Department for Digital, Culture, Media & Sport

Ipsos MORI

Cyber Security Breaches Survey 2021

Education institutions findings annex

This annex includes findings from the samples of UK education institutions included in this year's Cyber Security Breaches Survey. The results primarily cover:

- primary schools
- secondary schools
- further education colleges.

The appendix at the back includes indicative findings from a smaller sample of universities.

The annex supplements a main Statistical Release and infographic summaries published by the Department for Digital, Culture, Media and Sport (DCMS), covering the 2021 results for businesses and charities.

There is another Technical Annex, available on the same GOV.UK page, that provides the methodological details of the study and copies of the main survey instruments to aid interpretation of the findings.

The Cyber Security Breaches Survey is a quantitative and qualitative study of UK businesses, charities and education institutions. It helps these organisations to understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports the government to shape future policy in this area.

For this latest release, the quantitative survey was carried out in winter 2020/21.

Responsible analyst:

Emma Johns
07990602870

Statistical enquiries:

evidence@dcms.gov.uk
@DCMSinsight

General enquiries:

enquiries@dcms.gov.uk

Media enquiries:

020 7211 2210

Contents

Chapter 1: Overview of the data

1.1 Summary of methodology

Schools and colleges

The survey of education institutions comprised a random probability telephone survey, carried out from 12 October 2020 to 22 January 2021. It included:

- 135 primary schools
- 158 secondary schools
- 57 further education colleges.

The school samples include a random selection of free schools, academies, Local Authority-maintained schools and special schools.

The samples were selected from the following sources:

- All institutions in England: Get Information About Schools
- Schools in Scotland: Scottish Government School Contact details
- FE Colleges in Scotland: Colleges Scotland directory
- Schools in Wales: Welsh Government Address list of schools
- FE Colleges in Wales: Colleges Wales directory
- Schools in Northern Ireland: NI Department of Education database
- FE Colleges in Northern Ireland: NI Direct FE College directory.

Higher education institutions

We also surveyed 28 UK universities. As this sample is too small to be statistically reliable, we have opted to exclude these results from the main body of this report. Instead, the raw survey data are included at the end in an appendix.

In addition, we carried out seven qualitative interviews with universities, recruited from the survey. These interview findings have been incorporated into the main Statistical Release. In this annex, we also include the key findings that were more specific to universities in the appendix, as well as a selection of quotes from these interviews to illustrate the themes raised.

For the higher education institutions, we built a bespoke sample, by supplementing the universities already included in the Get Information About Schools database with universities outside England taken from other online lists, e.g. the Universities UK website, cross-referenced against the comprehensive list of Recognised Bodies on GOV.UK (which also includes, for example, degree-awarding arts institutes).

1.2 A note on representativeness

The education institution samples are all unweighted. They were surveyed as simple random samples, with no stratification. As such, they should be considered as representative samples. As the sample sizes are relatively small compared to the business and charity survey samples, the margins of error are higher:

- ±5-8 percentage points for primary schools
- ±5-8 percentage points for secondary schools
- ±7-12 percentage points for further education colleges.

As noted above, the universities sample is not statistically reliable, and we cannot put a margin of error around the universities data. However, as the population of higher education institutions in the UK is very small (175 universities or other types of higher education institution), the

results from a sample of this size can still provide a good *indication* of where universities stand in terms of their cyber security measures relative to other organisations.

1.3 Comparability to the main results for businesses and charities

In this report, we have primarily compared our three largest education institution samples against each other, and against the benchmark set by UK businesses. The report is intended to give a broad view of where schools and colleges lie in relation to businesses when it comes to cyber security.

1.4 Comparability to the Cyber Security Breaches Survey 2020

A smaller sample of primary schools (108) and secondary schools (72) were included in the 2020 survey, which was carried out in a methodologically consistent way. This means we can compare findings across years and comment on the direction of travel. However, given the large margins of error, we do not expect to find statistically significant differences across years. The changes from 2020 to 2021 should not be considered definitive, until we have accumulated further data over the coming years.

We also surveyed further education colleges in the 2020 survey, but the achieved sample was very small – we merged them with higher education institutions in last year's report – so this year's further education results can be considered a new baseline.

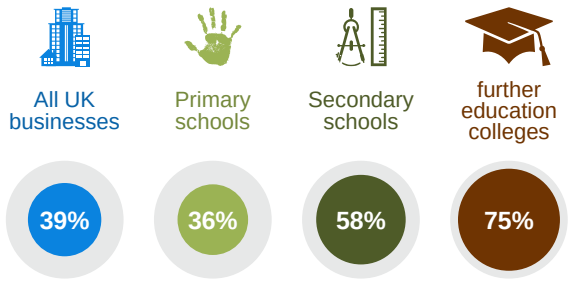
Chapter 2: Key findings

2.1 Incidence and impact of cyber security breaches or attacks

It is important to remember that the survey can only measure the breaches or attacks that organisations have themselves identified. There are likely to be hidden attacks, and others that go unidentified, so the findings reported here may underestimate the full extent of the problem.

As Figure 2.1 shows, primary schools are relatively close to the typical business in terms of how many identify breaches. Secondary schools and further education colleges are much more likely to identify breaches, and are closer to large businesses in this regard (64% of large businesses identify breaches, as covered in the main Statistical Release).

Figure 2.1: Percentage of organisations that have identified breaches or attacks in the last 12 months



Bases: 1,419 UK businesses; 135 primary schools; 158 secondary schools; 57 further education colleges

The proportion of businesses identifying breaches or attacks fell this year (from 46% in the 2020 survey to 39% now). Primary and secondary schools show a similar downward movement this year (from 41% and 76% respectively in 2020). In the main Statistical Release, we suggest this is not necessarily a fall in the number of attacks that organisations, including schools, are facing. Instead, it could be that there has been less monitoring and reporting of breaches this year, given the moves towards remote working during the COVID-19 pandemic.

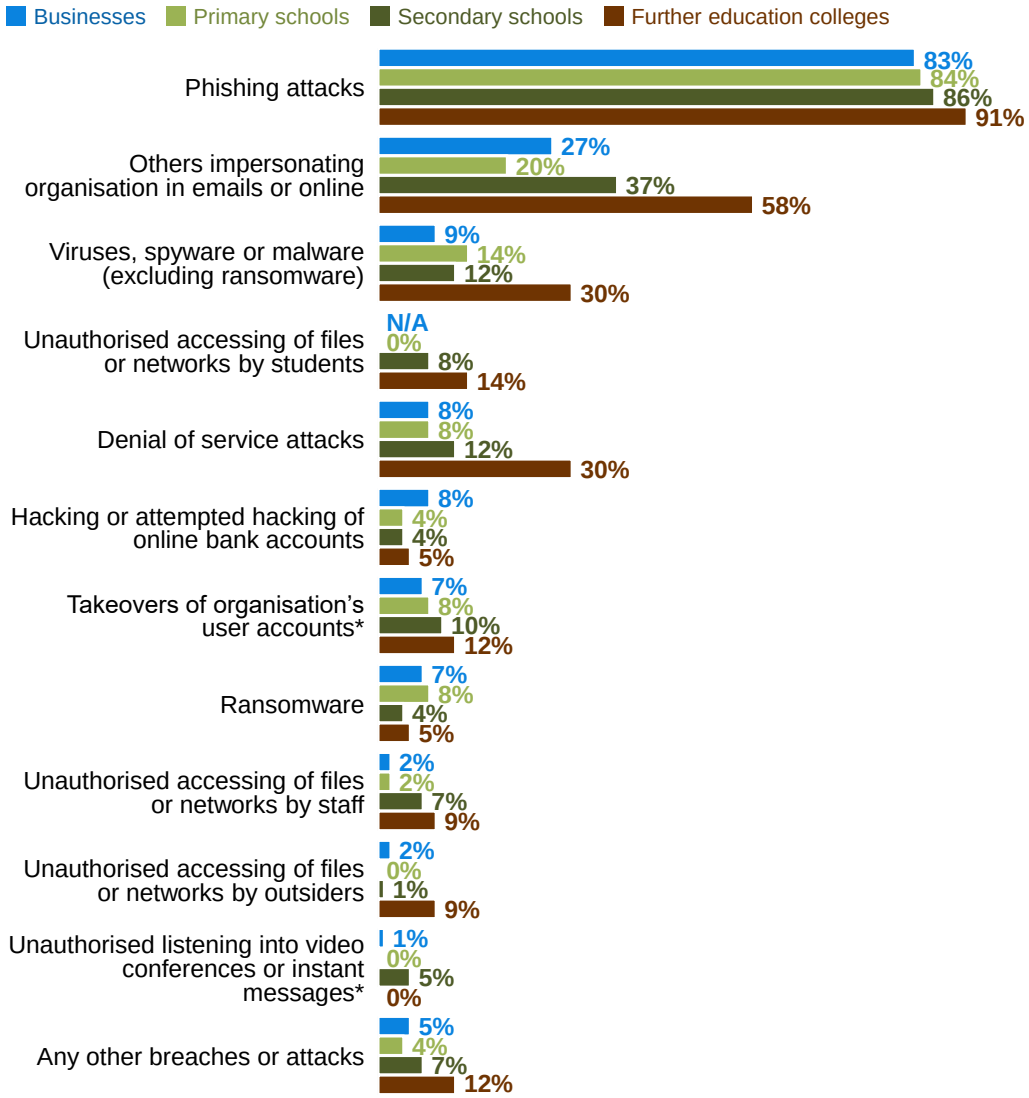
Types of breaches or attacks identified

The findings reported in the rest of Section 2.1 are based only on the institutions that have identified any breaches or attacks.

Figure 2.2 breaks down the types of breaches or attacks experienced. Schools do not necessarily stand apart from the typical business in terms of the kinds of breaches and attacks they are reporting.

On the other hand, further education colleges are more likely to have experienced a wider range of breaches, as the chart suggests. In fact, half say they have faced three or more different types of breaches or attacks in the last 12 months (vs. 13% of businesses, 16% of primary schools and 24% of secondary schools). Colleges are especially more likely to identify impersonation attacks, viruses or malware and denial of service attacks.

Figure 2.2: Percentage that have identified the following types of breaches or attacks in the last 12 months, among the education institutions that have identified any breaches or attacks



Bases: 748 businesses that identified a breach or attack in the last 12 months; 49 primary schools; 91 secondary schools; 43 further education colleges
*New codes for 2021

How are education institutions affected?

Among those that have experienced breaches or attacks in the last 12 months, colleges also appear to be more severely affected by them than schools:

- Around a quarter (26%) of further education colleges experience breaches or attacks at least once a week, which is similar to the average business (27%). This is lower for primary schools (6%) and secondary schools (15%).
- A third (33%) of further education colleges had a material outcome from these breaches, such as a loss of control, data or money. This is similar for secondary schools (33%) but lower for primary schools (24%). The latter are more in line with the UK business population (21%). An especially common outcome for colleges is around user accounts being compromised (in 21% of the colleges that have been breached).
- Three-quarters of further education colleges (74%) have been negatively impacted regardless of whether there was a material outcome or not. Most commonly, they report of

requiring new measures following the breach (58%), staff resources being diverted to deal with the breach (56%) and wider staff being prevented from carrying out their work activities because of the breach (26%). Four in ten primary schools (41%) and half of secondary schools (48%) report negative impacts, compared to a third of businesses (35%). Primary schools (33%) and secondary schools (40%) are also more likely than businesses (19%) to say staff resource had to be diverted to deal with the breach.

2.2 Senior management engagement with cyber security

The education institutions in our sample typically report a higher level of senior engagement with cyber security than the average UK business. In this sense, they are more like large businesses, which was also the case for schools last year.

- Over nine in ten say that cyber security is a high priority for their governors or senior management (98% of primary schools, 94% of secondary schools and 95% of colleges). This is more in line with large businesses (93%) than with the average UK business (77%).
- More than half update their governors or senior management on cyber security at least quarterly (57% of primary schools, 54% of secondary schools and 79% of colleges, vs. 50% of businesses).
- Around two-thirds of schools have a governor or senior manager with responsibility for cyber security (68% of primary schools and 66% of secondary schools, vs. 38% of businesses). Three-quarters of further education colleges similarly assign such responsibility at a senior level (77%).

2.3 Sources of information and guidance

Seeking information

Schools and colleges are more likely than the typical business to have sought information or guidance about cyber security from external sources in the last 12 months. Two-thirds of primary and secondary schools have done so (66% in each case) and nine in ten further education colleges have done so (88%).

The most common sources of information and guidance are:

- their external cyber security or IT providers (for 27% of primary schools, 23% of secondary schools and 42% of colleges)
- government and public sector sources (for 35% of primary schools, 32% of secondary schools and 28% of colleges).

There are also differences between schools and colleges. Schools are more likely to have reached out to local authorities (24% of primary schools and 11% of secondary schools). Four in ten colleges (39%) mention Jisc and the Janet Network, which provides UK universities and colleges with shared digital infrastructure and services.

For schools, the pattern of findings here is very similar to the 2020 survey.

Awareness of government guidance, initiatives and communications

There are still many education institutions, particularly primary schools, that have not heard of the various government guidance, initiatives and communications campaigns on cyber security. Awareness is much more widespread in further education colleges, where typically half or more are aware of the various communications covered in the survey:

- Around a third of primary schools (31%) and secondary schools (35%) have heard of the government's Cyber Aware communications campaign. Awareness is higher among further education colleges (56%).
- Just seven per cent of primary schools are aware of the Cyber Essentials scheme, rising to 30 per cent of secondary schools.[1] By contrast, almost nine in ten colleges report being aware (84%).
- While half (51%) of colleges have heard of the 10 Steps to Cyber Security, awareness of this guidance is lower among primary schools (29%) and secondary schools (39%).[2]
- The National Cyber Security Centre's (NCSC's) Board Toolkit is much more widely recognised in colleges (41%) than in primary schools (12%) or secondary schools (17%). However, it is worth noting that the Board Toolkit, which is aimed at senior managers and governing bodies, has not been specifically promoted across education institutions.
- This year, for the first time, we also asked about awareness of National Cyber Security Centre guidance on home working and video conferencing services, which was first published in 2020 in response to the COVID-19 pandemic and ensuing UK lockdown. All three education institutions show more awareness of this guidance than the typical business (21% of which are aware), but it is still much lower for primary schools (43%) than for secondary schools (63%) and colleges (74%).

2.4 Identifying cyber security risks

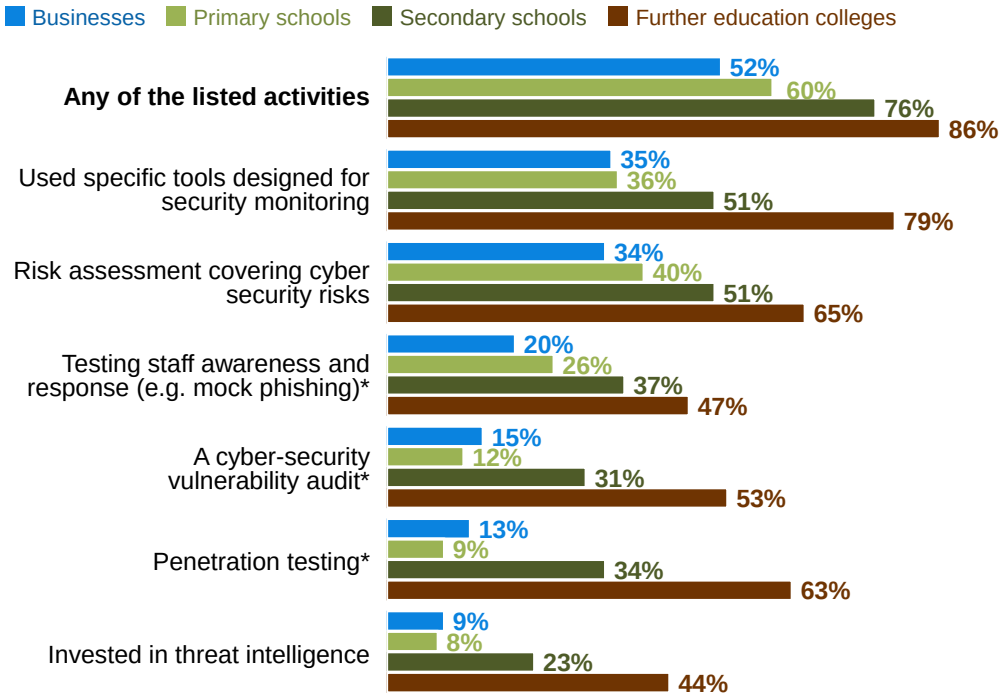
The majority of the education institutions have taken at least one of the actions shown in Figure 2.3 in the last 12 months, to help identify cyber security risks. Again, primary schools tend to be closer to the typical business (and, as such, more akin to micro businesses), whereas secondary schools and further education colleges tend to have more sophisticated approaches.

Colleges are specifically more likely than schools to be carrying out security monitoring, audits, penetration testing and investing in threat intelligence.

[1] The government-endorsed Cyber Essentials scheme enables organisations, including education institutions, to be certified independently for having met a good-practice standard in cyber security.

[2] The 10 Steps to Cyber Security guidance aims to summarise what organisations should do to protect themselves.

Figure 2.3: Percentage of education institutions that have carried out the following activities to identify cyber security risks in the last 12 months



Bases: 1,419 UK businesses; 135 primary schools; 158 secondary schools; 57 further education colleges
*New codes for 2021

All types of education institutions are also more likely than businesses to say they have reviewed supplier-related risks to cyber security, although this still appears to be an uncommon activity for schools.

- Around a fifth of primary schools (19%) and a quarter of secondary schools (24%) say they have reviewed such risks posed by their immediate suppliers or partners, versus four in ten further education colleges (40%). This compares to 12 per cent of businesses.
- Across the board, under two in ten have reviewed risks presented by their wider supply chains (15% of primary schools, 15% of secondary schools and 18% of further education, compared to 5% of businesses).

2.5 Actions taken to manage or mitigate risks

Staff training and awareness raising

Cyber security training or awareness raising activities are not currently the norm in schools. A third of primary schools (34%) and four in ten secondary schools (39%) have undertaken any such activities in the last 12 months. This rises to just over half of further education colleges (56%), which is more in line with large businesses (47%).

Cyber security planning and documentation

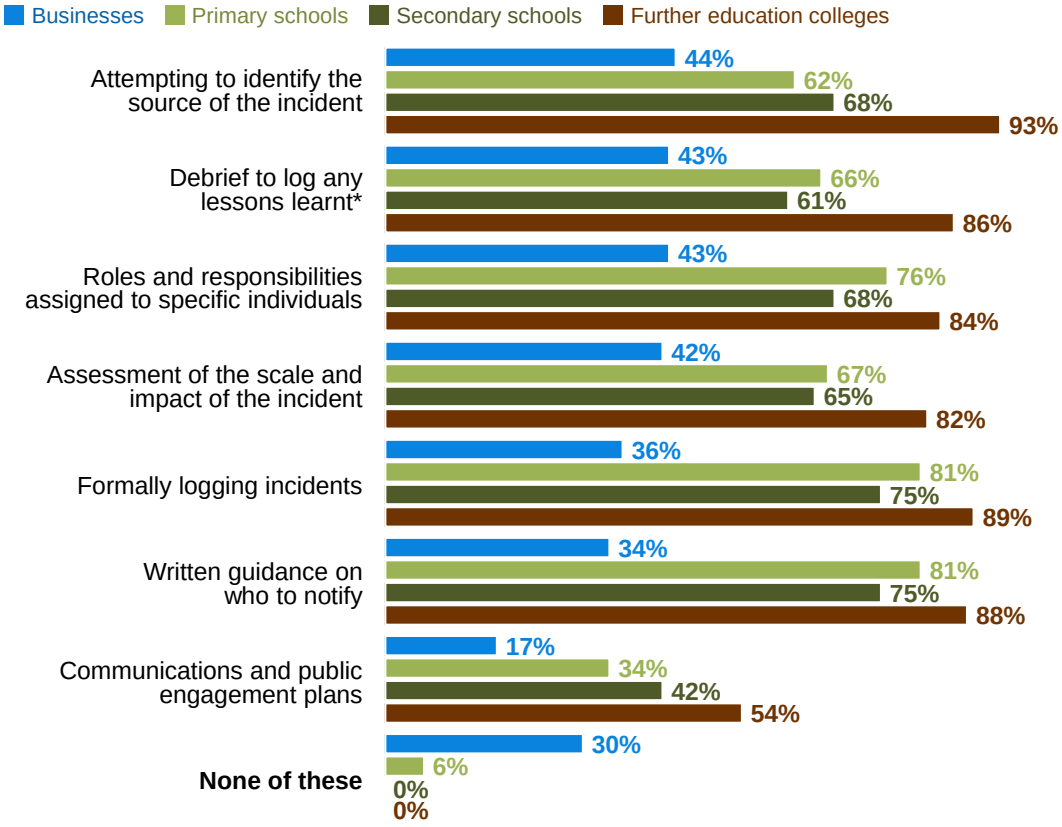
In terms of documentation, all three groups of education institutions are far more developed than the typical business, and much more akin to large businesses:

- Three-quarters of primary and secondary schools have a cyber security policy (75% in each case). Policies are much more ubiquitous in further education colleges (84%).

- Business continuity plans covering cyber security also tend to be in place in the majority of these institutions, although they are less common in primary schools (56% of primary schools, 68% of secondary schools and 86% of colleges have such plans in place).
- Incident response planning is also more sophisticated than in the average business, as Figure 2.4 indicates. Colleges are more likely to have plans that encompass each area in the chart than schools.

This year, the proportion of businesses with cyber security policies fell compared to 2020 (from 38% to 33%). The shifts in the secondary school data suggests a similar decrease – last year, over nine in ten secondary schools (92%) were recorded as having a policy.

Figure 2.4: Percentage of education institutions that take the following actions, or have these measures in place, for when they experience a cyber security incident



Bases: 1,419 UK businesses; 135 primary schools; 158 secondary schools; 57 further education colleges
*New code for 2021

Insurance against cyber security breaches

Around half of further education colleges (49%) report being insured against cyber risks, with a smaller proportion of primary schools (36%) and secondary school (27%) reporting this.

It is worth noting that around half of the individuals in cyber roles that we interviewed in primary and secondary schools did not know whether their school had this kind of insurance (56% and 58% respectively) and neither did four in ten of the interviewees from colleges (40%).[3] This

[3] Our interviewers sought to interview the senior person with most responsibility for cyber security within an organisation, who might be expected to know if the organisation was insured against cyber security breaches or attacks. This individual was identified by the organisation for us.

compares to just 18 per cent of business interviewees not knowing. It highlights that cyber security is perhaps more siloed in education institutions, and therefore considered separately from financial matters like insurance.

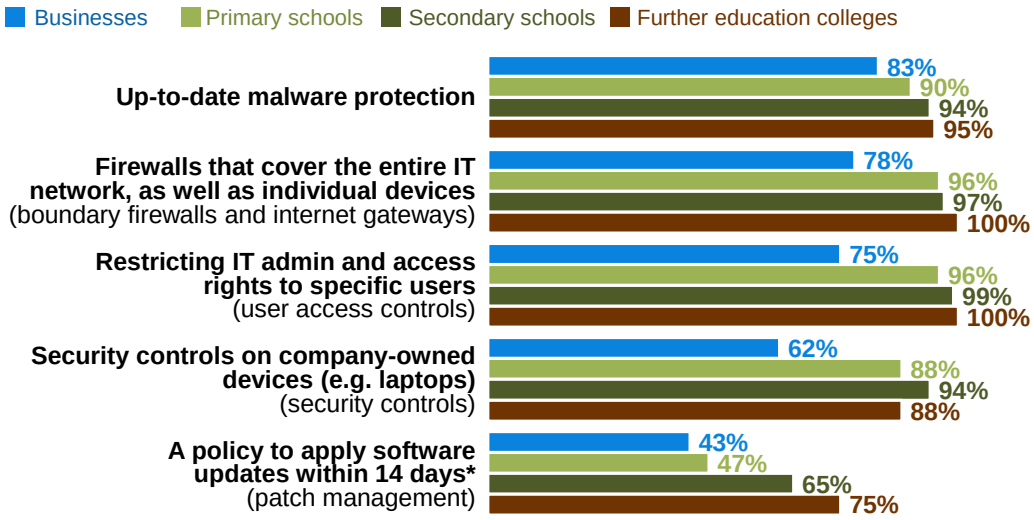
For schools, these results are very similar to last year.

Technical rules and controls

The survey covers a range of technical rules and controls that organisations may have in place to help minimise the risk of cyber security breaches (split out in Figures 2.5 and 2.6). Many of these are basic good practice controls taken from government guidance for the 10 Steps to Cyber Security or the Cyber Essentials scheme.

Overwhelmingly, education institutions have technical rules or controls covering the four of the five technical areas laid out in the Cyber Essentials guidance: boundary firewalls and internet gateways, secure configurations, user access controls and malware protection. Primary schools are notably weaker in the fifth area – patch management – with just half (47%) having a policy to apply software updates within 14 days.

Figure 2.5: Percentage of education institutions that have the rules or controls in place in the five technical areas from Cyber Essentials



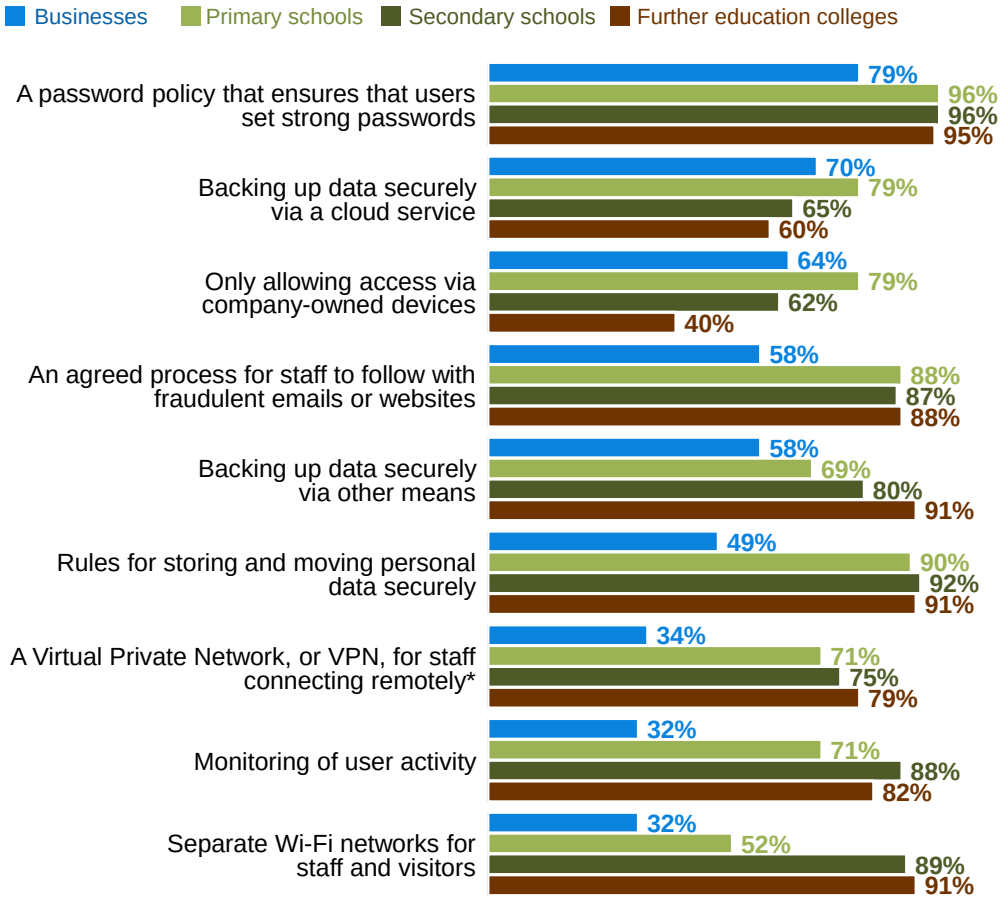
Bases: 1,419 UK businesses; 135 primary schools; 158 secondary schools; 57 further education colleges
Bold wording used in questionnaire
*New code for 2021

This year, we also included a new question on the presence of Virtual Private Networks (VPNs). These have become increasingly important during the COVID-19 pandemic, as more schools and colleges are forced to teach remotely. The survey shows that around seven to eight in ten institutions report having a VPN in place.

Primary schools are less likely than other education institutions to have guest Wi-Fi networks. Related to this, primary schools are more likely than the other institutions to only allow access via their own devices. This may reflect the nature of their activities – dealing with young children who would not typically be allowed their own internet access at school.

It is also notable that cloud back-ups are much more common in primary schools, while other education institutions are more likely to use other means for secure back-ups.

Figure 2.6: Percentage of education institutions that have additional rules or controls in place



Bases: 1,419 UK businesses; 135 primary schools; 158 secondary schools; 57 further education colleges
New code for 2021

These findings, where questions are consistent across years, are similar to the 2020 survey.

Outsourcing cyber security

Our sample suggests that outsourcing cyber security is more common among primary schools than other education institutions. A total of 73 per cent of primary schools say an external provider manages their cyber security for them, compared with 44 per cent of secondary schools and 35 per cent of further education colleges. This pattern is similar to the 2020 survey.

2.6 Implementing the 10 Steps to Cyber Security

The government's 10 Steps to Cyber Security guidance sets out a comprehensive risk management regime that both businesses and charities can follow to improve their cyber security standards. It is not, however, an expectation that organisations comprehensively apply all the 10 Steps – this will depend on each organisation's cyber risk profile.

These steps have been mapped to several specific questions in the survey. This is not a perfect mapping – many of the steps are overlapping and require organisations to undertake action in the same areas – but it gives an indication of whether organisations have taken relevant actions on each step.

Table 2.1 brings together these findings, some of which have been individually covered earlier in this annex.

Table 2.1: Percentage of education institutions undertaking action in each of the 10 Steps areas

	Step description – *and how derived from the survey*	Businesses	Primary	Secondary	Further
1	Information risk management regime – *have formal cyber security policies and the board are kept updated on actions taken*	30%	68%	69%	81%
2	Secure configuration – *organisation has a policy to apply software updates within 14 days (definition changed in 2021)*	43%	47%	65%	75%
3	Network security – *network firewalls*	78%	96%	97%	100%
4	Managing user privileges – *restricting IT admin and access rights to specific users*	75%	96%	98%	100%
5	User education and awareness – *have formal policy covering what staff are permitted to do on the organisation's IT devices and carry out cyber security training for staff (definition changed in 2021)*	9%	27%	34%	49%
6	Incident management	64%	94%	88%	97%
7	Malware protection – *up-to-date malware protection*	83%	90%	94%	95%
8	Monitoring – *monitoring user activity or using security monitoring tools*	49%	82%	91%	91%
9	Removable media controls – *have formal policy covering what can be stored on removable devices*	21%	62%	65%	70%
10	Home and mobile working – *have formal policy covering remote or mobile working*	23%	67%	68%	77%

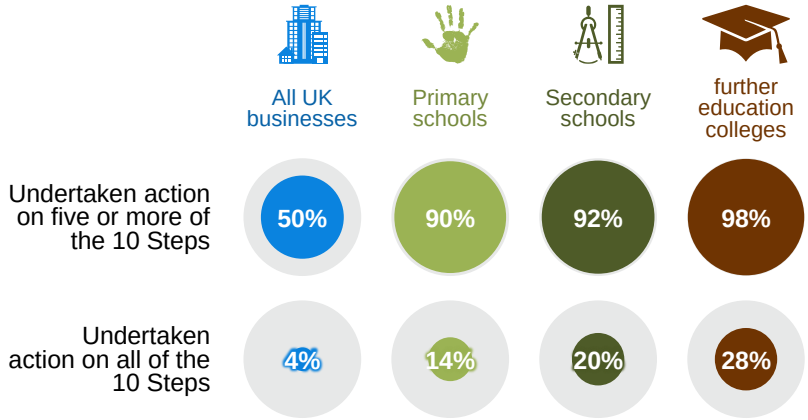
This table shows that the areas that are less well covered among schools in particular (rather than further education colleges) are to do with:

- user education and awareness
- information risk management regimes
- secure configurations
- removable media controls
- remote or mobile working policies – which has also become more important under the COVID-19 pandemic.

Looking at these 10 Steps together, virtually all education institutions have taken action on at least five of these steps, but there is still a way to go before these institutions have taken action in all 10 areas as demonstrated in Figure 2.6.

It is important to note that the scores for schools in this year's report are lower, but this is primarily because of the more stringent definition for Step 5, which now includes staff training (which is relatively uncommon across all types of organisations).

Figure 2.7: Percentage of education institutions that have undertaken action in half or all the 10 Steps guidance areas



Bases: 1,419 UK businesses; 135 primary schools; 158 secondary schools; 57 further education colleges

Appendix A: Higher education institutions findings

Quantitative survey findings

The following tables show the findings at key questions for the 28 higher education institutions that took part in the survey. Since this is a very low sample size, we show the raw number of respondents giving each answer, rather than a percentage.

The findings are not necessarily statistically representative, but they indicate that higher education institutions are probably close to large businesses in terms of their approaches to cyber security.

Where fewer than five institutions gave a specific response, we have either supressed the response or merged it with others in order to prevent the data from being disclosive.

Types of breaches or attacks identified in the last 12 months

Base – all higher education institutions	**28**
Any breaches or attacks	26
Phishing attacks	24
Others impersonating organisation in emails or online	21
Denial of service attacks	13
Viruses, spyware or malware (excluding ransomware)	11
Unauthorised accessing of files or networks by staff	10
Unauthorised accessing of files or networks by outsiders	6
Unauthorised listening into video conferences or instant messaging	6
Ransomware	5
Merged responses: • Hacking or attempted hacking of online bank accounts • Takeovers of the organisation’s user accounts, • Unauthorised accessing of files or networks by students • Any other types of cyber security breaches or attacks	19

How often higher education institutions have reported breaches or attacks in the last 12 months

Base – all identifying breaches or attacks	**26**
Merged responses: several times a day and once a day	9
Merged responses: once a week and once a month	9
Merged responses: • Less than once a month • Once only • Refused • Don’t know	8

Higher education institutions that had any of the following outcomes from breaches or attacks

Base – all identifying breaches or attacks	**26**
Any listed outcome	**17**
Temporary loss of access to files or networks	6
Compromised accounts or systems used for illicit purposes	10
Website, or online services taken down or made slower	6
Money stolen	5
Personal data altered, destroyed or taken	5
Merged responses:	10

- Lost access to relied-on third-party services
- Software or systems corrupted or damaged
- Damage to physical devices or equipment
- Permanent loss of files (not personal data)
- Lost or stolen assets, trade secrets or intellectual property
- Money was paid as a ransom

Higher education institutions that were impacted in any of the following ways from breaches or attacks

Base – all identifying breaches or attacks	**26**
Any listed impact	**21**
Additional staff time to deal with breach or inform others	18
New measures needed for future breaches or attacks	15
Stopped staff carrying out daily work	11
Complaints from customers	7
Other repair or recovery costs	5
Merged responses:	5

- Reputational damage
- Discouraged from carrying out intended future business activity
- Prevented provision of goods or services
- Loss of revenue
- Goodwill compensation to customers
- Fines or legal costs

Extent to which cyber security is seen as a high or low priority for senior managers

Base – all higher education institutions	**28**
Very high priority	16
Merged responses: • Fairly high priority – the majority of the 12 gave this response • Fairly low priority • Very low priority • Don't know	12

How often senior managers are given an update on any actions taken around cyber security

Base – all higher education institutions	**28**
Merged responses: • Each time there is a breach • Daily • Weekly • Monthly – the majority of the 14 gave this response	14
Merged responses: • Quarterly – the majority of the 13 gave this response • Annually • Less than once a year • Never • Don't know	13

Higher education institutions that have the following governance or risk management arrangements

Base – all higher education institutions	**28**
A formal policy or policies in place covering cyber security risks	26
A Business Continuity Plan that covers cyber security	25
Board members with responsibility for cyber security	24
An outsourced provider that manages cyber security (response supressed due to small number of respondents)	*

Sources of information or guidance on cyber security from the last 12 months (unprompted)

Base – all higher education institutions	**28**
Any government or public sector sources	**15**
National Cyber Security Centre (NCSC)	10
Responses supressed due to small number of respondents: • Government's Cyber Essentials materials • Government intelligence services (e.g. GCHQ) • GOV.UK	*
External cyber security or IT providers	11
Jisc and the Janet Network	10
Cyber Security Information Sharing Partnership (CISP)	5
Specialist IT blogs, forums or websites (response supressed due to small number of respondents)	*

Higher education institutions aware of the following government guidance, initiatives or communication campaigns

Base – all higher education institutions	**28**
Cyber Essentials	27
10 Steps to Cyber Security	24
NCSC guidance on secure home working and video conferencing	24
Cyber Aware	20
NCSC Board Toolkit	18

Higher education institutions that have carried out the following activities to identify cyber security risks in the last 12 months

Base – all higher education institutions	**28**
Any of the listed activities	**28**
Risk assessment covering cyber security risks	23
Carried out a cyber security vulnerability audit	22
Penetration testing	22
Used specific tools designed for security monitoring	21
Tested staff (e.g. with mock phishing exercises)	21
Invested in threat intelligence	18

Higher education institutions that have had training or awareness raising sessions on cyber security in the last 12 months

Base – all higher education institutions	**28**
Yes	23
Merged responses: • No • Don't know	5

Higher education institutions that take the following actions, or have these measures in place, for when they experience a cyber security incident

Base – all higher education institutions	**28**
Formally logging incidents	26
Written guidance on who to notify	26
Roles or responsibilities assigned to specific individuals	26
An assessment of the scale and impact of the incident	26
Attempting to identify the source of incident	25
Debriefs to log any lessons learnt	25
Communications and public engagement plans	24

Higher education institutions that have carried out work to formally review the potential cyber security risks presented by the following groups of suppliers

Base – all higher education institutions	**28**
Their immediate suppliers or partners	16
Their wider supply chain	6

Higher education institutions that have the following types of insurance against cyber security risks

Base – all higher education institutions	**28**
A specific cyber security insurance policy	11
Cyber security cover as part of a wider insurance policy	5
Not insured against cyber security breaches or attacks	6
Don't know	6

Higher education institutions that have the following rules or controls in place

Base – all higher education institutions	**28**
Restricting IT admin and access rights to specific users	28
A password policy that ensures users set strong passwords	28
An agreed process for staff to follow we fraudulent emails or websites	28
Up-to-date malware protection	27
Firewalls that cover your entire IT network, as well as individual devices	27
Security controls on company-owned devices (e.g. laptops)	27
Separate Wi-Fi networks for staff and for visitors	27
A virtual private network, or VPN, for staff connecting remotely	26
Backing up data securely via other means (not a cloud service)	24
Rules for storing and moving personal data files securely	24
Monitoring of user activity	21
Backing up data securely via a cloud service	18
A policy to apply software security updates within 14 days	17
Only allowing access via institution-owned devices	5

Number of higher education institutions undertaking action in each of the 10 Steps areas

	Step description – *and how derived from the survey*	**N**
	Base – all higher education institutions	**28**
1	Information risk management regime – *have formal cyber security policies and the board are kept updated on actions taken*	25
2	Secure configuration – *organisation has a policy to apply software updates within 14 days (definition changed in 2021)*	17
3	Network security – *network firewalls*	27
4	Managing user privileges – *restricting IT admin and access rights to specific users*	28
5	User education and awareness – *have formal policy covering what staff are permitted to do on the organisation's IT devices and carry out cyber security training for staff (definition changed in 2021)*	23
6	Incident management	28
7	Malware protection – *up-to-date malware protection*	27
8	Monitoring – *monitoring user activity or using security monitoring tools*	24
9	Removable media controls – *have formal policy covering what can be stored on removable devices*	22
10	Home and mobile working – *have formal policy covering remote or mobile working*	24

Qualitative findings

These findings are based on the seven in-depth interviews with higher education institutions. They complement the qualitative findings reported in the main Statistical Release.

The impact of COVID-19 on cyber security

Unlike other large organisations, the universities we spoke to already had processes and systems in place to facilitate remote working before the pandemic. It was normal for students to log into university networks or online services remotely (i.e. off campus), and there was an expectation that academic staff would frequently need to travel for their work, so these institutions already had things like security monitoring tools, Virtual Private Networks (VPNs), policies for home working and bringing your own device (BYOD) and, in some cases, video conferencing in place before March 2020.

There was a sense that the NCSC COVID-19-related guidance, covering issues such as home working, BYOD and video conferencing services (which interviewees were instructed to look at before the interview) was less relevant for universities, given that these areas were already part of their normal operations.

As such, the challenge brought about by COVID-19 and the ensuing lockdown was around scaling up the existing solutions in a short space of time. Interviewees talked about having to:

- increase VPN capacity
- issue more laptops to staff – one university had to repurpose old hardware because the new laptops they had ordered were not delivered in time
- bring in new policies (e.g. around video conferencing) and raise awareness of existing policies for home working
- introduce more comprehensive monitoring and logging, which sometimes meant investing in new monitoring tools.

"All of these things, we pretty much had before the lockdown, but we've scaled them up to support more people."

This scaling up on one hand led to increased spending on cyber security – one interviewee noted that their university had made the equivalent of two years of investment in three months. It had also accelerated planned changes like the implementation of multi-factor authentication for staff accounts or the rollout of Office 365.

On the other hand, it had considerably stretched resources. IT and cyber teams were working on multiple large projects at once, for example implementing new security monitoring tools at the same time as configuring and sending out large swathes of hardware to staff working from home. One interviewee also mentioned that the speed of change made it hard to carry out due diligence checks with IT suppliers and they risked taking shortcuts in this area.

There was scepticism as to whether COVID-19 had led to a change in university boards' attitudes towards cyber security. Generally, there was a feeling that management boards did not fully appreciate cyber security and had historically underinvested in cyber security and infrastructure projects, which had then slowed down the ability for cyber teams to scale up in spring and summer 2020. Some interviewees also felt that, as a driver of change, COVID-19 paled in comparison to experiencing a breach or being told about breaches at other universities.

"The higher education sector has suffered a number of cyber incidents, and that has been a bigger driver than COVID and lockdown for us. COVID and lockdown was about extending and increasing the use of tools and services we already had, and using them in a different way or more broadly. It wasn't a radical shift."

Upcoming cyber security priorities and expectations for the future

The upcoming areas of focus for university cyber teams were very similar to large organisations in general. However, there were some specific themes emerging from these seven interviews:

- Generally, interviewees expected investment in cyber security to rise over time, and for there to be a gradual increase in awareness of cyber security issues among the university leadership. This was linked to an increasing number of examples of cyber attacks on the higher education sector, which were catching the attention of management boards.

  "The cost versus risk profile is changing, and we are now understanding the risks a bit better. We are looking for significant investment in the cyber and protection areas."

- IT and cyber teams were very focused on making continuous improvements in technical cyber security tools and controls, typically having some sort of plan, roadmap or strategy for the next 12 months. This was commonly part of a wider IT strategy. Setting up a security information and event management (SIEM) service was frequently mentioned. One interviewee noted that Jisc had recently launched their own SIEM solution for universities which was considered more cost-effective than other options.

- A couple of interviewees also had the Cyber Essentials or Cyber Essentials Plus accreditations as part of their plans, with a view to implementing a more consistent minimum standard of cyber security across all teams and departments in their institutions.

  "We are going to obtain Cyber Essential Plus. That will bring changes to working practice. We will need some further security controls put in place to achieve the requirements of Cyber Essentials Plus. That will obviously need to be approved at the exec level."

- There was ongoing concern about the risks posed by the volume of staff working from home and the lack of direct control that cyber teams had over these staff.

  "Before, we would have used office equipment, office desktops, and they are obviously then centrally managed. We are now reliant on users keeping their own devices up to date."

Impressions of NCSC guidance on cyber security

In general, NCSC guidance was positively received and felt to be sufficiently technical. Despite some interviewees thinking that the COVID-19-specific guidance from the NCSC did not make a difference to their institution, they said it would always be reviewed as part of a range of information and guidance on cyber security. One interviewee said they had used the video conferencing guidance package as a basis for their own guidelines issued to staff, and for staff training that they later rolled out.

The NCSC was considered to be a credible and authoritative voice in cyber security. One interviewee said having the NCSC viewpoint on various issues, such as VPNs, was a helpful reassurance for the actions the university had taken.

Approaches to cyber risk management

The higher education institutions we spoke to tended to have very mature approaches to cyber risk management. In general, these approaches were very IT-focused, and the centring of responsibility on IT teams may have left gaps.

Risk assessments and audit processes were generally overseen by IT teams, even if done externally. One institution had incorporated cyber security risks into the university's wider ethics processes. They felt this could go further – ethics checks were taken very seriously across academia, and having cyber security be considered as part of an ethics check had the potential, in their view, to greatly shift the working culture.

We spoke to one university that had a supplier risk management process. Their IT teams reviewed supplier risks at the tendering and contracting stages, using questionnaires and an approved supplier screening process. However, there were concerns about the ability of staff to circumvent this process by buying services directly from suppliers without the IT team's knowledge. There were so many contracts that some were liable to get missed. There was also uncertainty about being able to get clear incident response information from a supplier, if they had a cyber security incident.

Cyber security insurance

The university findings on cyber security insurance were very similar to those for businesses and charities (covered in the main Statistical Release). However, there was a sense that universities were more risk averse in this area than private sector businesses. Those that had insurance policies felt that these were absolutely essential. In their view, there needed to be zero risk of the university ceasing to function after a major cyber incident, given the size of the institution and the number of researchers, students and partners relying on it.

Cyber accreditations

As previously mentioned, achieving cyber security accreditations was a major focus area for a couple of the universities we interviewed. Accreditations were felt to provide a clear framework and guidance on how to best manage cyber security. They could also guide an institution on the areas they needed to work on, regardless of whether they secured the accreditation or not.

"Even if we go through the process, complete most of it, but there are a few bits that we can't functionally do because it's too restrictive or doesn't fit the way we work, at least we've done the exercise to improve our position, and we know where we stand."

There was also a view that having accreditations would help to change the working culture, as all staff would then be responsible for maintaining cyber security standards, across teams and departments.

"I have proposed to the CIO to have Cyber Essentials for the whole university, not just one department. We really should meet a minimum standard across the university."

At the same time, one interviewee noted that some parts of the university needed to be accredited to more stringent standards because of the nature of their work. For example, they said that faculties that were working with the government needed to have Cyber Essentials Plus, while the parts that handled sensitive personal data, like the medical school, needed to be ISO 27001-accredited.

Appendix B: Further information

1. The Department for Digital, Culture, Media and Sport would like to thank the following people for their work in the development and carrying out of the survey and for their work compiling this report.

    - Harry Williams, Ipsos MORI
    - Orla Leggett, Ipsos MORI
    - Nick Coleman, Ipsos MORI
    - Jayesh Navin Shah, Ipsos MORI
    - Professor Steven Furnell, University of Nottingham.

2. The Cyber Security Breaches Survey was first published in 2016 as a research report, and became an Official Statistic in 2017. The previous reports can be found at https://www.gov.uk/government/collections/cyber-security-breaches-survey. This includes the full report, infographics and the technical and methodological information for each year.

3. The responsible DCMS analyst for this release is Emma Johns. The responsible statistician is Harry Smart. For enquiries on this release, from an official statistics perspective, please contact Harry at evidence@dcms.gov.uk.

4. For general enquiries contact:

    Department for Digital, Culture, Media and Sport
    100 Parliament Street
    London
    SW1A 2BQ

5. DCMS statisticians can be followed on Twitter via @DCMSinsight.

6. The Cyber Security Breaches Survey is an Official Statistics publication and has been produced to the standards set out in the Code of Practice for Official Statistics. For more information, see https://www.statisticsauthority.gov.uk/code-of-practice/. Details of the pre-release access arrangements for this dataset have been published alongside this release.

7. This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms.

Department for Digital, Culture, Media & Sport

4th Floor
100 Parliament Street
London
SW1A 2BQ