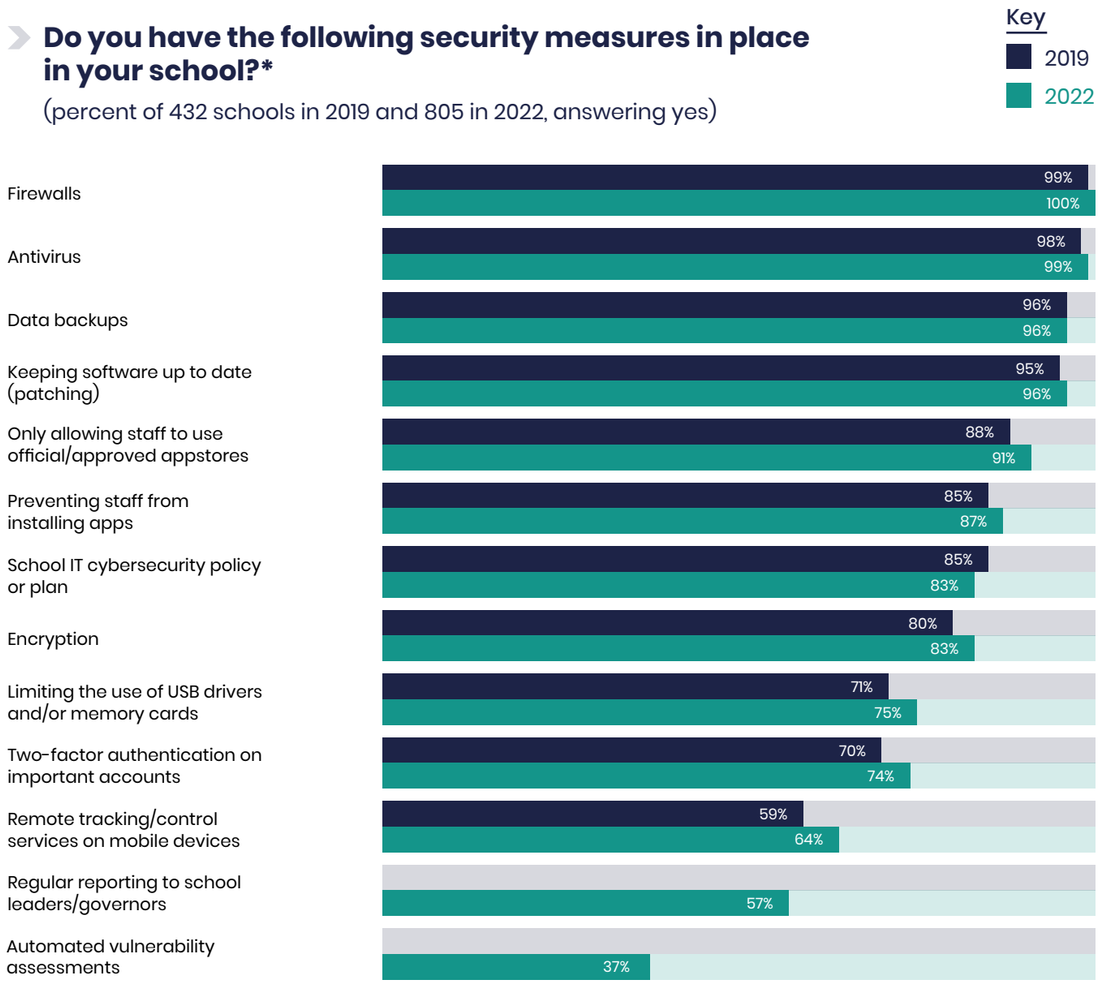
Exercise in a Box[15] is an online tool from the NCSC which can help your school to test and practice your response. It is completely free for schools to use and you don't need to be an expert to use it.

The NCSC provide guidance on **incident management**[16] including how to effectively detect, respond to and resolve cyber incidents.

Security measures taken by Schools

Do you have the following security measures in place in your school?*

(percent of 432 schools in 2019 and 805 in 2022, answering yes)



*Governor and vulnerability assessment questions were not asked during the 2019 audit

Highlights

100%
of schools have a firewall

99%
of schools have an anti-virus system

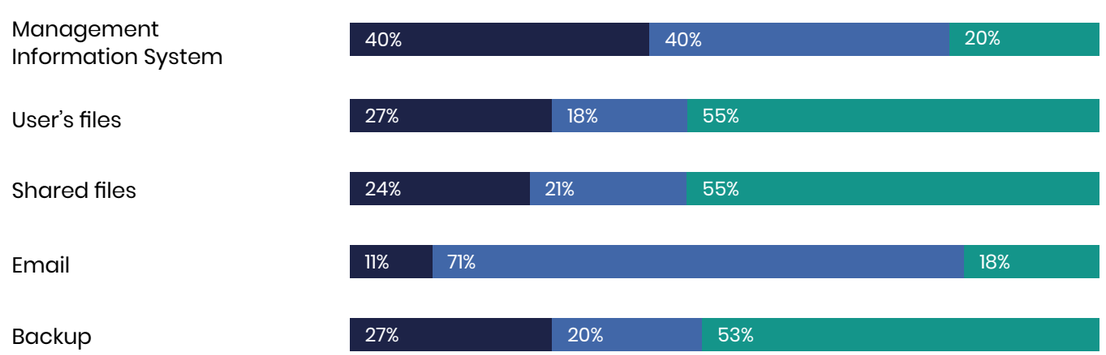
96%
of schools have a backup solution in place

96%
of schools patch their software

Antivirus[17], **backups**[18] and **patching**[19] followed **firewalls**[20] as the next three most popular attack-prevention technical measures in place. Each were present in at least **96%** of all schools, which is a reassuring sign of fundamental protections in place in UK schools.

Where are your core IT services?

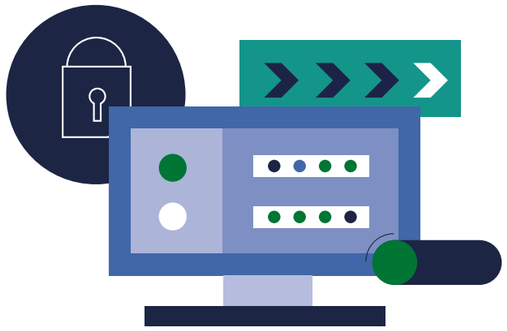
(Based on 805 schools)



The Cloud

Cloud usage continues to grow steadily, both in volume and the type of services being built and hosted in it. Cloud is usually the preferred option for schools whether exclusively or using a hybrid approach often hosting their servers on-premises.

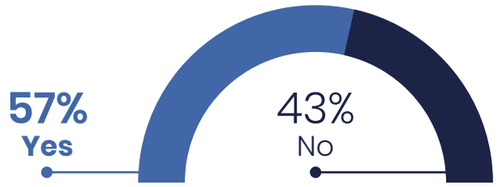
Against this background, it's essential that new services are chosen and built in a way which reflects their security needs and the **NCSC's cloud security guidance**[21] will support your school through this process.



Planning, Policy & Practice

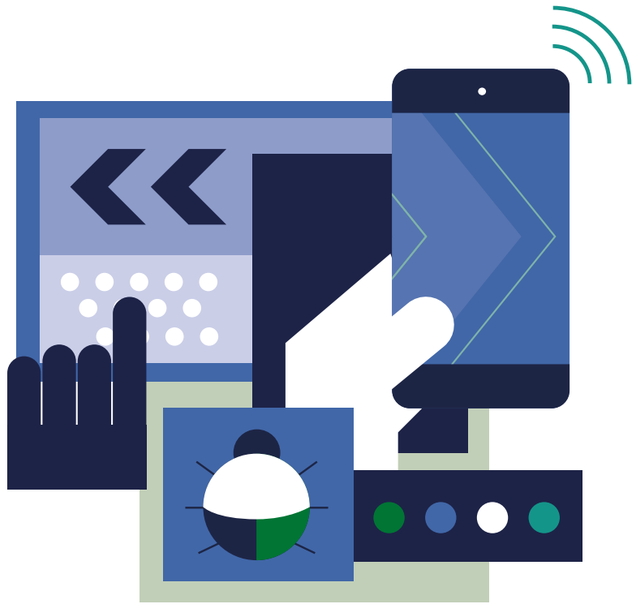
Schools rely heavily on IT and online services to function. They also hold large amounts of sensitive personal data on pupils, parents and staff. All this needs to be kept safe and secure.

Do you report regularly to school leaders and/or governors?

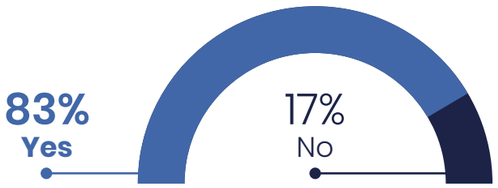


The NCSC has published a **list of questions**[22] for school governors and trustees to ask school leaders, to help improve a schools understanding of its cyber security risks.

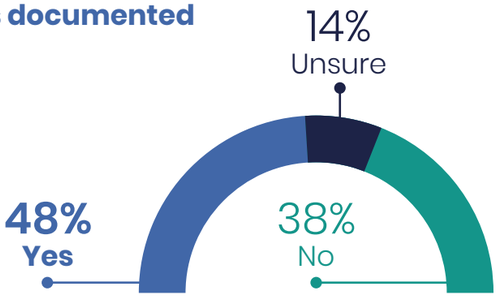
For larger schools or for those schools who want to deepen their understanding, the NCSC **Board Toolkit**[23] is an additional resource for advice on collaborating with suppliers and partners to support the protection of their own networks.



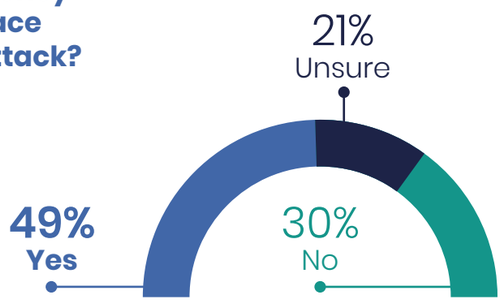
Does your school have an IT cybersecurity policy or plan?



Are your school's core IT services documented in a risk register or similar?



Does your school have a contingency or business continuity plan in place that covers a cyber-breach or attack?



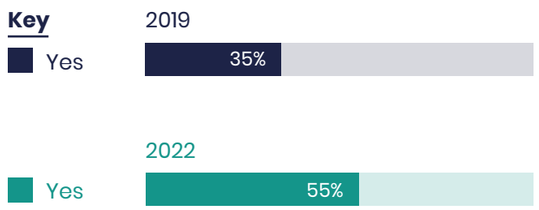
These three documents are generally interdependent and cross-reference each other to ensure joined-up planning, policy and practice. Yet **30%** of schools were unsure whether they had a business continuity plan and **38%** if their schools core IT services were documented in a risk register. In 2019, **41%** of schools had a business continuity plan, in 2022 this had increased to **49%**.

Training

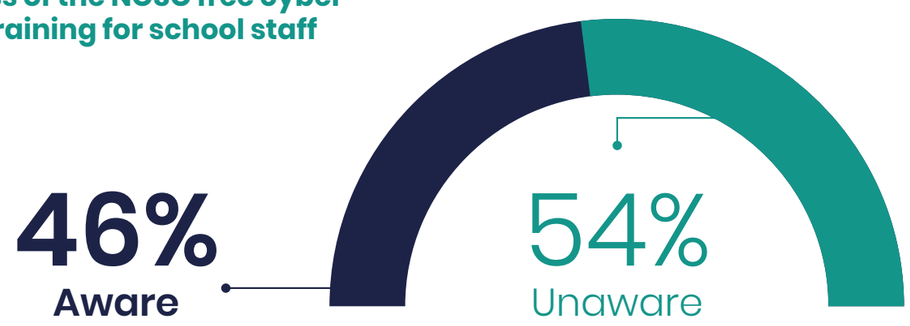
Since 2019, the NCSC has launched a range of resources including **practical tips**[24] and the **Cyber Security for Schools web page**[25] to support schools in training their staff.

Non-IT staff cyber security training has now increased from **35%** in 2019 to **55%** in 2022 with **46%** of schools now aware of the NCSC free **cyber security training for school staff.**[26]

Have any of your non-IT staff received cybersecurity training?



Awareness of the NCSC free cyber security training for school staff



More resources and guidance

For more resources, guidance and information on your cybersecurity needs for school, there are a number of additional resources you may want to consider.

- Cyber Security for Schools **web page**[25]
- The NCSC **website**[27]
- **Infographics**[28] for bringing technical guidance to life
- The NCSC **Education and Skills**[29] pages
- **Cyber Essentials**[30] – a government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks.
- **Active Cyber Defence**[31] – a range of free tools for schools to use to reduce the harm from commodity cyber attacks.

References

Have you ever?

1. **Response & Recovery** (https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery/resources)

Breakdown of incidents

2. **Mitigating malware and ransomware attacks** (https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks)
3. **Phishing attacks: defending your organisation** (https://www.ncsc.gov.uk/guidance/phishing)
4. **Cyber security training for school staff** (https://www.ncsc.gov.uk/information/cyber-security-training-schools)
5. **Scam emails, texts, websites, adverts or phone calls** (https://www.ncsc.gov.uk/collection/phishing-scams)
6. **Small Business Guide** (https://www.ncsc.gov.uk/collection/small-business-guide)
7. **Email security and anti-spoofing** (https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing)
8. **Mail Check** (https://www.ncsc.gov.uk/information/mailcheck)
9. **Web Check** (https://www.ncsc.gov.uk/information/web-check)
10. **Password policy** (https://www.ncsc.gov.uk/collection/passwords/updating-your-approach)
11. **Using a strong and separate password for email** (https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email)
12. **Password managers** (https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers)
13. **Multi-factor authentication** (https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services)
14. **Two-step verification** (https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email)
15. **Exercise in a Box** (https://www.ncsc.gov.uk/information/exercise-in-a-box)
16. **Incident management** (https://www.ncsc.gov.uk/collection/incident-management)

Security measures taken by Schools

17. **Antivirus** (https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product)
18. **Backups** (https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data)
19. **Patching** (https://www.ncsc.gov.uk/blog-post/the-problems-with-patching)
20. **Firewalls** (https://www.ncsc.gov.uk/cyberessentials/advice)
21. **NCSC's cloud security guidance** (https://www.ncsc.gov.uk/collection/cloud)

Planning, Policy & Practice

22. **List of questions** (https://www.ncsc.gov.uk/information/school-governor-questions)
23. **Board Toolkit** (https://www.ncsc.gov.uk/collection/board-toolkit)

Training

24. **Practical tips** (https://www.ncsc.gov.uk/blog-post/helping-school-staff-to-work-safely-online)
25. **Cyber Security for Schools web page** (https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools)
26. **Cyber security training for school staff** (https://www.ncsc.gov.uk/information/cyber-security-training-schools)
27. **Website** (https://www.ncsc.gov.uk/)
28. **Infographics** (https://www.ncsc.gov.uk/information/infographics-ncsc)
29. **Education and Skills** (https://www.ncsc.gov.uk/section/education-skills/schools#main)
30. **Cyber Essentials** (https://www.ncsc.gov.uk/cyberessentials/overview)
31. **Active Cyber Defence** (https://www.ncsc.gov.uk/section/active-cyber-defence/introduction)

National Cyber Security Centre
a part of GCHQ

LGfL

www.ncsc.gov.uk

To find this report online visit:
securityaudit.lgfl.net