Department for Digital, Culture, Media & Sport

Cyber Security Breaches Survey 2022

Educational institutions findings annex

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

- primary schools
- secondary schools
- further education colleges
- higher education institutions

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 2022 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 an influential research study for UK cyber resilience, aligning with the National Cyber Strategy. It is primarily used to inform Government policy on cyber security, making the UK cyberspace a secure place to do business. The study explores the policies, processes, and approach to cyber security for businesses, charities, and educational institutions. It also considers the different cyber-attacks these organisations face, as well as how these organisations are impacted and respond.

For this latest release, the quantitative survey was carried out in winter 2021/22 and the qualitative element in early 2022.

Responsible analyst:

Maddy Ell
07825025654

Responsible statistician:

Robbie Gallucci

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, colleges and higher education institutions

The survey of educational institutions comprised a random probability telephone survey, carried out from 6 October 2021 to 21 January 2022. It included:

- 198 primary schools
- 221 secondary schools
- 34 further education colleges
- 37 higher education institutions

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 in Scotland, Wales and Northern Ireland: Universities UK website, cross-referenced against the comprehensive list of Recognised Bodies on GOV.UK

Higher education institutions

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.

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
- ± 7-12 percentage points for higher education institutions.

1.3 Comparability to the main results for businesses and charities

In this report, we have primarily compared our four 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, colleges and higher education institutions lie in relation to businesses when it comes to cyber security.

1.4 Comparability to the Cyber Security Breaches Survey 2021

A smaller sample of primary schools (135) and secondary schools (158) were included in the 2021 survey compared to the 2022 survey, which was carried out in a methodologically consistent way. However, a larger number of further education colleges (57) took part in the 2021 survey compared to the 2022 survey, though this was still a small overall base. 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 2021 to 2022 should not be considered definitive until we have accumulated further data over the coming years.

We also surveyed higher education institutions in the 2021 survey, but the achieved sample was very small, so will not be comparable to the findings in this year's survey.

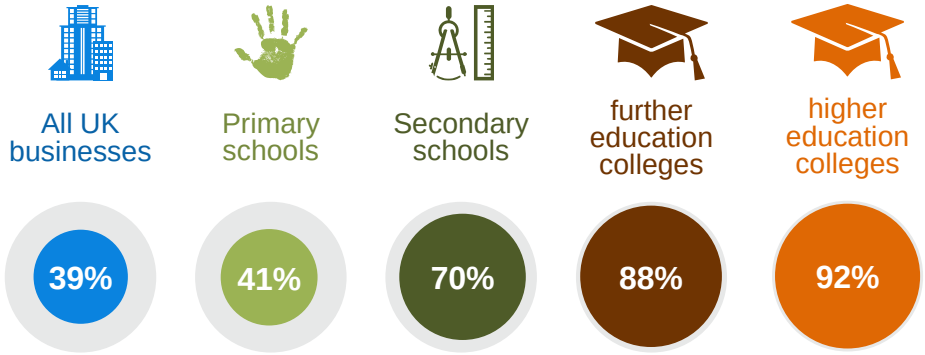
Chapter 2: Key findings

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 or attacks. Secondary schools were much more likely to identify breaches or attacks and are closer to large businesses in this regard (72% of large businesses identify breaches or attacks, as covered in the main Statistical Release). Of all the educational institutions surveyed, further education colleges (88%) and higher education colleagues (92%) were most likely to identify breaches or attacks.

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



Bases: 1,243 UK businesses; 198 primary schools; 221 secondary schools; 34 further education colleges; 37 higher education institutions

The proportion of businesses identifying breaches or attacks in 2022 remained at the same level as the previous year (39% breaches or attacks were reported in both 2021 and 2022). Similarly breaches or attacks identified within primary schools stayed at similar levels (36% reported in 2021 and 41% reported in 2022). However, within secondary schools there was a significant increase in the breaches or attacks identified this year (58% reported in 2021 compared to 70% in 2022).

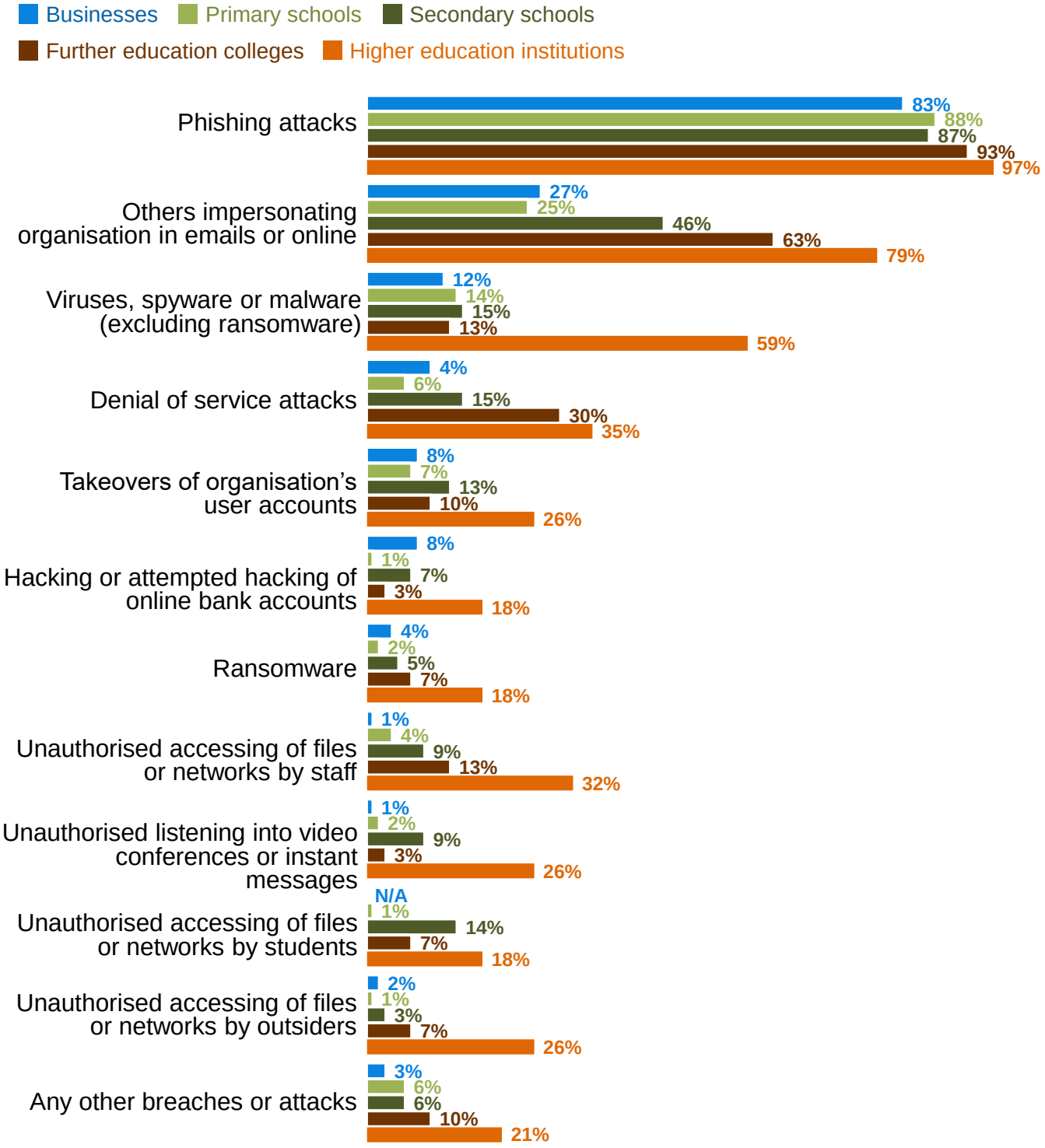
Types of breaches or attacks identified

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 and shows that 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 and higher education institutions are more likely to have experienced a wider range of breaches or attacks, as the chart suggests. Higher education institutions (73%) and further education colleges (56%) are particularly likely to identify impersonation attacks. Furthermore, higher education institutions are significantly more likely than other types of educational institution to identify viruses, spyware or malware (59%) and unauthorised accessing of files (32%).

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



Bases: 573 businesses that identified a breach or attack in the last 12 months; 81 primary schools; 155 secondary schools; 30 further education colleges; 34 higher education institutions

How are educational institutions affected?

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

- Around six in ten (62%) higher education institutions reported experiencing breaches or attacks at least weekly. In comparison, further education colleges (20%), secondary schools (23%) and primary schools (12%) reported experienced fewer weekly breaches or attacks.
- Seventy-one per cent of higher education institutions experience a negative outcome, such as a loss of money or data from a breach. Half (50%) stated their accounts or systems were compromised and used for illicit purposes. Counter to this further education colleges (42%), secondary schools (33%) and primary schools (20%) were less likely to report a negative outcome.
- Around nine in ten higher education institutions (88%) have been negatively impacted regardless of whether there was a material outcome or not. Most commonly, they report new measures being needed to prevent or protect against future breaches or attacks (79%) and additional staff time to deal with the breach or attack, or to inform or stakeholders (76%). Secondary schools (63%), further education colleges (53%) and primary schools (40%) are less likely to have been negatively impacted regardless of whether there was a material outcome or not. Higher education institutions (76%), further education colleges (43%), secondary schools (41%) and primary schools (23%) are more likely than businesses (22%) to say staff resource had to be diverted to deal with the breach.

2.2 Senior management engagement with cyber security

The educational 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.

- Almost all say that cyber security is a high priority for their governors or senior management (100% of higher education institutions, 100% of further education colleges, 98% of primary schools and 95% of primary schools). This is more in line with large businesses (95%) than with the average UK business (82%).
- More than half update their governors or senior management on cyber security at least quarterly (86% of higher education institutions, 82% of further education colleges, 68% of primary schools and 67% of secondary schools, vs. 50% of businesses and 80% of large businesses).
- Around two-thirds of schools have a governor or senior manager with responsibility for cyber security (68% of primary schools and 64% of secondary schools, vs. 34% of businesses and 62% of large businesses). Three-quarters of further education colleges (76%) and nine in ten higher education institutions (92%) similarly assign such responsibility at a senior level.

2.3 Sources of information and guidance

Seeking information

Higher education institutions (78%) are more likely than further education colleges (74%), secondary schools (71%) and primary schools (70%), to have sought information or guidance about cyber security from external sources in the last 12 months. In all cases all educational institutions included in this survey are more likely than businesses (48%) to have sought information or guidance about cyber security from external sources in the last 12 months.

The most common sources of information and guidance are:

- government and public sector sources (for 70% of higher education institutions, 37% of secondary schools, 35% of further education colleges and 33% of primary schools)

- their external cyber security or IT providers (for 38% of higher education institutions, 34% of primary schools, 28% of secondary schools and 26% of further education colleges)

There are also differences between schools, colleges and higher education institutions. Schools are more likely to have reached out to local authorities (15% of primary schools and 8% of secondary schools). Six in ten of the higher education institutions (59%) and half of the further education colleges (47%) mention Jisc (a not-for-profit company that provides digital infrastructure, services, and guidance for UK further and higher education institutions) and the Janet Network (The Janet Network supports innovative learning and teaching within higher education, underpins collaborations with research partners and enables business efficiencies), which provides UK universities and colleges with shared digital infrastructure and services.

For schools, the pattern of findings here is very similar to the 2021 survey.

Awareness of government guidance, initiatives and communications

There are still many educational 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 and higher education institutions, where typically half or more are aware of the various communications covered in the survey:

- Just under half of primary schools (45%) and just under six in ten secondary schools (55%) have heard of the government's Cyber Aware communications campaign. Awareness is higher among higher education institutions (59%) and further education colleges (74%).
- There was lower awareness of the Cyber Essentials scheme in primary schools (24%) and secondary schools (52%), than was reported in further education colleges (88%) and higher education institutions (100%)[1].
- While higher education institutions (95%) and further education colleges (65%) were more likely to have heard of the 10 Steps to Cyber Security, awareness of this guidance is lower among secondary schools (44%) and primary schools (38%)[2].
- The National Cyber Security Centre's (NCSC's) Board Toolkit is much more widely recognised in higher education institutions (81%) than in further education colleges (41%), secondary schools (31%) and primary schools (19%). However, it is worth noting that the Board Toolkit, which is aimed at senior managers and governing bodies, has not been specifically promoted across educational institutions.

2.4 Identifying cyber security risks

The majority of the educational 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 have less sophisticated approaches more akin to small businesses, whereas secondary

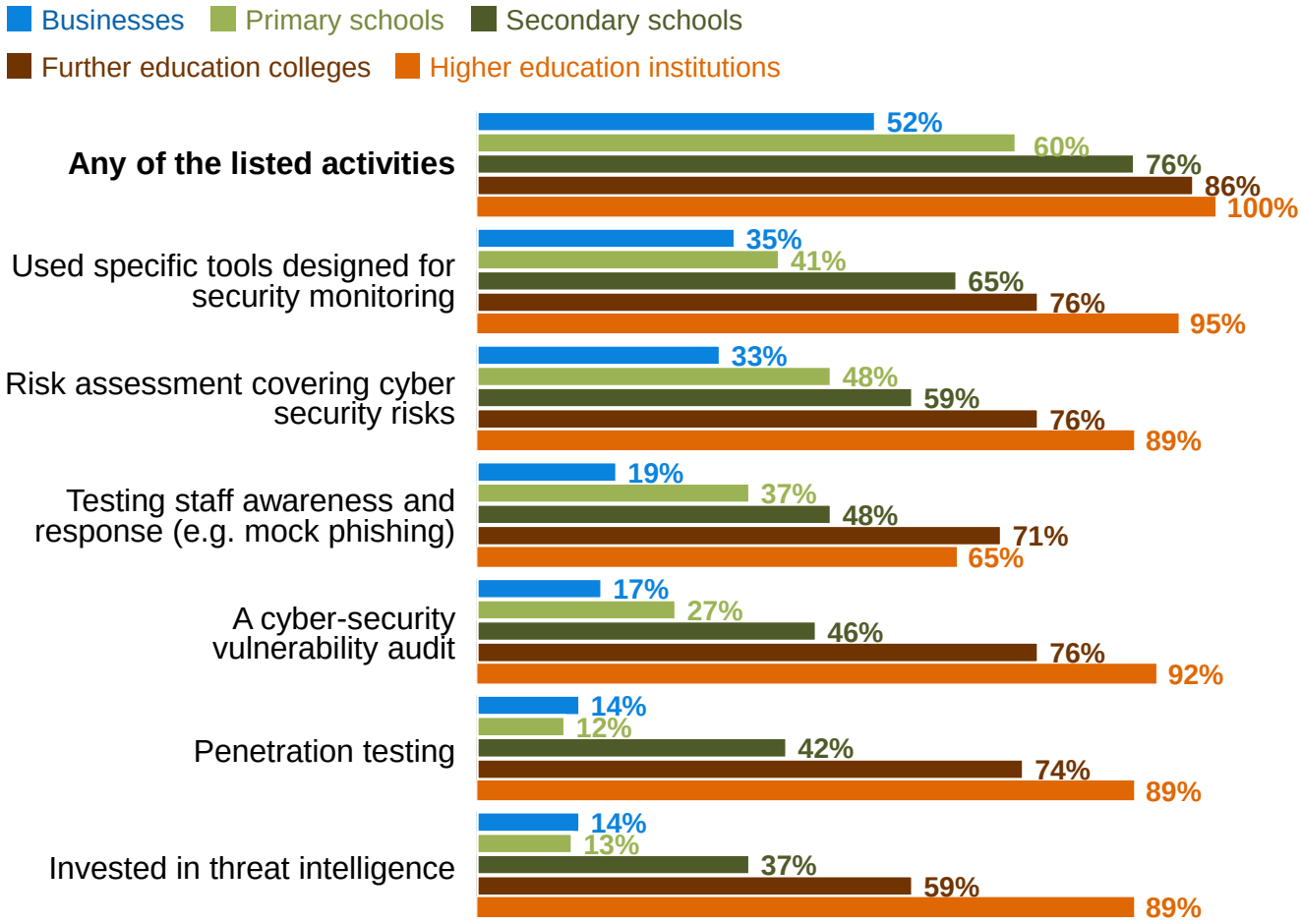
[1] The government-endorsed Cyber Essentials scheme enables organisations, including educational institutions, to be certified independently for having met a good-practice standard in cyber security.

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

schools, further education colleges and higher education institutions tend to have more sophisticated approaches.

Further education colleges and higher education institutions are specifically more likely than schools to be carrying out security monitoring, audits, penetration testing, testing staff awareness and response, investing in threat intelligence and conducting risks assessments.

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



Bases: 1,243 UK businesses; 198 primary schools; 221 secondary schools; 34 further education colleges; 37 higher education institutions

All types of educational institutions are also more likely than businesses to say they have reviewed supplier-related risks to cyber security, although this still appears to be a less common activity for primary schools and further education colleges.

- Around three in ten primary schools (29%) and further education colleges (32%) say they have reviewed such risks posed by their immediate suppliers or partners, as have just over one in three secondary schools (36%). Higher education institutions are more likely to do so, with around six in ten (62%) reviewing such risks. This compares to 13% of businesses.
- Higher education institutions (32%) are most likely to have reviewed the risks presented by their wider supply chains. In contrast, 15% of primary schools, and around two in ten secondary schools (18%) and further education colleges (21%) are less likely to have

reviewed the risks presented by their wider supply chains. This compares to under one in ten (7%) businesses.

2.5 Actions taken to manage or mitigate risks

Staff training and awareness raising

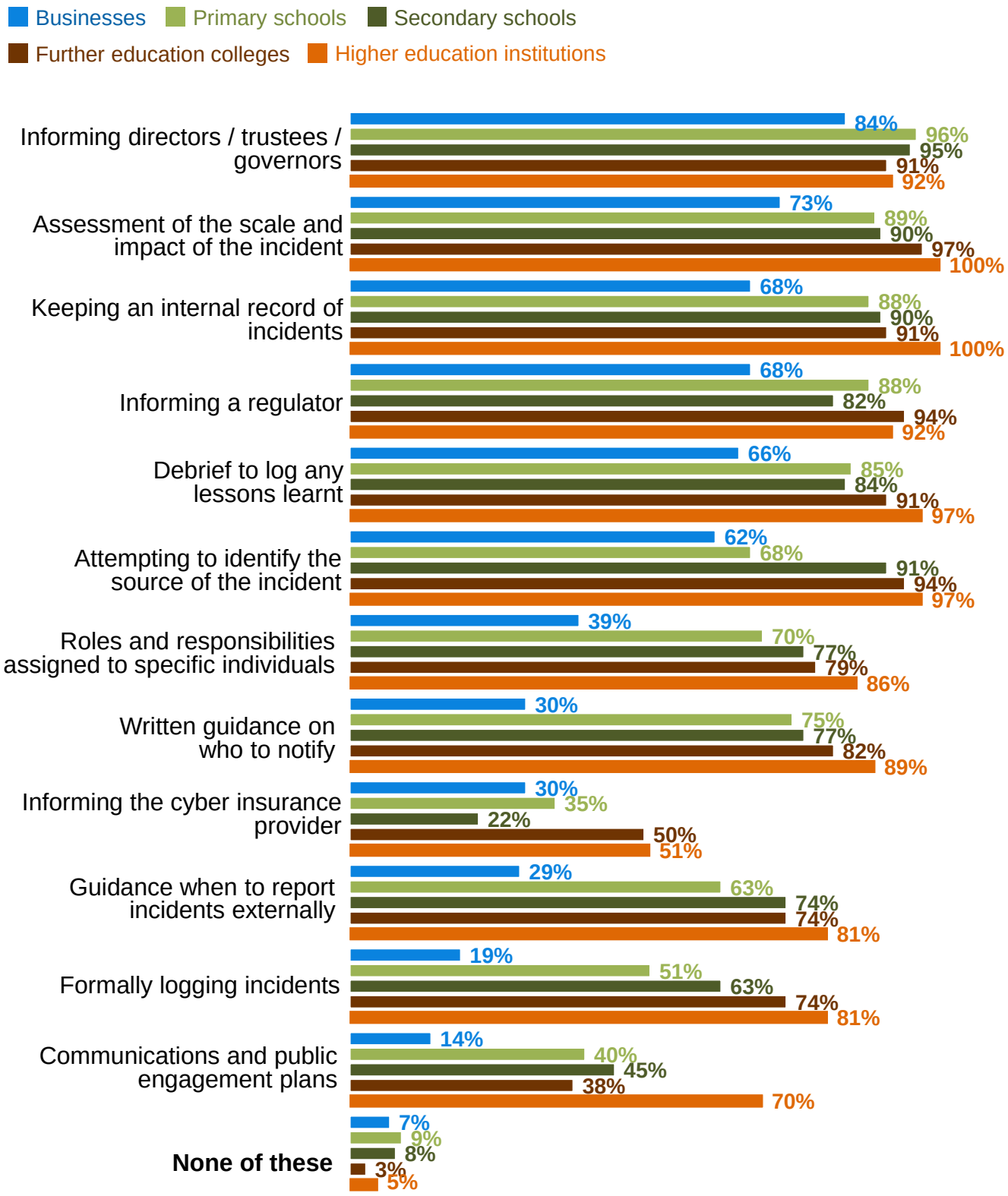
Cyber security training or awareness raising activities are less common in schools than further and higher education institutions. Around four in ten of primary schools (42%) and around half of secondary schools (51%) have undertaken any such activities in the last 12 months. This rises to around eight in ten further education colleges (82%) and all higher education institutions (100%).

Cyber security planning and documentation

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

- Around seven in ten primary (69%) and secondary schools (71%) have a cyber security policy. Policies are slightly more ubiquitous in further education colleges (79%) and higher education institutions (86%).
- Business continuity plans covering cyber security also tend to be in place in most of these institutions, although they are less common in primary schools (63% of primary schools, 69% of secondary schools, 84% of higher education institutions and 88% of further education colleges have such plans in place).
- Incident response planning in educational institutions is also more sophisticated than in the average business, as Figure 2.4 indicates. Higher education institutions (81%) and further education colleges (74%) are more likely to have a formal incident response plan than schools (63% of secondary schools and 51% of primary schools). Response planning in higher education institutions and further education colleges are more likely to have plans that encompass each area in the chart than schools.

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



Bases: 1,243 UK businesses; 198 primary schools; 221 secondary schools; 34 further education colleges; 37 higher education institutions

Insurance against cyber security breaches

Around two thirds of further education colleges (68%) and higher education institutions (65%) report being insured against cyber risks, with a smaller proportion of primary schools (41%) and secondary schools (31%) 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 (47% and 48% respectively)[3]. This compares to 20% of businesses not knowing. It highlights that cyber security is perhaps more siloed in schools, and therefore considered separately from financial matters like insurance.

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

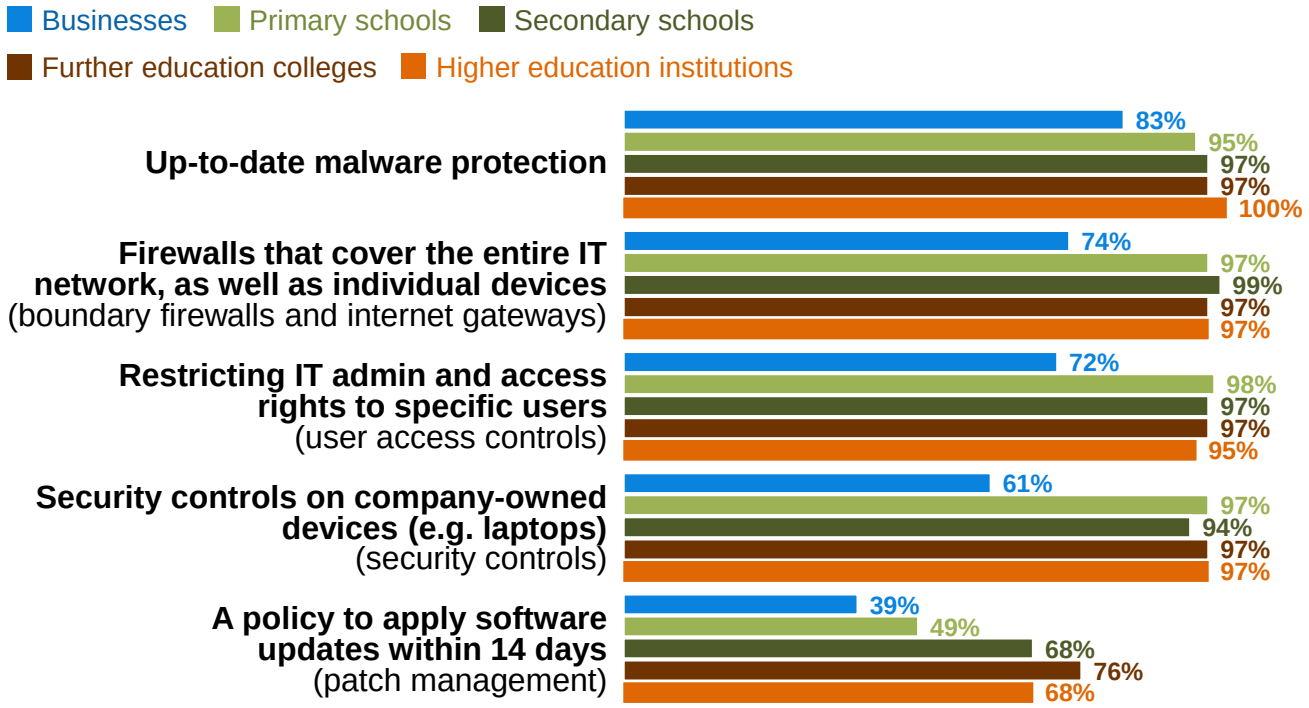
Technical rules and controls

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, educational 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 area of patch management compared to other types of educational institutions, with around half (49%) having a policy to apply software updates within 14 days.

[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.

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



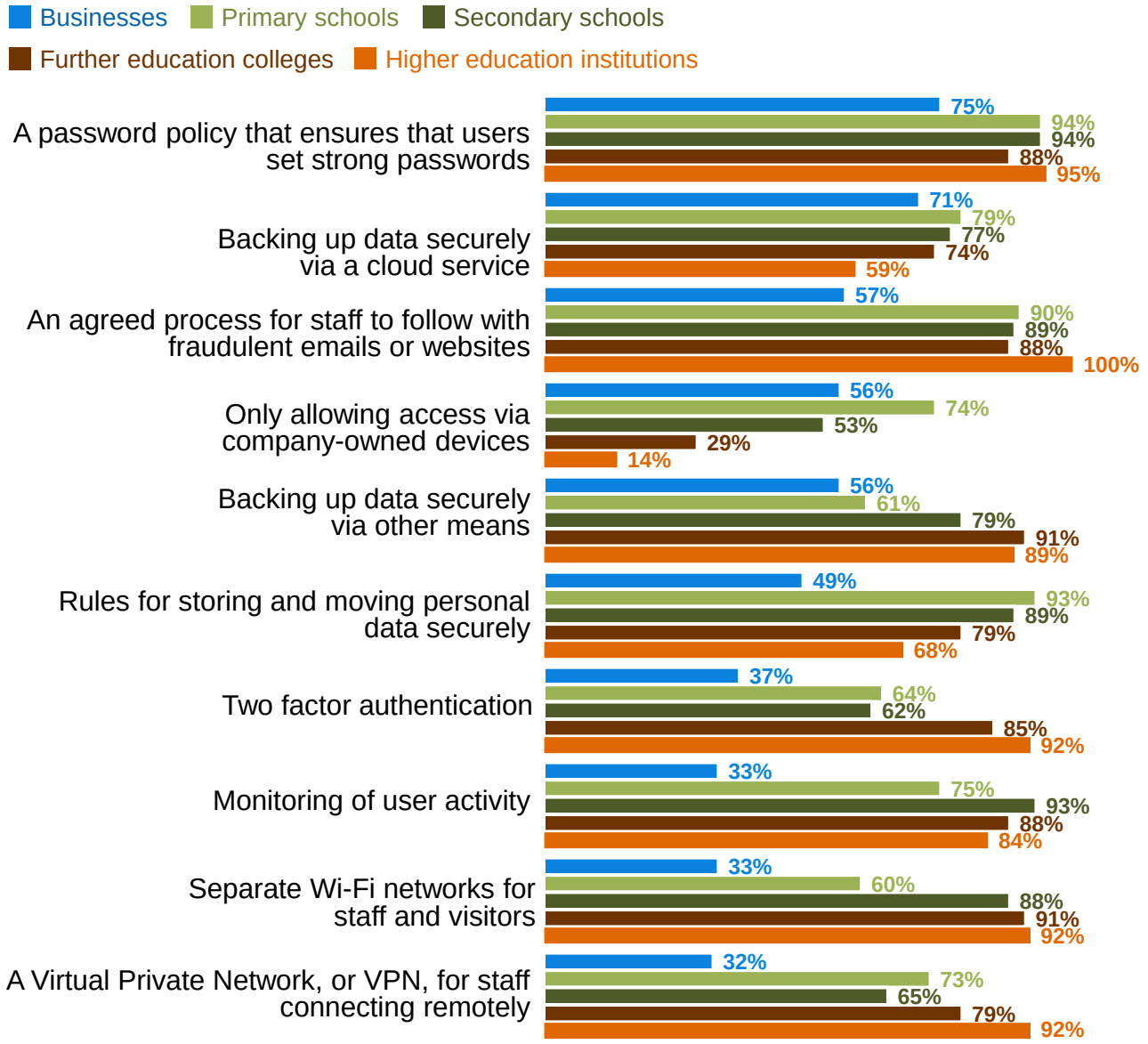
Bases: 1,243 UK businesses; 198 primary schools; 221 secondary schools; 34 further education colleges; 37 higher education institutions

Bold wording used in questionnaire

Primary schools are less likely than other educational 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 educational institutions are more likely to use other means for secure back-ups.

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



Bases: 1,243 UK businesses; 198 primary schools; 221 secondary schools; 34 further education colleges; 37 higher education institutions.

These findings, where questions are consistent across years, are similar to the 2021 survey.

Outsourcing cyber security

Our sample suggests that outsourcing cyber security is more common among primary schools than other educational institutions. A total of 80% of primary schools say an external provider manages their cyber security for them, compared with 44% of secondary schools, 19% of higher education institutions and 18% of further education colleges.

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. In addition, this year NCSC updated their 10 steps guidance[4], so we have not mapped the figures onto the previous year's findings due to these changes.

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

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

	Step description – *and how derived from the survey*	Primary	Secondary	Further	Higher
1	**Risk management** – *Organisations who update boards at least annually and have at least 2 of the following: a cyber security policy or strategy, adherence to Cyber Essentials or Cyber Essentials Plus, undertake risk assessments, have cyber insurance (either a specific or non-specific policy), undertake cyber security vulnerability audits, have an incident response plan, managing suppliers or supply chain cyber risks.*	77%	78%	94%	95%
2	**Engagement and training** – *Organisations that train staff or do mock phishing exercises*	100%	66%	85%	100%
3	**Asset management** – *Organisations that list of critical assets*	62%	71%	76%	87%
4	**Architecture and configuration** – *Organisations that configure firewalls and either: secure configurations, i.e., security controls on company devices or have a policy around what staff are permitted to do on company devices*	96%	95%	97%	97%

[4] Ten Steps government guidance was rewritten this year. Therefore Ipsos have reconfigured how we map responses in the survey to the Ten Steps, and, as such, they are not comparable to 2021 or previous years.

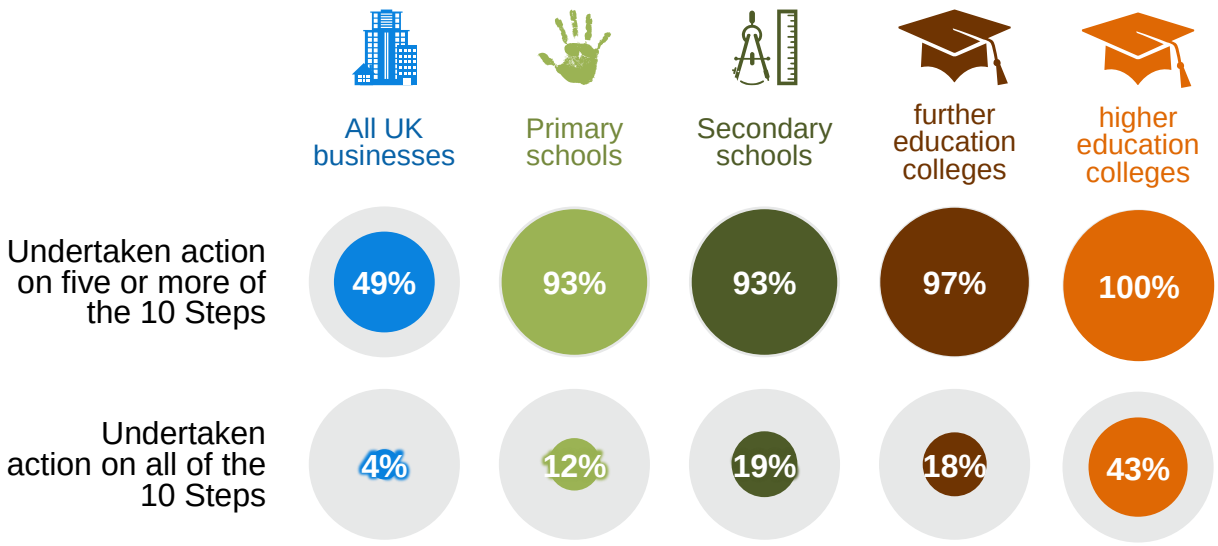
	Step description – *and how derived from the survey*	Primary	Secondary	Further	Higher
5	**Vulnerability management** – *Organisations that have a patching policy and at least one of the following: undertake vulnerability audits, penetration testing, update anti-malware, or have a policy covering SaaS*	49%	68%	76%	68%
6	**Identity and access management** – *Organisations that restrict admin rights or password policy or two factor authentication*	100%	100%	97%	100%
7	**Data security** – *Organisations with cloud or other backups and at least one of the following: secure personal data transfers, have policy covering removable storage or on how to store data*	88%	91%	88%	87%
8	**Logging and monitoring** – *Organisations with monitoring tools or if log breaches and had a breach*	52%	81%	91%	97%
9	**Incident management** – *Organisation with incident response plans or formal debriefs*	89%	88%	97%	100%
10	**Supply chain security** – *Organisations that monitor risks from suppliers or wider supply chain*	31%	38%	39%	68%

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

- risk management
- asset management
- logging and monitoring

Looking at these 10 Steps together, virtually all educational 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 2.7.

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



Bases: 1,243 UK businesses; 198 primary schools; 221 secondary schools; 34 further education colleges; 37 higher education institutions

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.

Cyber security decision making and culture

There was variation amongst educational institutions in how they budgeted for cyber security. Some had a specific cyber security budget, whereas for others the budget was shared with IT or part of capital expenditure. Having cyber security as part of a larger budget tended to increase the competition between business objectives. It made long-term or large spending more difficult, such as through spending to foster culture change or to create training programmes. In general, there tended to be a low level of knowledge of cyber security amongst those in the senior management team. This meant that their approach to cyber security was often not 'hands on' enough, and decisions were made on a reactive basis. As an example, one university was able to secure a budget increase after a ransomware attack. They also felt that this led to a change in attitudes amongst senior management whereby cyber security was seen as an investment to ensure they could progress as an institution.

"We've had an injection of following a ransomware attack. Yeah, we've been given a much bigger budget the priorities have changed significantly… At a senior level should be about, what are we trying to protect? Fundamentally and really understand that. Not things but strategic aims, what underpins our strategic priorities, what things can stop our progress."

Higher education institution

Where there was an individual at senior level with an understanding of cyber security, decision making was more efficient. This enabled cyber security to be seen as a high risk and meant consequences of not being proactive were well understood. This also led to senior staff gaining greater awareness of the importance of cyber security, with steering groups and board updates on cyber risks embedding knowledge and fostering decision making.

"I provide an update to our audit and risk committee twice a year to explain our current understanding to risk position and our current level risk and how we bring that down to an

acceptable level. That gives exec oversight. In addition to that we have a number of working groups."

Higher education institution

The most crucial aspect for changing the culture around cyber security was the behaviour of end users. Educational institutions often struggled to properly convey the importance of individual behaviour for cyber security hygiene. Organisations understood that the process would be long and difficult, and that the tone in which they conveyed their message was very important: no one should be made to feel guilty for making a mistake. Training was a vital part of cyber security culture change, but it was often underfunded, and some felt that commercial packages did not have enough impact.

"The challenge is always the change in the culture, and changing the understanding of the risk. You have to be able to talk the language of the user what...poor behaviour could result in"

Higher education institution

"The biggest challenge is getting people to understand the 'even with multi-layered defences... a single person can still bring down the whole system"

Higher education institution

Cyber security insurance

Higher education institutions tended to feel that cyber insurance would give them access to the best expertise in the event of an attack. Universities tended to have wide-ranging policies of a large monetary value. These policies included help with ransomware attacks and most included post-incident support, such as forensic analysis and protection against class-action suits. However, some universities we spoke to said that it was becoming more difficult to retain a cyber-insurance policy. This was often because of the increasing stringency of the requirements. One university we spoke to had put in multi-factor authentication (MFA) for all their accounts, as it was required by their policy. They believed they would soon be required to put MFA on all services, which would be difficult to implement. Another we spoke to said their insurer had informed them that their policy could no longer cover ransomware payments.

"Being able to bring in a digital forensic team that is really skilled with enough manpower to deal quickly and efficiently with the incident. Our international security team - they don't have infinite resources, they're not sufficiently expert in digital forensics, especially at short notice."

Higher education institution

"Some universities are being priced out of [cyber insurance] because they can't meet the requirements"

Higher education institution

Threat intelligence

We asked universities about how they used threat intelligence. Some universities received threat intelligence through their work with particular clients who were well-placed in the cyber-security industry. Others used cloud-based services which specialised in threat intelligence such as Qualys. Some had partnerships with security firms, such as NCC Group, which provided them with up-to-date threat intelligence. The intelligence they received focused on what was most likely to cause a cyber-security incident. Although institutions were glad that the intelligence was provided to them, some felt that they did not have the necessary resources to act upon it. Others used the intelligence as a basis for informing trustees about their wider cyber-security strategy.

“These security operation centres…they provide raw threat intelligence. What you do with it, is the real challenge."

Higher education institution

Information seeking

The educational institutions we spoke to tended to be proactive when it came to seeking out information on cyber-security. They sought out information from a wide range of sources. This included official channels, such as CISC, Jisc CISO Forums, the British government (e.g. NCSC or MOD), and the FBI. It also included unofficial channels such as forums to update users on the latest cyber-security threats. Participants would also seek out information in response to stories in the media about attacks. Some institutions implemented changes after seeking out information, such as changing cyber-security measures to be able to spot ransomware attacks sooner.

"We will follow up with government agencies, NCSC or MOD with regards to more in-depth information, regarding attacks or compromises”

Higher education institution

Ransomware

The educational institutions we spoke to felt ransomware was a serious threat. This was because it seen as unique in its ability to shut down important systems. There was also a sense that the threat from ransomware was increasing. One institution mentioned the ‘double-pronged’ approach of ransomware for universities: they could lose operational control or access to their systems, and could also be threatened with leaked data. Institutions seemed to have a high level of protection, including multi-factor authentication (MFA) as well as improved malware. However, there was a feeling that this was likely not to be enough, due to the sheer volume of attacks sent at their systems. Although most institutions had not suffered a ransomware attack, a smaller number had. One institution described having to rebuild their system for scratch in the aftermath. Almost all institutions said that they would not pay a ransom if attacked – this was often a policy decided at a trustee level.

"There's not many threats that can bring all teaching, all research, all activities to a halt for a few weeks, so it's something we take very seriously and we're rightly nervous about."

Higher education institution

"In addition to having well-rehearsed backup procedures, we've deployed MFA and have improved anti-malware on our endpoints. We've increased monitoring on our servers and a platform giving us a central view of our server and its behaviour. We've got a host of other controls as well."

Higher education institution

External reporting of breaches

The educational institutions we spoke to stated they would report any cyber incident to different agencies, depending on the kind of attack. For financial attacks, participants said they would contact their bank as well as Action Fraud. For other types of cyber-attacks, such as a suspected breach or ransomware, participants said they would report to the Information Commissioners Office (ICO), or the NCSC if their website was compromised. In contrast to the businesses we interviewed, higher education institutions tended to feel that they would always report breaches.

"We would, we would engage with the NCSC, and if there was anything significant we would tell them but it would be only the level of general interest."

Higher education institution

Managed Security Providers (MSPs)

The institutions we spoke to received a wide range of services from their MSPs, including student records, payroll processes, print services. Institutions tended to have quite a refined process for choosing MSPs: some would meet the product team to ensure that the service met the needs of their organisation. All institutions seemed to feel that MSPs provided them with much needed services. Some said that using MSPs was beneficial because it allowed them to measure performance against clear metrics which could be delivered upon – this was easier than holding internal staff to account. Institutions tended to pick MSPs on the basis of trust – i.e. trust in a large tech company's ability to provide a secure service. Like businesses, institutions did not audit MSPs on their own cyber security practices due to the high level of trust they placed in them.

"We're going for systems with, you know, big players with good reputations. And that's part of that sort of trust relationship."

Higher education institution

Appendix A: Further information

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
- Eleanor Myers, Ipsos
- Alice Stratton, Ipsos
- Dejon Silvera, Ipsos
- Jayesh Navin Shah, Ipsos.

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.

The responsible DCMS analyst for this release is Maddy Ell. The responsible statistician is Robbie Gallucci. For enquiries on this release, from an official statistics perspective, please contact the team at evidence@dcms.gov.uk.

For general enquiries contact:

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

Telephone: 020 7211 6000

DCMS statisticians can be followed on Twitter via @DCMSinsight.

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.

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