CYBER SECURITY

SCHOOLS AUDIT 2019

KEY FINDINGS

National Cyber Security Centre
a part of GCHQ

LGfL

FOREWORD

NCSC

The internet and the wide array of digital applications and services available present schools with exciting opportunities to support teaching and learning, as well as enabling the effective management of a school. As the reliance on digital solutions in schools has increased, so has the importance of securing these technologies.

Alongside these important digital services, our schools also hold considerable amounts of sensitive personal information on parents, children and staff so it's more important than ever that schools have access to the appropriate tools and advice to help them keep this valuable information safe.

We welcome the role taken by the London Grid for Learning in leading this audit which will deepen our understanding of how cyber security is currently managed in school settings. The findings in this report will help the National Cyber Security Centre and our partner organisations work together with schools on practical solutions that meet the cyber security needs of the education sector across the UK.

Sarah Lyons,
Deputy Director for Economy & Society, NCSC

LGfL

Cyber security education within the school curriculum is key if we are to prepare tomorrow's workforce today – and schools are working hard on this – but there are other pressing needs too.

Budgets are tight, the curriculum is squeezed, and school is all about keeping children safe and providing the best-possible education. So you won't often hear schools talking about their cyber security preparedness.

Whilst it was hospitals rather than schools which suffered major disruption from the WannaCry virus, schools are just as likely as any organisation to face DDoS and phishing attacks.

That's why we were keen to work with the NCSC to establish exactly what is happening in schools and how we can help.

Mark Bentley, Safeguarding & Cybersecurity Manager, LGfL

INTRODUCTION

LGfL (London Grid for Learning) and the **NCSC** (National Cyber Security Centre, part of GCHQ) carried out a joint audit of cyber security in schools across the UK, to produce a snapshot of schools' current systems, protections and preparedness and future technology and training needs.

The findings of this report will be used to help shape and improve the UK's response to cyber security support in education in the face of a growing and sophisticated threat landscape, and to help schools focus on educating the children in their care.

METHOD

The audit was open from **15 March – 30 April 2019.**

432 schools took part.

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

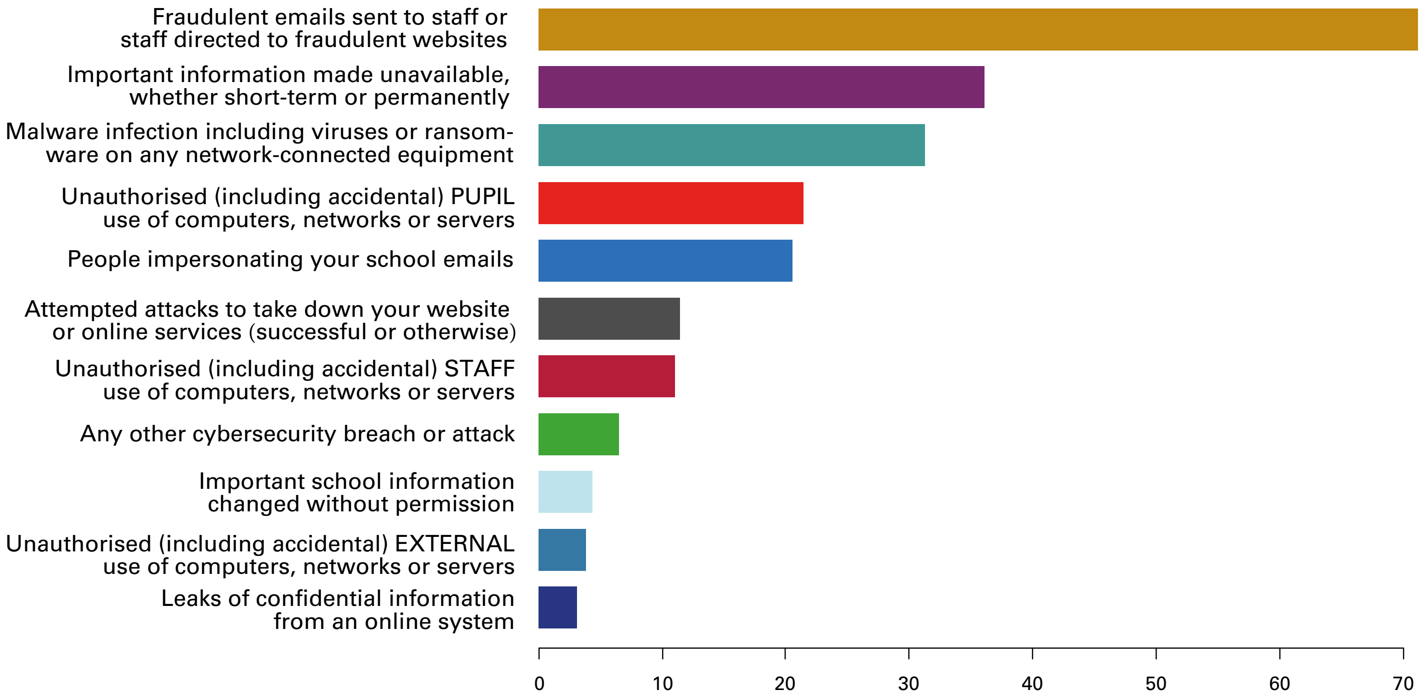
The statistics in this report were generated by Statistical Services Centre Ltd.

SUMMARY

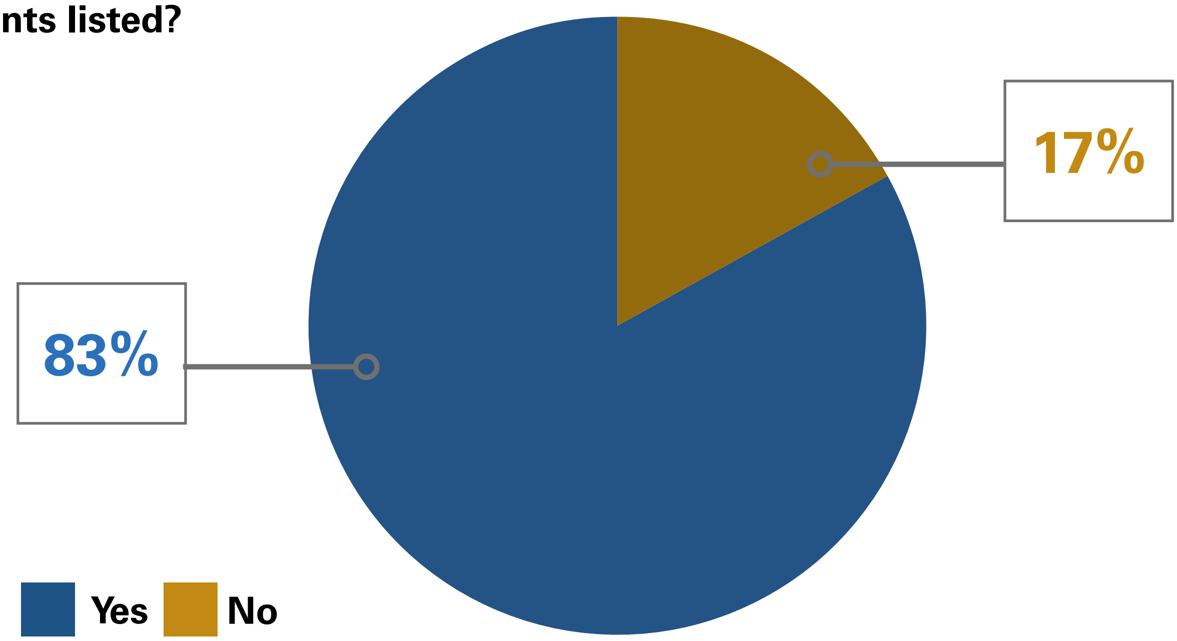
- Nearly all schools **(97 percent)** said that losing access to network-connected IT services would cause considerable disruption.
- Only around a third of schools **(35 percent)** train non-IT staff in cyber security.
- A focus on support for non-IT staff is a clear need, and it looks like this would be well received, with **92 percent** of schools telling us they would welcome more cyber security awareness training for staff.
- The vast majority of schools **(83 percent)** had experienced at least one of the types of cyber security incidents we asked about.
- For example, **69 percent** of schools had suffered a phishing attack and **35 percent** had experienced periods with no access to important information
- All schools had at least some of the protective technologies or systems in place that we asked about.
- **98 and 99 percent** of schools, respectively, had antivirus and firewall protections.
- There was relatively low use of strong cyber security practices such as mobile-device management and two-factor authentication.
- **85 percent** of schools had a cyber security policy or plan, but only **45 percent** included core IT services in their risk register and only **41 percent** had a business continuity plan.
- Less than half of schools **(49 percent)** were confident that they are adequately prepared in the event of a cyber-attack.

HAVE YOU EVER...?

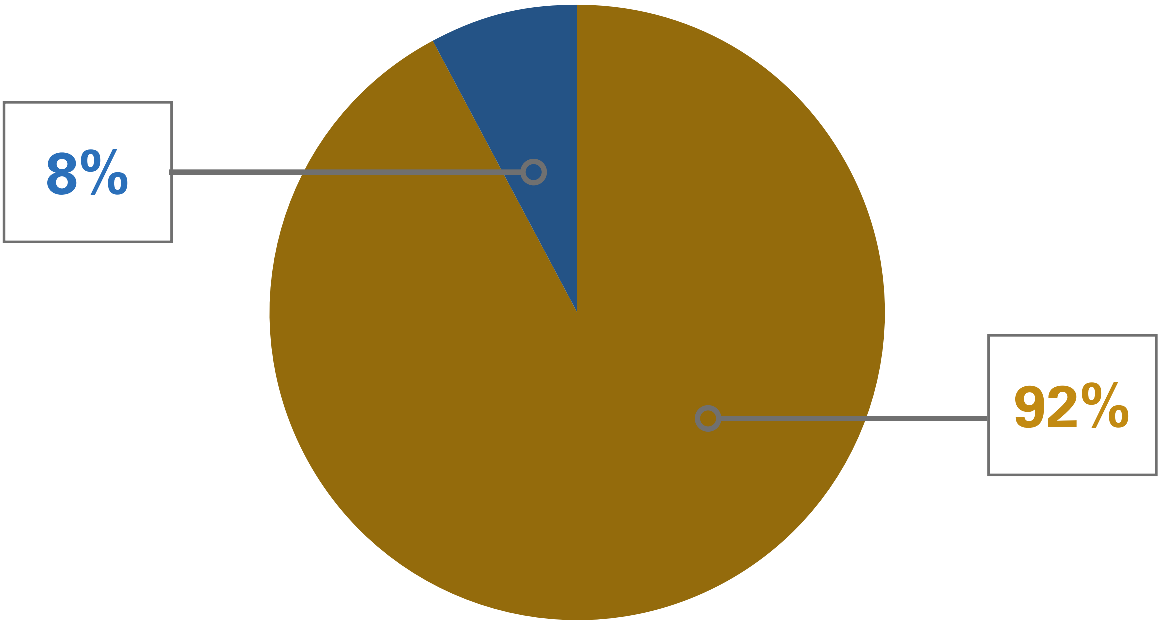
As far as you know, have you ever experienced the following? (% of 432 schools answering yes)

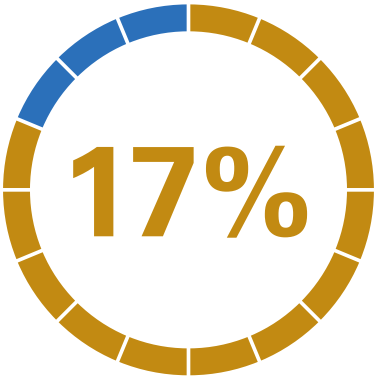


Did you experience any of the cyber-incidents listed?



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





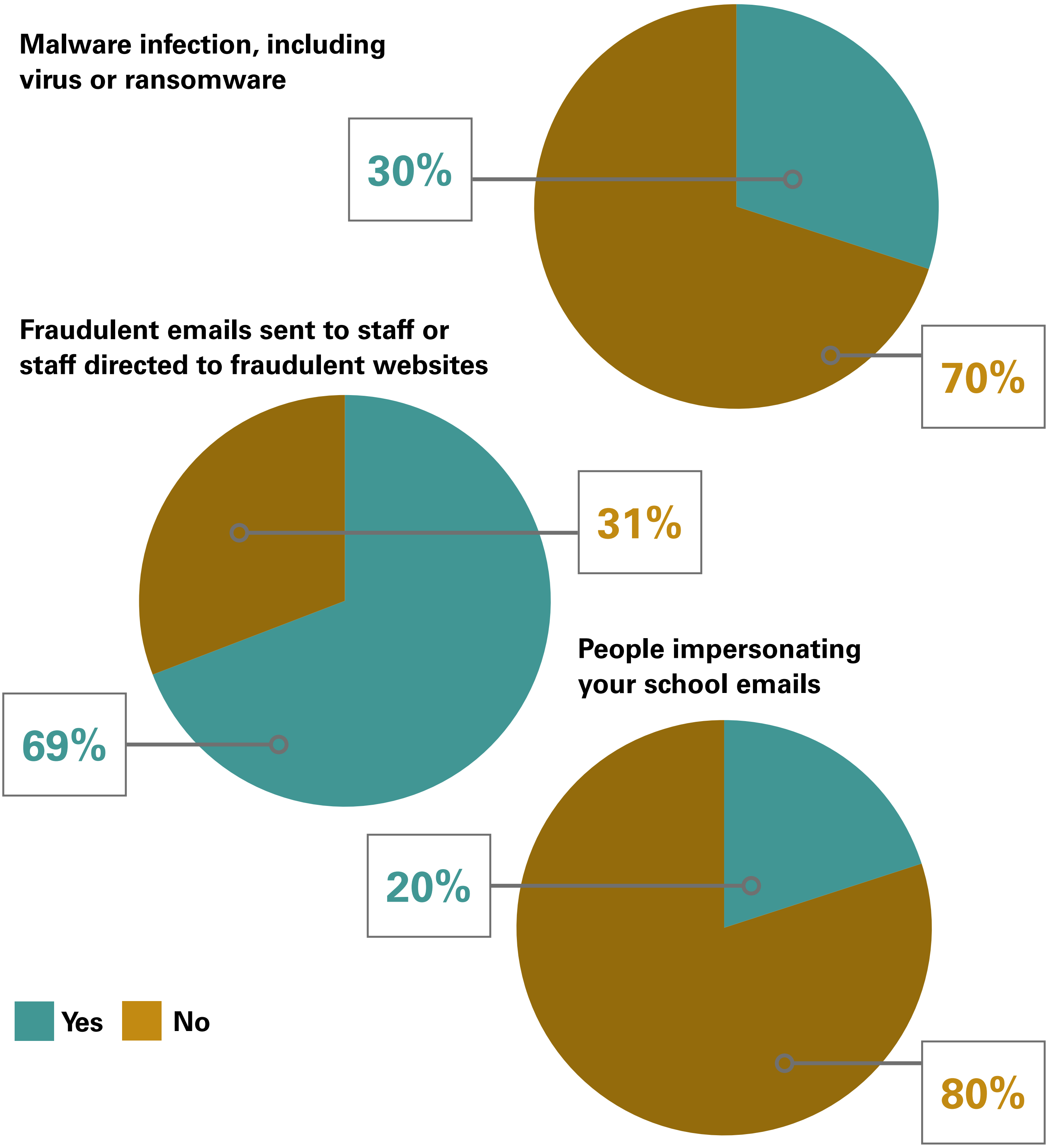
of schools believed they had escaped all types of incident we asked about (p4).

However, the impact of these incidents was seemingly well mitigated for the most part: only 8 percent of those questioned said that school life had been significantly disrupted by a cyber-incident.

There was only one incident that none of the 432 schools were aware of: not a single school knew of parents losing money due to a cyber-incident or attack involving the school.

🟦 **Yes** 🟨 **No**

BREAKDOWN OF INCIDENTS



Malware infection, including virus or ransomware

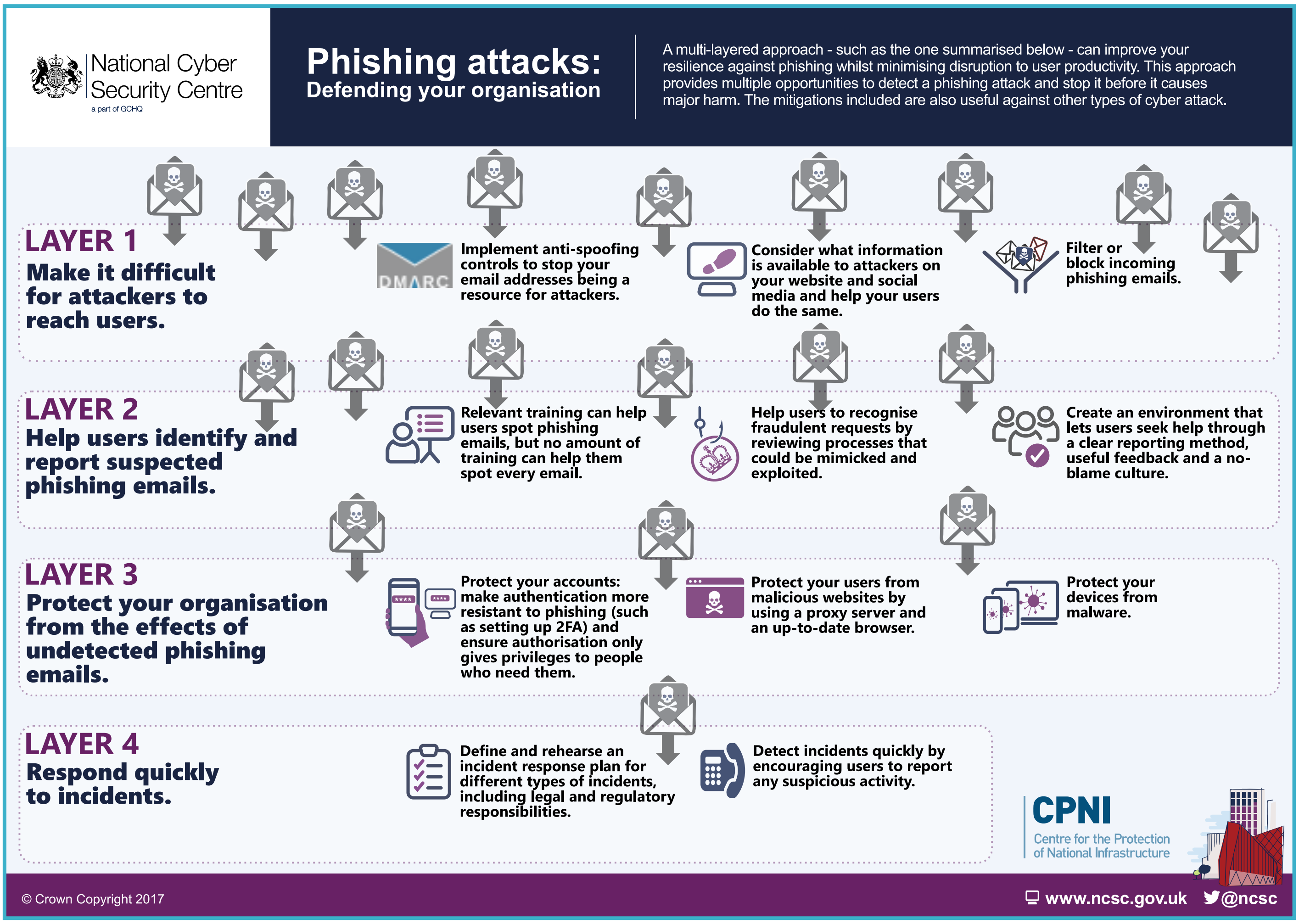
Fraudulent emails sent to staff or staff directed to fraudulent websites

People impersonating your school emails

- 30 percent of schools have been a victim of a malware infection, including virus or ransomware.
- 69 percent of schools had suffered phishing attacks.
- 20 percent of schools had suffered spoofing attacks.

Phishing and spoof emails can hit an organisation of any size and type. This kind of email attack may have various ultimate aims, for example gathering credentials (usernames and passwords), diverting payments or downloading malware, so a range of both technical and process controls should be in place to create a layered defence.

The NCSC Small Business Guide offers helpful advice on phishing which is equally relevant for schools, such as the guidance in the infographic below:



National Cyber Security Centre
a part of GCHQ

Phishing attacks:
Defending your organisation

A multi-layered approach - such as the one summarised below - can improve your resilience against phishing whilst minimising disruption to user productivity. This approach provides multiple opportunities to detect a phishing attack and stop it before it causes major harm. The mitigations included are also useful against other types of cyber attack.

LAYER 1
Make it difficult for attackers to reach users.

- Implement anti-spoofing controls to stop your email addresses being a resource for attackers.
- Consider what information is available to attackers on your website and social media and help your users do the same.
- Filter or block incoming phishing emails.

LAYER 2
Help users identify and report suspected phishing emails.

- Relevant training can help users spot phishing emails, but no amount of training can help them spot every email.
- Help users to recognise fraudulent requests by reviewing processes that could be mimicked and exploited.
- Create an environment that lets users seek help through a clear reporting method, useful feedback and a no-blame culture.

LAYER 3
Protect your organisation from the effects of undetected phishing emails.

- Protect your accounts: make authentication more resistant to phishing (such as setting up 2FA) and ensure authorisation only gives privileges to people who need them.
- Protect your users from malicious websites by using a proxy server and an up-to-date browser.
- Protect your devices from malware.

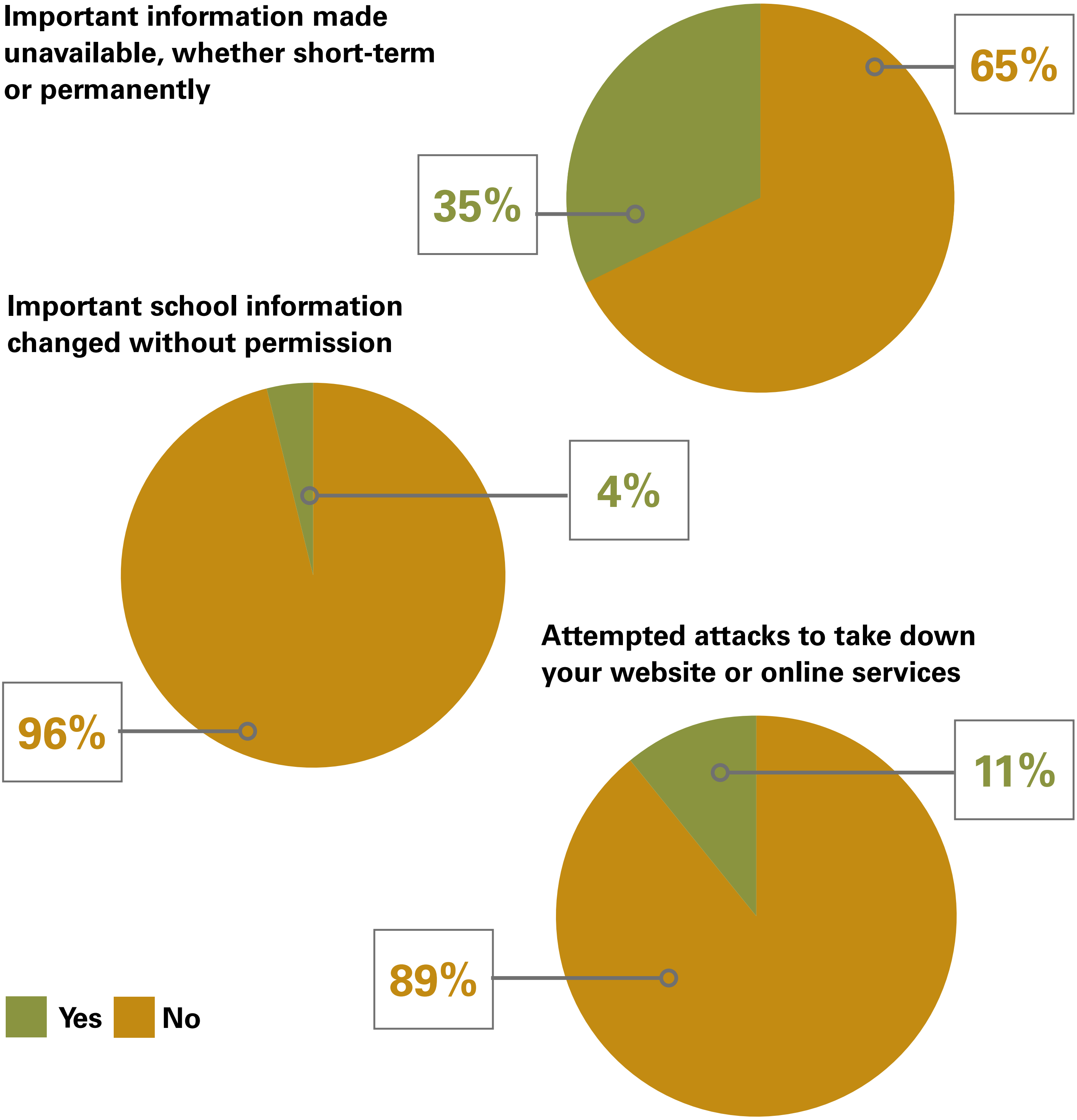
LAYER 4
Respond quickly to incidents.

- Define and rehearse an incident response plan for different types of incidents, including legal and regulatory responsibilities.
- Detect incidents quickly by encouraging users to report any suspicious activity.

CPNI
Centre for the Protection of National Infrastructure

www.ncsc.gov.uk @ncsc

[1] https://www.ncsc.gov.uk/collection/small-business-guide



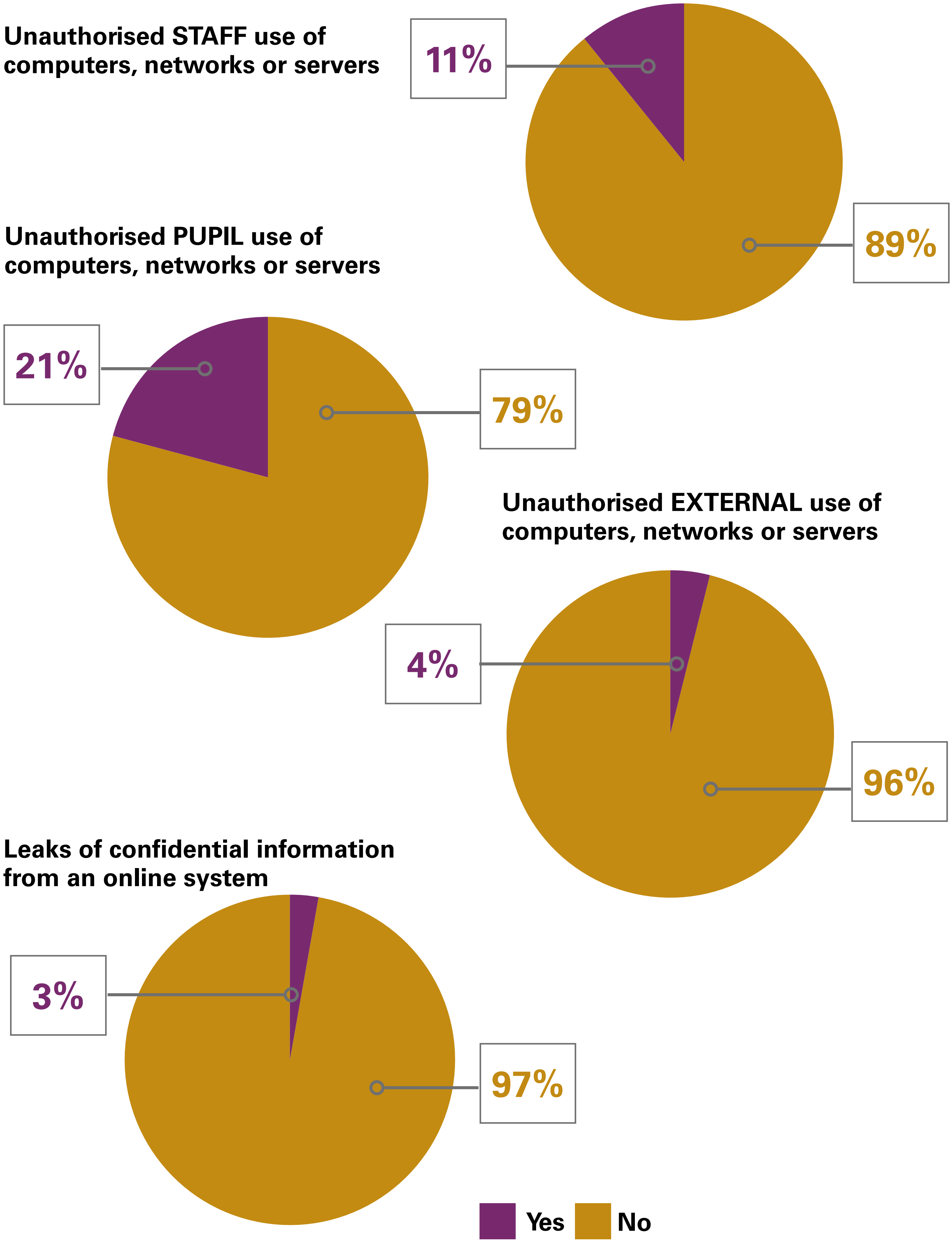
Important information made unavailable, whether short-term or permanently

Important school information changed without permission

Attempted attacks to take down your website or online services

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

Nonetheless, 4 percent of schools had experienced school information being changed without permission, 11 percent were aware of attacks on their website and 35 percent had experienced periods with no access to important information – this could have serious ramifications for a school



Unauthorised STAFF use of computers, networks or servers

Unauthorised PUPIL use of computers, networks or servers

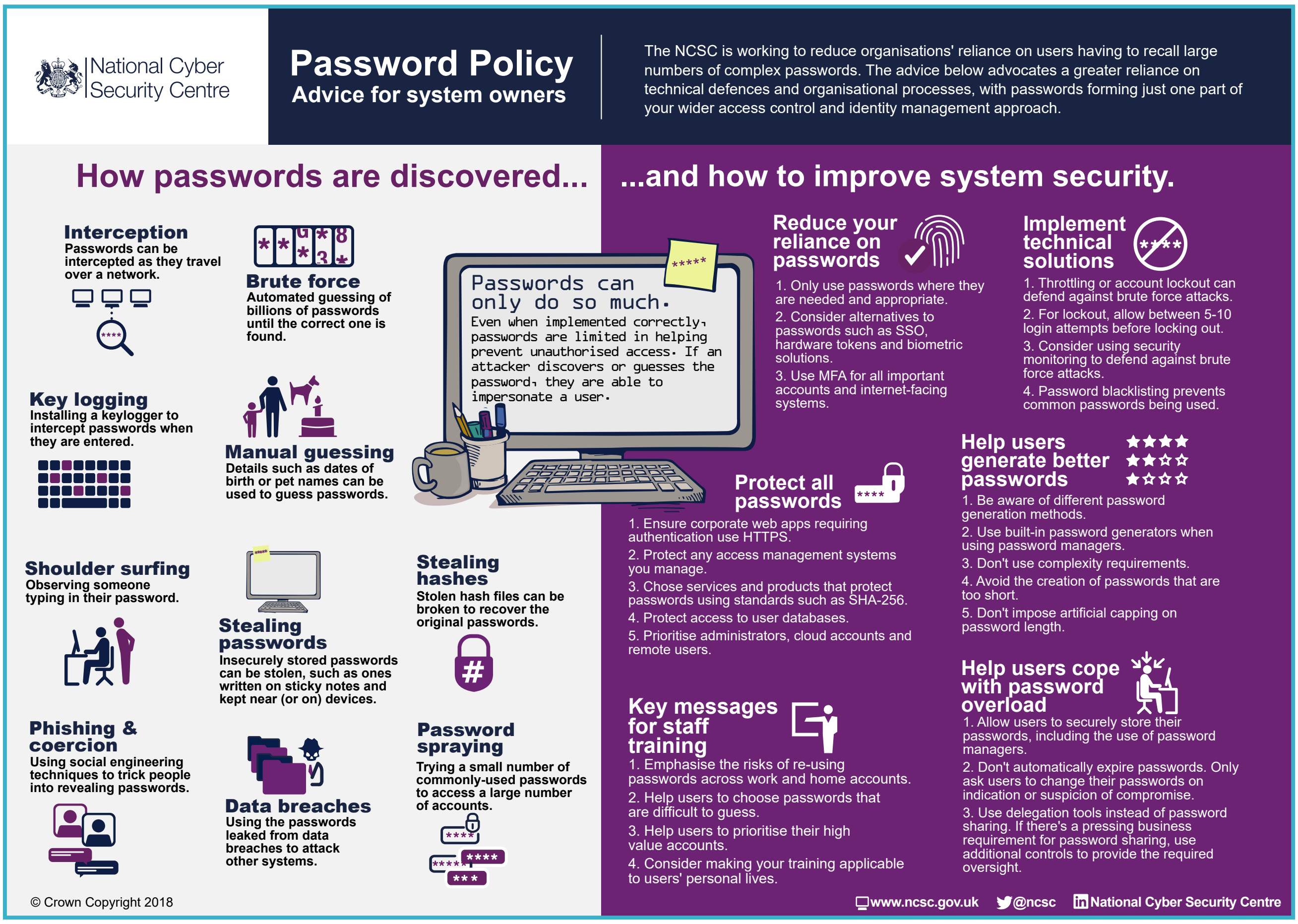
Unauthorised EXTERNAL use of computers, networks or servers

Leaks of confidential information from an online system

Since GDPR came into force in May 2018, schools have had new requirements placed upon them regarding data access and protection.

Nonetheless, 21 percent of schools had experienced non-authorised IT system use by pupils.

Schools were aware of data breaches in



National Cyber Security Centre

Password Policy

Advice for system owners

The NCSC is working to reduce organisations' reliance on users having to recall large numbers of complex passwords. The advice below advocates a greater reliance on technical defences and organisational processes, with passwords forming just one part of your wider access control and identity management approach.

How passwords are discovered...

Interception
Passwords can be intercepted as they travel over a network.

Brute force
Automated guessing of billions of passwords until the correct one is found.

Key logging
Installing a keylogger to intercept passwords when they are entered.

Manual guessing
Details such as dates of birth or pet names can be used to guess passwords.

Passwords can only do so much.
Even when implemented correctly, passwords are limited in helping prevent unauthorised access. If an attacker discovers or guesses the password, they are able to impersonate a user.

Shoulder surfing
Observing someone typing in their password.

Stealing passwords
Insecurely stored passwords can be stolen, such as ones written on sticky notes and kept near (or on) devices.

Stealing hashes
Stolen hash files can be broken to recover the original passwords.

Phishing & coercion
Using social engineering techniques to trick people into revealing passwords.

Data breaches
Using the passwords leaked from data breaches to attack other systems.

Password spraying
Trying a small number of commonly-used passwords to access a large number of accounts.

© Crown Copyright 2018

...and how to improve system security.

Reduce your reliance on passwords
1. Only use passwords where they are needed and appropriate.
2. Consider alternatives to passwords such as SSO, hardware tokens and biometric solutions.
3. Use MFA for all important accounts and internet-facing systems.

Implement technical solutions
1. Throttling or account lockout can defend against brute force attacks.
2. For lockout, allow between 5-10 login attempts before locking out.
3. Consider using security monitoring to defend against brute force attacks.
4. Password blacklisting prevents common passwords being used.

Protect all passwords
1. Ensure corporate web apps requiring authentication use HTTPS.
2. Protect any access management systems you manage.
3. Chose services and products that protect passwords using standards such as SHA-256.
4. Protect access to user databases.
5. Prioritise administrators, cloud accounts and remote users.

Help users generate better passwords
1. Be aware of different password generation methods.
2. Use built-in password generators when using password managers.
3. Don't use complexity requirements.
4. Avoid the creation of passwords that are too short.
5. Don't impose artificial capping on password length.

Key messages for staff training
1. Emphasise the risks of re-using passwords across work and home accounts.
2. Help users to choose passwords that are difficult to guess.
3. Help users to prioritise their high value accounts.
4. Consider making your training applicable to users' personal lives.

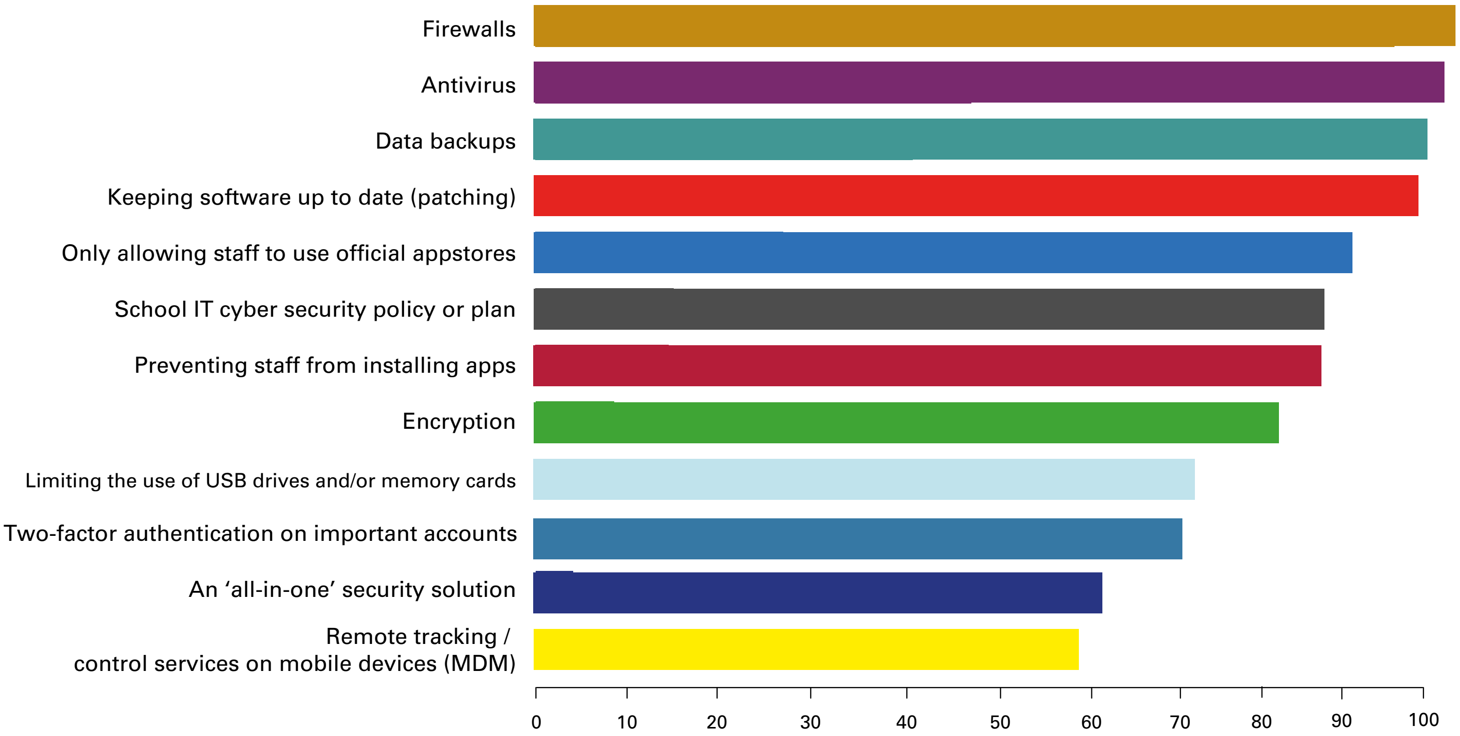
Help users cope with password overload
1. Allow users to securely store their passwords, including the use of password managers.
2. Don't automatically expire passwords. Only ask users to change their passwords on indication or suspicion of compromise.
3. Use delegation tools instead of password sharing. If there's a pressing business requirement for password sharing, use additional controls to provide the required oversight.

www.ncsc.gov.uk @ncsc National Cyber Security Centre

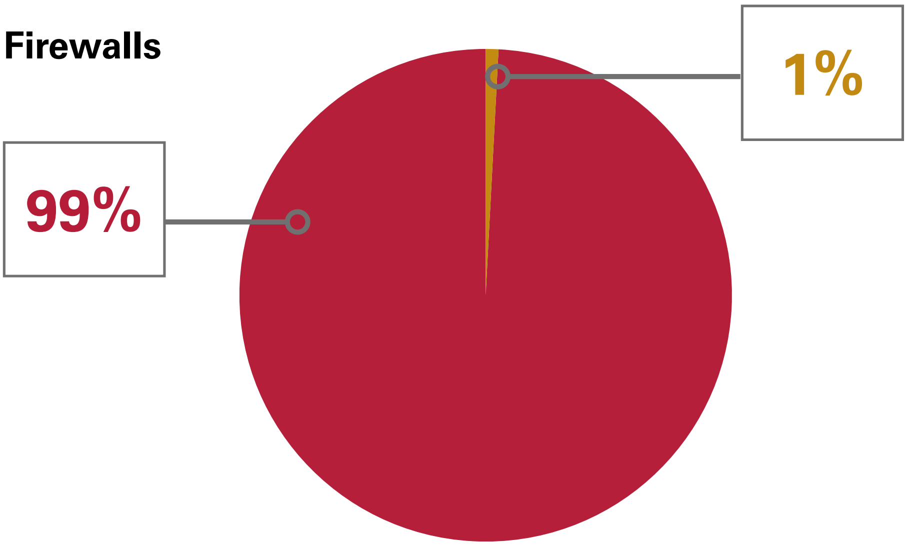
Following guidance such as the strategies published by the NCSC for password administration can help to avoid unauthorised access in the first place. This includes implementing technical defences as well as helping staff and students to choose sensible passwords and manage them effectively.

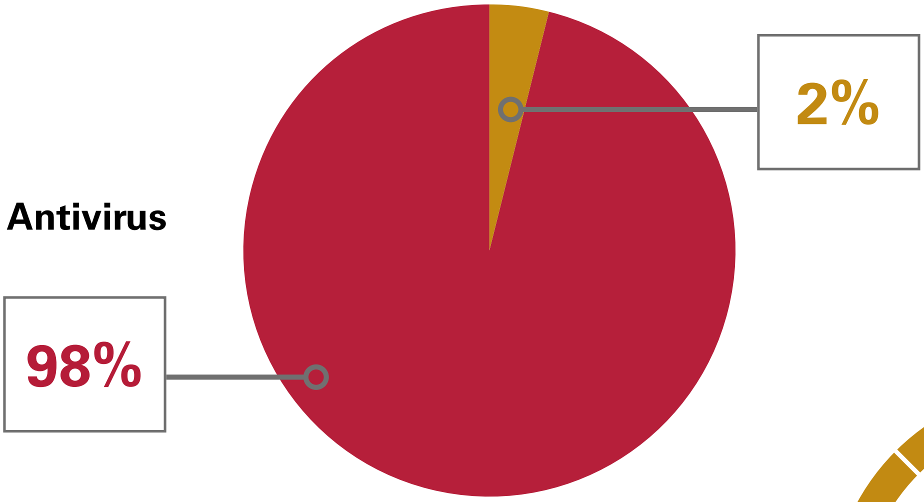
CYBERPREPARED?

Do you have the following measures in place in your school? (% of 432 schools answering yes)

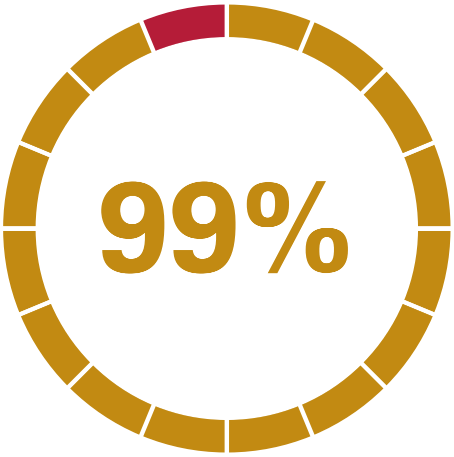


BREAKDOWN OF PROTECTIONS



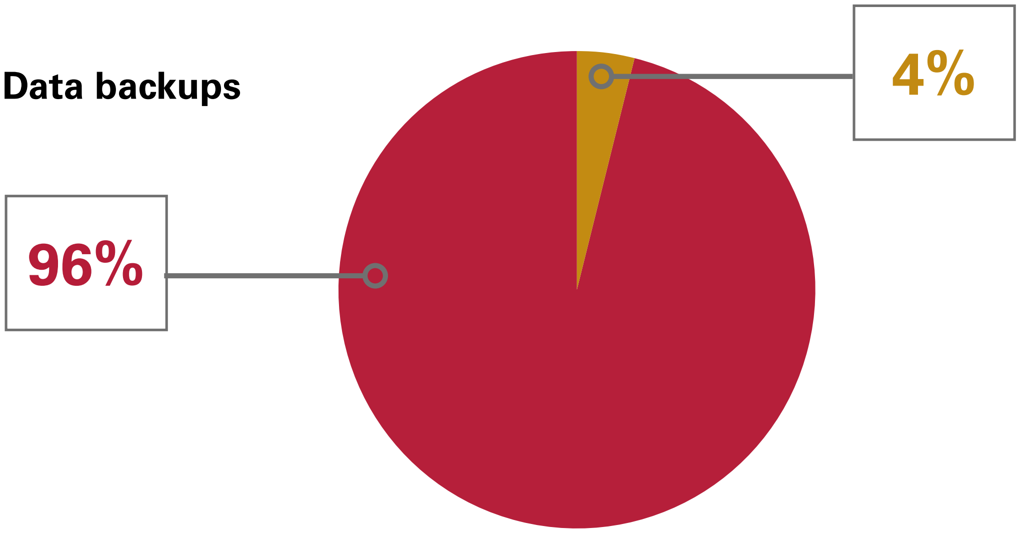


🟥 Yes 🟨 No

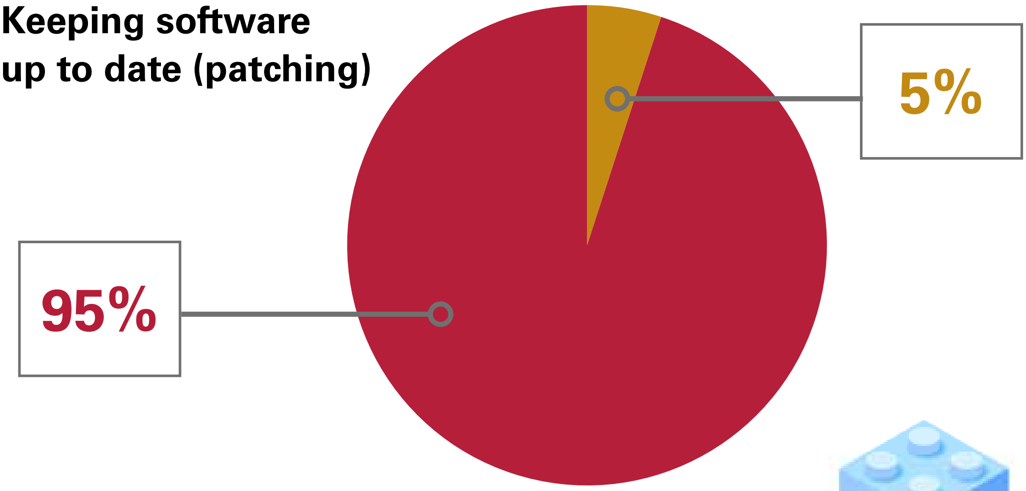


of schools know
they have a firewall.

Data backups

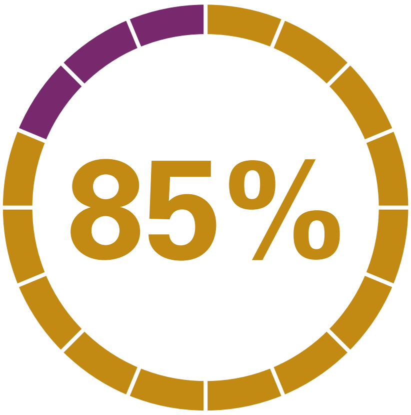


Keeping software up to date (patching)

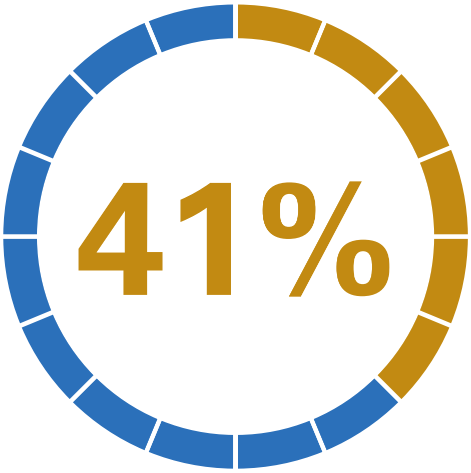


Antivirus, backups and patching followed firewalls as the next three most popular attack-prevention technical measures in place. Each were present in over 95 percent of all schools, which is a reassuring sign of fundamental protections in place in UK schools.

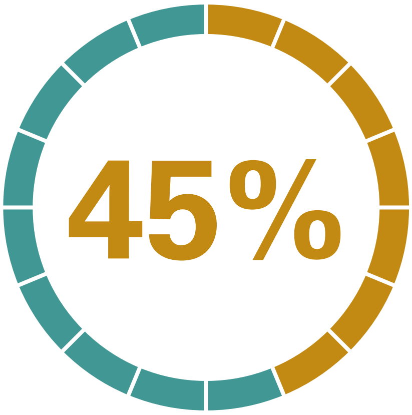
🟥 Yes 🟨 No



of schools had a cyber security policy or plan



of schools had a business continuity plan

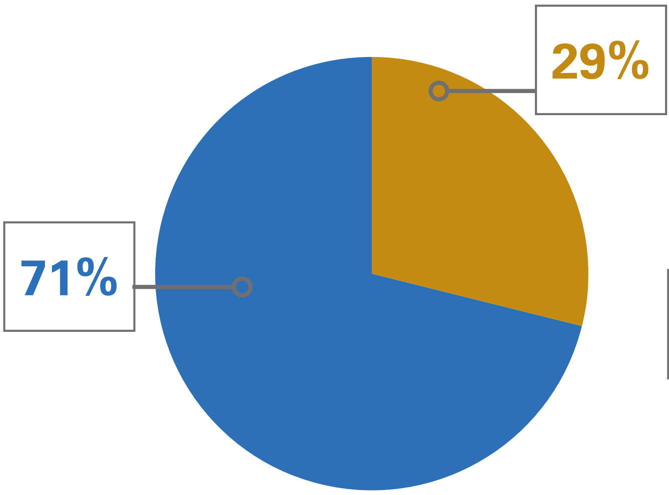


of schools had IT services in a risk register

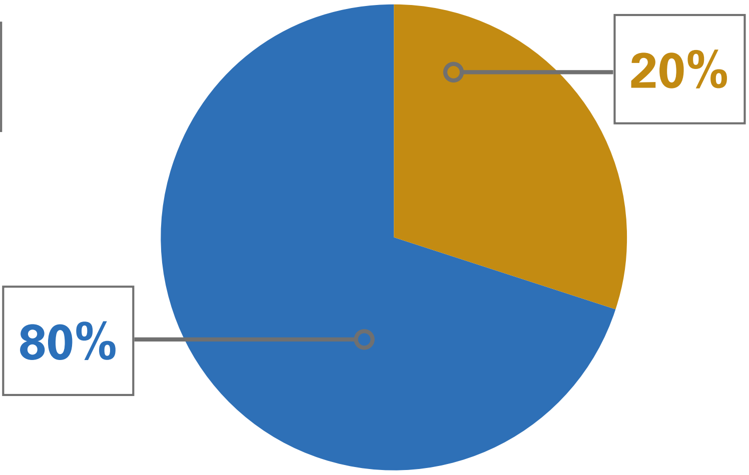
Schools in England were between 2 and 3 times more likely to have a business continuity plan or IT service risk register than a school in Scotland.

These three documents are generally interdependent and cross-reference each other to ensure joined-up planning, policy and practice, yet 20 percent of all schools surveyed had a cyber security plan but did not know if they had a business continuity plan or risk register of core IT services.

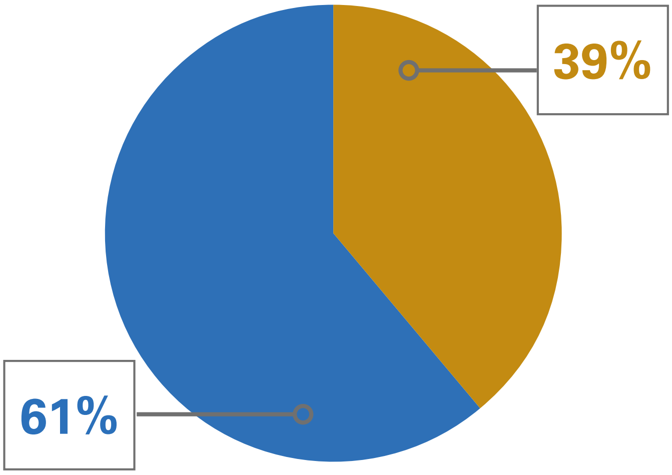
Limiting the use of USB drives and/or memory cards



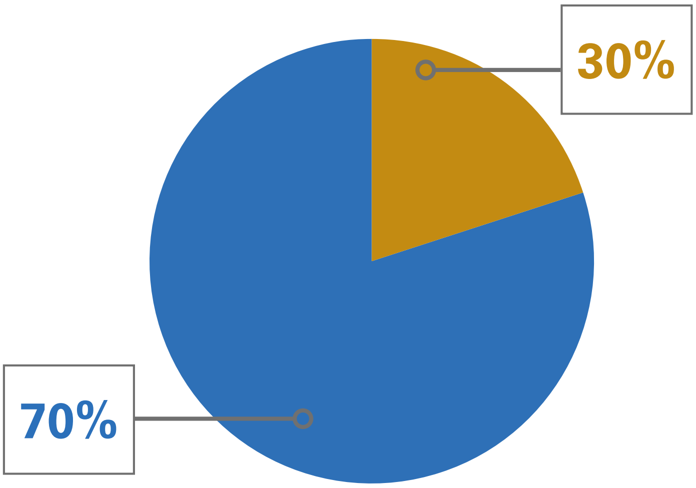
Encryption



An ‘all-in-one’ security solution



Two factor authentication on important accounts



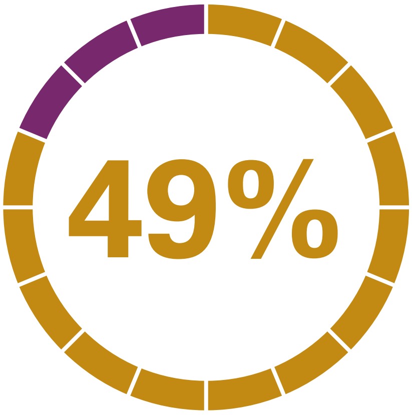
🟦 Yes 🟧 No

7 in 10 schools limit the use of USB drives and memory cards.
8 in 10 schools encrypt their data.
7 in 10 schools use two-factor authentication on important accounts.

Multiple security vendors offer one-stop-shop products designed to cover all security needs;
3 in 5 schools current use one.

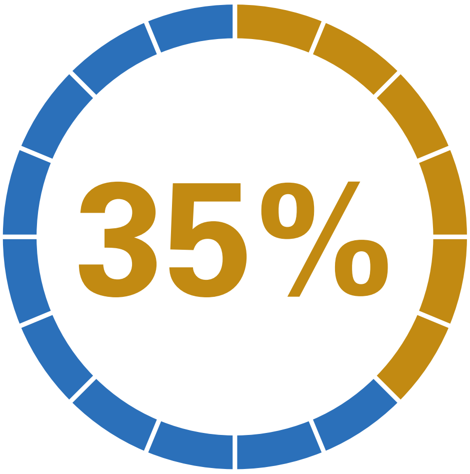
TRAINING

Less than half of schools



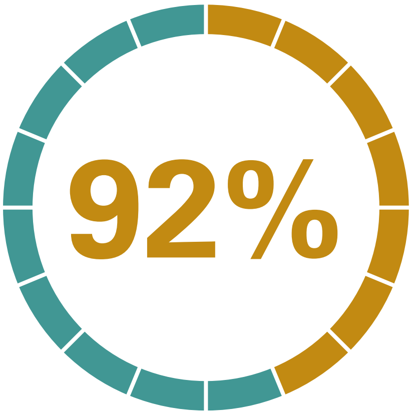
felt adequately prepared for a cyber-attack or incident

Although social engineering plays a role in many incidents, only



of non-IT staff in schools have received cyber security training

Schools are open to help in this area



would welcome more cyber security awareness training for staff

National Cyber Security Centre
a part of GCHQ

www.ncsc.gov.uk

LGfL

www.lgfl.net

find this report online at securityaudit.lgfl.net