GOV.UK

Department for Science, Innovation & Technology

Home Office

Official Statistics

Cyber security breaches survey 2025: education institutions findings

Published 10 April 2025

Contents

This publication is available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-education-institutions-findings

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 annex supplements a main Statistical Release (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025) published by the Department for Science, Innovation and Technology (DSIT) and the Home Office, covering the 2025 results for businesses and charities.

Methodological details of the study and copies of the main survey instruments to aid interpretation of the findings are available in the Technical Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-technical-report), available on the same GOV.UK page.

The Cyber Security Breaches Survey is a research study on UK cyber resilience. 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 and cyber crimes these organisations face, as well as how these organisations are impacted and respond.

For this latest release, the quantitative survey and qualitative interviews were carried out between August and December 2024.

Lead analyst and responsible statistician: Saman Rizvi

Enquiries: cybersurveys@dsit.gov.uk

Summary

Prevalence and impact of cyber security breaches and attacks

- Prevalence of cyber security breaches or attacks in the last 12 months was high among secondary schools (60%), further education colleges (85%), and higher education institutions (91%). They were all more likely to experience a breach or attack than businesses overall (43%).
- Primary schools were close to the businesses overall in terms of how many identified breaches or attacks (44% primary schools and 43% businesses).
- Amongst those who identified a breach or attack, further education colleges and higher education institutions were also more likely than businesses overall to experience a wider range of attack types, such as impersonation (68% of further and higher education institutions combined compared to 34% of businesses overall), viruses or other malware (42% of further and higher education institutions combined compared to 18% of businesses overall), and denial of service attacks (36% of further and higher education institutions combined compared to 5% of businesses overall).
- Further and higher education institutions were more likely to be affected by cyber breaches and attacks on a frequent (weekly) basis (30%) compared to primary schools (9%) and secondary schools (16%). Four in ten further and higher education institutions (40%) experienced a negative outcome from a breach.

Engagement with cyber security

- Education institutions typically reported a higher level of board engagement with cyber security (98% of primary schools, 95% of secondary schools, 98% of further education colleges and 97% of higher education institutions) than businesses overall (72%). In this sense, they were more like large businesses (96%).
- As in previous years, many educational institutions expressed low awareness of government guidance like the National Cyber Security Centre’s (NCSC) 10 Steps to Cyber Security and Board Toolkit, certification schemes like Cyber Essentials, and communications campaigns like Cyber Aware. Awareness of these initiatives continued to be higher in education institutions than in businesses and charities and was much more widespread in further education colleges and higher education institutions than in primary and secondary schools.

Approaches to cyber security

- All educational institutions had a level of preparedness and planning for cyber security that was notably more advanced than that of businesses overall, bearing more resemblance to large businesses. At least eight in ten educational institutions had an established cyber security policy (82% of primary schools, 81% of secondary schools, 92% of further education colleges and 84% of higher education institutions).
- The majority of education institutions had taken action in the last 12 months to help identify cyber security risks (e.g. undertaking risk assessments) (84% of primary schools, 86% of secondary schools, 98% of further education colleges and 100% of higher education institutions), and on a number of measures were more active in this year's survey than in 2024. However, further education colleges and higher education institutions continued to have more sophisticated cyber risk management approaches than schools.
- All types of education institutions were more likely than businesses overall to have technical controls in place in the five technical areas covered in Cyber Essentials.

Chapter 1: Overview of the data

1.1 Summary of methodology

Each year, the Cyber Security Breaches Survey includes two strands: a quantitative survey and follow-up qualitative interviews with some of the organisations taking part in the survey.

Quantitative survey
The 2025 survey of educational institutions comprised a random probability telephone survey, carried out from August to December 2024. It included:

- 250 primary schools
- 240 secondary schools
- 52 further education colleges
- 32 higher education institutions

The school samples included 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 (https://get-information-schools.service.gov.uk/)
- Schools in Scotland: Scottish Government School Contact details (https://www2.gov.scot/Topics/Statistics/Browse/School-Education/Datasets/contactdetails)
- FE Colleges in Scotland: Colleges Scotland directory (https://collegesscotland.ac.uk/our-members/colleges-in-scotland)
- Schools in Wales: Welsh Government Address list of schools (https://gov.wales/address-list-schools)
- FE Colleges in Wales: Colleges Wales directory (https://www.gov.wales/further-education-institutions-contact-details)
- Schools in Northern Ireland: NI Department of Education database (http://apps.education-ni.gov.uk/appinstitutes/default.aspx)
- FE Colleges in Northern Ireland: NI Direct FE College directory (https://www.nidirect.gov.uk/contacts/further-education-fe-colleges)
- Higher education institutions in Scotland, Wales and Northern Ireland: Universities UK website (https://www.universitiesuk.ac.uk/about/Pages/member-institutions.aspx), cross-referenced against the comprehensive list of Recognised Bodies (https://www.gov.uk/check-a-university-is-officially-recognised/recognised-bodies) on GOV.UK

Qualitative interviews
In addition, we carried out 11 qualitative interviews with institutions that took part in the survey including:

- 1 primary schools
- 3 secondary schools
- 3 further education institutions
- 4 higher education institutions

In this annex, we include the key findings from these education institutions, as well as a selection of quotes from these interviews to illustrate the themes raised. We do not provide specific job title descriptions when attributing the quotes as these may be disclosive. Participants in these interviews were all cyber or IT specialists.

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 less representative samples.

As the sample sizes are relatively small compared to the business and charity survey samples, the margins of error were higher. There is also greater uncertainty over estimates which have the highest variation e.g. where around 50% of respondents answered “yes”. Below highlights the upper bound for the most uncertain estimates of the 95% confidence margins of error[footnote 1] for each type of education institution:

- ± 6.2 percentage points for primary schools
- ± 6.2 percentage points for secondary schools
- ± 12.5 percentage points for further education colleges
- ± 15.7 percentage points for higher education institutions

1.3 Comparability to the main results for businesses and charities

In this annex, we have primarily compared our four largest types of 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 Comparisons with previous surveys

The findings from 2025 are compared with equivalent findings from the 2024 survey. The 2025 sample sizes for all four types of educational institutions were similar to, or slightly higher than, those obtained in 2024. Because of the small sample sizes for further education colleges (43 in 2024, 52 in 2025) and higher education institutions (31 in 2024, 32 in 2025), changes between years should be treated with caution, and should be viewed as indicative only.

Where appropriate, the report also comments on longer-term changes since 2020 (the first year that education institutions were included in the survey). This analysis seeks to identify broad patterns of change over time, rather than specific instances of statistically significant changes.

Whilst there were no changes to the methodology between 2024 and 2025, there were some minor changes to the questionnaire which are fully detailed in the Technical Annex (https://www.gov.uk/government/statistics/cyber-

security-breaches-survey-2025/cyber-security-breaches-survey-2025-technical-report). None of the 2025 changes impact the ability to compare data in this Education Annex from 2025 to previous years of the survey.

Chapter 2: Key findings

2.1 Prevalence and impact of cyber security breaches or attacks

It is important to remember that the survey could only measure the breaches or attacks that organisations have themselves identified. There were likely to be hidden attacks, and others that go unidentified, so the findings reported here may have underestimated the full extent of cyber security incidents.

As Figure 2.1 shows, primary schools were relatively close to businesses overall in terms of how many identified breaches or attacks (44% primary schools compared to 43% businesses overall). Secondary schools were more likely to identify breaches or attacks (60%) and were closer to medium businesses (67%) in this regard. Of all the educational institutions surveyed, further education colleges (85%) and higher education institutions (91%) 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

Primary schools	44%
Secondary schools	60%
Further education colleges	85%
Higher education institutions	91%
Businesses overall	43%

Bases: 250 primary schools; 240 secondary schools; 52 further education colleges; 32 higher education institutions; 2,179 businesses overall

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 a breach or attack.

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 were reporting. Schools almost universally had lower levels of breaches and attacks than further education colleges and higher education institutions.

In schools, phishing was by far the most common type of breach or attack (89% for both primary and secondary schools). The level of various types of attacks tended to be consistent with those experienced in 2024.

Further and higher education institutions combined had the highest levels of incidence for most breaches or attacks, including:

- phishing attacks (97% compared to 89% for both primary schools and secondary schools)
- impersonation (68% compared to 32% primary schools and 50% secondary schools)
- viruses, spyware or malware (42% compared to 9% primary schools and 22% secondary schools)
- denial of service attacks (36% compared to 2% primary schools and 10% secondary schools)
- any other breaches or attacks (not listed in Figure 2.2) (22% compared to 1% primary schools and 3% secondary schools).

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

Type of Breach or Attack	Primary schools	Secondary schools	Further and higher education institutions	Businesses overall
Phishing attacks	89%	89%	97%	85%
People impersonating, in emails or online, your organisation or your staff	32%	50%	68%	34%
Viruses, spyware or malware	9%	22%	42%	18%

Type of Breach or Attack	Primary schools	Secondary schools	Further and higher education institutions	Businesses overall
(excluding ransomware)				
Hacking or attempted hacking of online bank accounts	6%	3%	11%	6%
Denial of service attacks	2%	10%	36%	5%
Takeover of organisation's user accounts	6%	6%	14%	7%
Unauthorised accessing of files or networks by staff	6%	10%	11%	2%
Ransomware	7%	3%	15%	6%
Unauthorised accessing of files or networks by students	5%	17%	11%	0%
Unauthorised accessing of files or networks by outsiders	4%	1%	5%	2%
Any other breaches or attacks	1%	3%	22%	4%

Bases: Those that identified a breach or attach in the last 12 months; 109 primary schools; 144 secondary schools; 73 further and higher education institutions (combined due to low base for higher education); 1,132 businesses overall.

How are educational institutions affected?

Among those that had experienced breaches or attacks in the last 12 months, higher education institutions were more likely to be affected than further education colleges and schools.

One in three (30%) further and higher education institutions reported experiencing a breach or attack at least weekly. In comparison, primary schools (9%) and secondary schools (16%) experienced significantly fewer weekly breaches or attacks.

One in four further and higher education institutions (40%) experienced negative outcomes from a breach. A fifth (22%) stated that their accounts or systems were compromised and used for illicit purposes. By contrast, primary schools (13%) and secondary schools (19%) were less likely to report a negative outcome.

Qualitative insights on perceptions of cyber security risk

The qualitative interviews indicated that educational institutions continued to place a high priority on cyber security. Interviewees tended to perceive a high level of risk for their institutions and for the education sector as a whole.

> “We’re quite a big target [for phishing and ransomware attacks], obviously education is a massive target because we’ve got the money of the government and the academies behind us.” **Secondary school**

Some interviewees felt that the level of concern over cyber security had increased, alongside greater awareness among staff. This could have been as a result of recent cyber security breaches which had raised staff awareness and understanding, as well as regular staff training, which could help to foster a culture where staff were aware of potential risks (for example, in reporting suspicious emails). Some interviewees also noted that there was a growing emphasis on compliance and accreditation, both internally and from government.

> “We had a big [cyber security] incident a couple of weeks ago, and that always shifts people’s perception of risks, even though it doesn’t actually change the risks themselves.” **Higher education institution**

When asked about the types of risks they were facing, interviewees often mentioned phishing attacks, generally via email. These attacks could be targeted at the institution or on individual students’ accounts.

> “We regularly see students just installing software willy nilly and not realizing that they’ve had their account breached from a cracked

> Telegram app, or they've signed up for a service that's been breached." **Further education college**

Several interviewees expected the level of risk to increase further over the next 12 months, with threats becoming ever more sophisticated and with more targeted spear phishing. One interviewee commented on the growing role of artificial intelligence (AI), which offered both opportunities and threats.

> "It's an evolving thing. I mean, also AI…gives us theoretically more potential protections, but also makes the attacks better." **Further education college**

Interviewees discussed the actions they were taking to combat threats. They mentioned specific changes, such as moving to a more cloud-based approach, strengthening procedures for quarantining emails and implementing their own regular external vulnerability scans.

> "We're going to be doing a lot of tightening up of security things that are on lists of lots of small things that need doing…we will be putting more restrictions on staff and students accounts." **Higher education institution**

As in previous years, some interviewees discussed the financial constraints faced by educational institutions, which could restrict their ability to improve their cyber security. One interviewee noted that, as cyber security tools were becoming more sophisticated, costs were also increasing.

2.2 Senior management engagement with cyber security

The educational institutions in our sample typically reported a higher level of senior engagement with cyber security than businesses overall. In this sense, they were more like large businesses, which was also the case in previous years.

Almost all reported that cyber security was a high priority for their governors or senior management (98% of primary schools, 95% of secondary schools, 98% of further education colleges and 97% of higher education institutions). These findings have remained very consistent over time since 2020.

The majority of education institutions updated their governors or senior management on cyber security at least quarterly: 91% of higher education institutions, 81% of further education colleges, 73% of primary schools (up from 63% in 2024) and 67% of secondary schools. This compared with 63% of medium businesses and 83% of large businesses.

Around eight in ten educational institutions had a governor or senior manager with responsibility for cyber security (compared with 27% of businesses and 66% of large businesses). This applied to 83% of primary schools (a significant increase from 71% in 2024), 76% of secondary schools, 85% of further education colleges and 81% of higher education institutions.

Qualitative insights on senior management engagement

The qualitative interviews indicated a varied level of understanding of cyber security among senior management and board members. Some boards demonstrated a high level of knowledge and engagement, sometimes due to their own career backgrounds.

> "We have some actual expertise as well on the board from people who, in their main jobs, are involved in these types of areas. So we've always had a lot of good support from them and from senior management…I've always been stricken by how senior management and our board take this very seriously." **Higher education institution**

In other cases, knowledge was limited or varied between individuals, with senior management or board members relying on specialist staff or external contractors.

> "It depends on some of the board members because the board members have different focuses to spread the workload." **Primary school**

> "I think it's not the most digitally savvy executive board, so they do struggle, but they understand it in higher level terms. That's how I describe it to them. So I think they know enough to know what the important things we're doing and we need to do are." **Higher education institution**

Communication with boards and senior management was typically through a regular, structured process of meetings, reviews and reports. For example, one interviewee said they carried out a quarterly review in the form of a written report, followed by a personal meeting. Another interviewee said that cyber security was discussed frequently by senior

management, both in formal meetings that occurred every two months, as well as in more informal ad-hoc settings.

> “Every quarter I do reports for them and I’ll be on one of the committee meetings that they can ask me questions and review how everything’s gone.” **Further education college**

Institutions varied in terms of the level and nature of involvement by board members in decisions on cyber security. This tended to reflect the levels of knowledge and engagement that they showed. Some boards were highly engaged and involved with decision-making. In some cases, board actively monitored or challenged staff on activities and processes.

> “Our board is very much in line on the importance of cyber security. It’s the highest thing on our risk register. They demand regular reports from myself and colleagues. They’re interested.” **Higher education institution**

In other institutions, board involvement was more a case of providing oversight, rather than active decision-making.

> “We’re pretty effective at what we do. So their oversight is more a case of just checking that.” **Further education college**

Overall, the interviews indicated a mixed picture of board involvement and understanding of cyber security. In some cases, board members were extremely knowledgeable and highly engaged, while other boards were less directly involved.

2.3 Sources of information and guidance

Seeking information

Eight in ten higher education institutions (81%) said they had sought information or guidance about cyber security from external sources in the last 12 months. Around seven in ten primary schools (74%), secondary schools (68%) and further education colleges (69%) sought information or guidance from external sources.

All types of education institutions included in this survey were more likely than businesses (42%) 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 were consistent with the 2024 survey, as follows:

- Government and public sector sources were used by one in four higher education institutions (28%) and further education colleges (23%), as well as by 20% of secondary schools and 14% of primary schools.
- More than four in ten higher education institutions (44%) used external cyber security or IT providers, as did three in ten primary schools (32%) and secondary schools (30%), as well as one in four further education colleges (25%).

There were also other differences between schools, colleges and higher education institutions. More than six in ten higher education institutions (63%) had sought information or guidance from the National Cyber Security Centre (NCSC), compared with 27% of further education colleges. The NCSC was mentioned by 11% of secondary schools and 5% of primary schools.

Both higher education institutions (56%) and further education colleges (44%) mentioned Jisc and the Janet Network[footnote 2], which provide UK universities and colleges with shared digital infrastructure and services. 15% of primary schools and 7% of secondary schools sought information from the Local Authorities.

Awareness of government guidance, initiatives and communications
As in previous surveys, there were still many educational institutions that had not heard of the various government guidance, initiatives and communications campaigns on cyber security. Awareness was, as found in previous years, much more widespread in further education colleges and higher education institutions, where typically half or more were aware of the various communications covered in the survey:

- Awareness of the government's Cyber Aware (https://www.ncsc.gov.uk/cyberaware/home) communications campaign decreased among higher education institutions (from 74% in 2024 to 56% in 2025). Awareness of the campaign remained similar among further education colleges (67%), secondary schools (55%) and primary schools (48%).
- As in previous years, large proportions of further education colleges (88%) and higher education institutions (87%) had heard of the Cyber Essentials (https://www.cyberessentials.ncsc.gov.uk/advice/) scheme, much higher than the proportions of secondary schools (43%) and primary schools (20%) that were aware of the scheme[footnote 3].
- Higher education institutions (69%) and further education colleges (62%) were more likely to have heard of the 10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps), whereas awareness of this guidance was lower among primary schools (38%) and secondary

schools (40%)[footnote 4]. Levels of awareness were in line with the 2024 survey.

- The National Cyber Security Centre's (NCSC's) Board Toolkit (https://www.ncsc.gov.uk/collection/board-toolkit) was recognised by more than half of higher education institutions (63%) and further education colleges (52%), compared with around one in four primary schools (28%) and secondary schools (27%). It is worth noting that the Board Toolkit, which is aimed at senior managers and governing bodies, had not been specifically promoted across educational institutions.

2.4 Identifying cyber security risks

As in 2024, the majority of the educational institutions had taken at least one of the actions shown in Figure 2.3 in the past 12 months to help identify cyber security risks. Primary schools still tended to have less sophisticated approaches, whereas further education colleges and higher education institutions tended to have more sophisticated ones. All types of educational institutions were more likely than businesses to have taken the various actions, continuing the trend from previous years.

Further education colleges and higher education institutions were specifically more likely than schools to carry out audits, penetration tests and invest in threat intelligence.

However, primary schools were more likely to have taken at least one of the actions in 2025 than they were in 2024 (up from 76% to 84%). In particular, primary schools were more likely to have conducted penetration testing (up from 15% to 23%).

There were no significant changes since 2024 among secondary schools. Overall, 86% of secondary schools had taken at least one of the actions.

In general, the levels of activity were similar among further education colleges and higher education institutions. However, higher education institutions were particularly likely to have conducted testing of staff awareness and response (94% compared to 77% of further education colleges) and to have invested in threat intelligence (72% compared to 58%).

Compared with the 2024 survey, higher education institutions were more likely to have tested staff awareness and response (up from 65% to 94%), but were less likely to have conducted risk assessment (down from 90% to 72%) and penetration testing (down from 81% to 69%). Further education colleges were also less likely to have conducted penetration testing (down

from 84% to 65%), but were more likely to have used specific tools designed for security monitoring (up from 70% to 92%).

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

Type of Activity	Primary schools	Secondary schools	Further education colleges	Higher education institutions	Business overall
Any of the listed activities	84%	86%	98%	100%	49%
Used specific tools designed for security monitoring	55%	60%	92%	94%	30%
Risk assessment covering cyber security risks	61%	65%	79%	72%	29%
Testing staff awareness and response (e.g. mock phishing)	47%	57%	77%	94%	18%
A cyber-security vulnerability audit	36%	46%	75%	72%	15%
Penetration testing	23%	31%	65%	69%	12%

Type of Activity	Primary schools	Secondary schools	Further education colleges	Higher education institutions	Business overall
Used or invested in threat intelligence	12%	26%	58%	72%	9%

Bases: 250 primary schools; 240 secondary schools; 52 further education colleges; 32 higher education institutions; 2,180 businesses overall

All types of educational institutions were more likely than businesses overall to say they had reviewed supplier-related risks to cyber security:

- Seven in ten higher education institutions (69%) said they had reviewed such risks posed by their immediate suppliers or partners, an increase from 2024 (up from 58%). By contrast, this proportion decreased among further education colleges (48%, down from 63% in 2024). Two in five secondary schools (38%) and one in four primary schools (26%, down from 35%) also said they had reviewed such risks. This compared to a minority (14%) of businesses overall.

Around three in ten higher education institutions (31%) said they had reviewed the risks presented by their wider supply chains, compared with 20% of secondary schools, 15% of primary schools and 8% of further education colleges (down from 26% in 2024). This compared to 7% of businesses overall.

Cyber security considerations when purchasing software
Just over half of schools (52% primary schools and 56% secondary schools), said they considered cyber security to a large extent when purchasing new software, as did just under seven in ten further education colleges (69%) and higher education institutions (66%). A further quarter of higher education institutions (25%) said they considered cyber security to some extent when purchasing new software, but that it was not a major concern (as did 17% further education colleges, 18% secondary schools and 17% primary schools).

Schools were more likely than further and higher education institutions to say that because they purchased new software from established or large companies that cyber security was not a major concern when purchasing (22% primary schools and 16% secondary schools vs. 10% further education colleges and 3% higher education institutions). A minority of all education institutions said they did not consider cyber security when

purchasing new software (1% primary schools, 3% secondary schools, 2% further education colleges, 3% higher education institutions).

Qualitative insights on supply chain risk

In the qualitative interviews, education institutions generally said they were confident about the cyber security practices of their suppliers. Some institutions had implemented systematic approaches to ensure their suppliers meet the necessary cyber security standards. This usually involved a set of questions that were asked of suppliers for assessment purposes.

> "We do have a minimum procurement process. We do have a basic set of security questions, and we try and look for certifications because it's the only way we will be able to demonstrate we've done some due diligence. So we are quite strict on that." **Higher education institution**

> "If there is any kind of incident, if it was a third party that caused it, we require them to go through our instant review process as well. So when it's a third party supplier or something goes wrong and we have an outage or anything like that, we say well you're going to need to go through our process as if it was an internal operation." **Higher education institution**

Some interviewees said they required suppliers to have Cyber Essentials accreditation, while others took this information into account in their assessment but did not make it a mandatory requirement.

> 'We ask them if they do [have Cyber Essentials]. But whether we adopt a supplier or not is a risk-based decision…It's not a complete "no", but it would contribute to increasing the risk, which would then be decided whether it's worth going with them or not.' **Higher education institution**

One interviewee acknowledged that they may need to introduce a more formalised system.

> "That's probably something that I need to chat with our different teams that actually do the main contact, that we should probably actually add that in, at least to say they should have Cyber Essentials." **Further education college**

Staff training and awareness raising

Cyber security training or awareness raising activities were less common in schools (albeit with majorities) than in further education colleges and higher education institutions. Two in three primary schools (66%) and seven in ten secondary schools (72%) had undertaken any such activities in the last 12 months. This rose to around nine in ten further education colleges (94%) and higher education institutions (91%). These figures were in line with the 2024 survey, although the longer-term picture showed an increase in activity among primary and secondary schools since 2021.

Cyber security planning and documentation

In terms of documentation, all four groups of educational institutions were far more developed than businesses overall, and much more akin to large businesses. Around eight in ten had a cyber security policy in primary schools (82%), secondary schools (81%) and higher education institutions (84%). The proportion was even higher in further education colleges (92%).

Business continuity plans covering cyber security also tended to be in place in most of these educational institutions. This applied to around three-quarters of primary schools (73%) and secondary schools (77%), and almost nine in ten further education colleges (88%) and higher education institutions (87%).

Similarly, at least seven in ten had a formal incident response plan: 71% of primary schools (up from 57% in 2024), 74% of secondary schools, 83% of further education colleges and 75% of higher education institutions (down from 87% in 2024).

Incident response planning in education institutions was also more sophisticated than in the businesses overall, as Figure 2.4 indicates. This applied in particular to having formal incident response plans, assigning roles and responsibilities to specific individuals, and having written guidance on who to notify and guidance on when to report incidents externally.

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

Type of Action taken	Primary schools	Secondary schools	Further education colleges	Higher education institutions	Busi over
Inform your governors of the incident	86%	81%	67%	69%	76%
Keep an internal record of incidents	78%	81%	83%	84%	58%

Type of Action taken	Primary schools	Secondary schools	Further education colleges	Higher education institutions	Busi over
Assessment of the scale and impact of the incident	67%	68%	69%	81%	56%
Formal debriefs to log any lessons learnt	72%	69%	69%	84%	54%
Inform your cyber insurance provider (among those with insurance)*	58%	50%	25%	0%	52%
Inform a regulator of the incidence when required	69%	60%	35%	44%	47%
Attempting to identify the source of the incident	57%	61%	69%	78%	45%
Roles and responsibilities assigned to specific individuals during or after incident	80%	83%	87%	87%	39%
Written guidance on who to notify	85%	85%	90%	81%	34%
Guidance on when to report externally (e.g. to regulators or insurers)	77%	78%	92%	84%	32%

Type of Action taken	Primary schools	Secondary schools	Further education colleges	Higher education institutions	Busi over
Formal incident response plan	71%	74%	83%	75%	23%
External communications and public engagement plans	48%	56%	81%	63%	16%
Used an NCSC-approved incident response company	21%	17%	19%	19%	15%

Bases: 250 primary schools; 240 secondary schools; 52 further education colleges; 32 higher education institutions; 2,180 businesses overall *Only asked of those that have cyber insurance (131 primary schools, 134 secondary schools, 40 further education colleges; 554 businesses overall; figures not shown for higher education institutions as base size is 18 which falls below the 30 threshold for reporting)

Compared with 2024, educational establishments were more likely to have taken various actions or have measures in place, specifically:

- Primary schools were more likely to have written guidance on who to notify (85% in 2025 compared to 76% in 2024), have guidance on when to report incidents externally (77% compared to 68%), have a formal incident response plan (71% compared to 57%) and to have used a NCSC approved incident response company (21% compared to 12%).
- Secondary schools were more likely to inform a regulator (60% in 2025 compared to 50% in 2024).
- Further education colleges were more likely to provide communications and public engagement plans (81% in 2025 compared to 65% in 2024) and to have guidance on when to report incidents externally (92% compared to 81%). However, further education colleges were less likely to have informed governors of the incident (67% in 2025 compared to 79% in 2024) and to have assessed the scale and impact of the incident (69% compared to 81%).
- Higher education institutions were more likely to have formal debriefs of lessons learned (84% in 2025 compared to 74% in 2024). However, higher education institutions were less likely to inform directors, trustees

or governors of the incident (69% in 2025 compared to 84% in 2024), to attempt to identify the source of the incident (78% compared to 90%) and to have a formal incident response plan (75% compared to 87%).

Insurance against cyber security breaches

A minority of primary schools (6%) and secondary schools (13%) have a specific cyber insurance policy. However, just under half of primary schools (47%) and secondary schools (43%) reported having cyber security cover as part of a broader insurance policy.

It is worth noting that many 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 (39% and 38% respectively)[footnote 5]. This compared to 20% of businesses overall not knowing. This highlights that cyber security is perhaps more siloed in schools and therefore considered separately from financial matters like insurance.

Further education colleges and higher education institutions were more likely to have specific cyber insurance policies (40% and 34% respectively) than primary and secondary schools. In addition, more than a third of further education colleges said they had cyber security cover as part of a broader insurance policy (37%), as did 22% of higher education institutions.

Technical rules and controls

The survey covered 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 (https://www.ncsc.gov.uk/collection/10-steps) or the Cyber Essentials scheme (https://www.gov.uk/government/publications/cyber-essentials-scheme-overview).

The government-endorsed Cyber Essentials scheme enables organisations to be independently certified for having met a good-practice standard in cyber security. Specifically, it requires them to enact basic technical controls across five areas:

- boundary firewalls and internet gateways
- secure configurations
- user access controls
- malware protection
- patch management (i.e., applying software updates).

Overwhelmingly, educational institutions had 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. Schools were notably weaker

in the area of patch management compared to further education colleges and higher education institutions: around half of primary schools (48%) had a policy to apply software updates within 14 days, as did just over half of secondary schools (56%, a significant decrease from 68% in 2024). This compared with nine in ten further education colleges (90%) and higher education institutions (91%).

Higher education institutions were less likely than in 2024 to have boundary firewalls and internet gateways in place (87% compared to 100%).

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

Rules or Controls	Primary schools	Secondary schools	Further education colleges	Higher education institutions	Busine overall
Up-to-date malware protection	92%	90%	100%	100%	77%
Firewalls that cover the entire IT network, as well as individual devices (boundary firewalls and internet gateways)	95%	95%	98%	87%	72%
Restricting IT admin and access rights to specific users (user access controls)	97%	98%	100%	91%	68%
Security controls on company-owned devices (e.g. laptops)	94%	97%	98%	97%	58%

Rules or Controls	Primary schools	Secondary schools	Further education colleges	Higher education institutions	Busine overall
A policy to apply software updates within 14 days (patch management)	48%	56%	90%	91%	32%

Bases: 250 primary schools; 240 secondary schools; 52 further education colleges; 32 higher education institutions; 2,180 businesses overall. (Text before parentheses used in questionnaire.)

As in previous years, primary schools were less likely than other educational institutions to have guest Wi-Fi networks (59% compared to 86% of secondary schools, 92% of further education colleges, and 87% of higher education institutions). Primary schools were also less likely to use a Virtual Private Network or VPN (55%), particularly when compared with higher education institutions (97%). Primary schools were more likely than the other institutions to only allow access via the school's own devices (73%), with higher education institutions much lower in this respect (19%). As noted in 2024, this may reflect the specific nature of dealing with young children.

It was also notable that primary schools were more likely to use cloud back-ups rather than other means for secure back-ups (89% compared to 52%), and this also applied to secondary schools (88% compared to 68%). Further education colleges commonly used both cloud back-ups and other means (81% compared to 83%), while higher education institutions were less likely to use cloud back-ups than other means for secure back-ups (66% compared to 81%).

Compared to 2024, the deployment of several controls and procedures had increased. Among secondary schools, there was an increase in the use of two factor authentication (up from 71% to 80%). Further education colleges were more likely to use a virtual private network or VPN (up from 70% to 83%).

Among higher education institutions, there was a shift away from cloud back-ups (down from 81% to 66%) towards other means for secure back-ups (up from 68% to 81%). Higher education institutions were less likely to report having an agreed process for staff to follow with fraudulent emails or websites (down from 97% to 84%).

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

Additional Rules or Controls	Primary schools	Secondary schools	Further education colleges	Higher education institutions
A password policy that ensures that users set strong passwords	92%	94%	100%	91%
Backing up data securely via a cloud service	89%	88%	81%	66%
Only allowing access via organisation-owned devices	73%	65%	56%	19%
An agreed process for staff to follow with fraudulent emails or websites	93%	93%	100%	84%
Backing up data securely via other means	52%	68%	83%	81%
Rules for storing and moving personal data securely	90%	90%	83%	69%
Any Two-Factor Authentication (2FA) for networks/applications	78%	80%	94%	100%
Separate Wi-Fi networks for staff and visitors	59%	86%	92%	87%
A virtual private network, or VPN for staff connecting remotely	55%	65%	83%	97%

Additional Rules or Controls	Primary schools	Secondary schools	Further education colleges	Higher education institutions
Monitoring of user activity	88%	91%	88%	78%

Bases:250 primary schools; 240 secondary schools; 52 further education colleges; 32 higher education institutions; 2,180 businesses overall

Outsourcing cyber security
As reported in 2024, outsourcing cyber security was more common among primary schools than other educational institutions. Eight in ten primary schools (79%) said an external provider managed their cyber security for them, compared with 57% of secondary schools, 33% of further education colleges and 41% of higher education institutions (up from 26%).

2.5 Implementing the 10 Steps to Cyber Security

The government's 10 Steps to Cyber Security (https://www.ncsc.gov.uk/collection/10-steps) guidance sets out a comprehensive risk management regime that organisations can follow to improve their cyber security standards. It is not, however, an expectation that organisations comprehensively apply all the 10 Steps as 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 as 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.

There have been some changes in 2025 compared with 2024:

- primary schools were more likely to have undertaken action in incident management (81% in 2025 compared to 70% in 2024), while they were less likely to have taken action in supply chain security (29% compared to 39%)
- secondary schools were more likely to have undertaken action in identity and access management (80% in 2025 compared to 71% in 2024) but

were less likely to have undertaken action in vulnerability management (56% compared to 68%)

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 two 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.	61%	65%	79%	72%
2 **Engagement and training** - Organisations that train staff or do mock phishing exercises	66%	72%	94%	91%
3 **Asset management** - Organisations that list of critical assets	70%	69%	90%	78%
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	99%	98%	100%	100%
5 **Vulnerability management** - Organisations that have a patching policy and at least one of the following: undertake	48%	56%	90%	91%

Step description and how derived from the survey	Primary	Secondary	Further	Higher
vulnerability audits, penetration testing, update anti-malware, or have a policy covering SaaS				
6 **Identity and access management** - Organisations that restrict admin rights or password policy or two factor authentication	78%	80%	94%	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	96%	98%	98%	97%
8 **Logging and monitoring** - Organisations with monitoring tools or if log breaches and had a breach	90%	92%	98%	100%
9 **Incident management** - Organisation with incident response plans or formal debriefs	81%	80%	90%	81%
10 **Supply chain security** - Organisations that monitor risks from suppliers or wider supply chain	29%	42%	48%	69%

Overall, this table shows, as it broadly did in 2024, that the areas that were less well covered among educational institutions were:

- risk management
- asset management
- supply chain security

In addition, there were areas that were less well covered in schools in particular (rather than further education colleges and higher education institutions):

- engagement and training
- vulnerability management

Looking at these 10 Steps together, nearly all educational institutions had taken action on at least five of these steps. However, there is still some progress to be made 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

Number of Actions taken	Primary schools	Secondary schools	Further education colleges	Higher education institutions	Business overall
Undertaken action on five or more of the 10 Steps	91%	91%	100%	100%	39%
Undertaken action on all of the 10 Steps	8%	18%	33%	47%	3%

Bases: 250 primary schools; 240 secondary schools; 52 further education colleges; 32 higher education institutions; 2,180 businesses overall

Appendix A: Further information

A1. The Department for Science, Innovation and Technology and the Home Office 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.

- Alice Stratton, Ipsos
- Nada El-Hammamy, Ipsos
- Eva Radukic, Ipsos
- Jono Roberts, Ipsos
- Hannah Harding, Ipsos

- Jayesh Navin Shah, Ipsos

A2. The Cyber Security Breaches Survey was first published in 2016 (https://www.gov.uk/government/publications/cyber-security-breaches-survey-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 (https://www.gov.uk/government/collections/cyber-security-breaches-survey). This includes the full report and the technical and methodological information for each year.

A3. The lead DSIT analyst and responsible statistician for this release is Saman Rizvi. The lead Home Office analyst for this release is Eleanor Fordham. For enquiries on this release, please contact DSIT at cybersecurity@dsit.gov.uk.

A4. 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/ (https://www.statisticsauthority.gov.uk/code-of-practice/). Details of the pre-release access arrangements for this dataset have been published alongside this release.

A5. This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252.

---

1. Further detail on the margins of error are included the separately published Technical Annex (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-technical-report) in section 1.6
2. Supports innovative learning and teaching within higher education, underpins collaborations with research partners and enables business efficiencies.
3. 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.
4. The 10 Steps to Cyber Security guidance aims to summarise what organisations should do to protect themselves.
5. 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.