Cyber security posture survey results 2020:

A snapshot of the cyber security landscape in HE and FE

TLP: GREEN

This presentation is marked TLP GREEN – this means that recipients may share information with peers and partner organisations within their sector or community, but not via publicly accessible channels.

Key headlines I

Cybersecurity structure and operations:

- Cyber security continues to be given high priority within institutions, evidenced by inclusion on risk registers and reporting of security risks/resilience to executive boards.
- The numbers of organisations with dedicated cyber security staff has risen this year, with implementation of SIEM systems becoming more common. Formalised 24/7 cover remains less common, with out of hours response to cyber security incidents provided on a less formal, best-efforts basis.

Cybersecurity posture and protection:

- Perceptions of organisation protection have dropped slightly in HE and increased in FE in the last year, although the overall mean posture score (on a scale of 1-10) has increased for both sectors. This could be driven by the challenges of COVID-19 this year, including the need to support the virtualisation of organisations and raise awareness of staff and students working remotely. Responses also indicate that, while improvements have been made and processes implemented, organisations are aware of the need to improve these processes in order to fully protect themselves against new threats.
- There have been big increases in the proportion of HE organisations achieving all three cyber security certifications, and of FE gaining Cyber Essentials and Cyber Essentials Plus. This progress has been largely driven by government policies and funding requirements, e.g. Cyber Essentials is a requirement of the Scottish Government, arising from the Scottish Cyber Resilience Public Sector Action Plan and the Education and Skills Funding Agency requires FES providers to progress to Cyber Essentials Plus for the 2021/22 funding year. Anecdotally we understand that organisations are also seeing accreditation as a key tool for organisational protection. The importance of multifactor authentication is also evident, with high numbers implementing or planning to introduce this over the next year.
- Managing the human element of cyber security is becoming a greater priority, as evidenced by greater numbers of organisations implementing training for staff, and comments identifying accidental data breaches as a threat.

Key headlines II

Cyber security threats and priorities:

- Following the trend of the last two years, phishing/social engineering is the top threat identified by both HE and FE, followed by ransomware/malware.
- Phishing/social engineering also emerges as the main cyber security incident experienced by both HE and FE organisations. With accidental data breaches also mentioned in open ends, and the increase of organisations providing training to staff, it appears human error remains of concern for both HE and FE.
- Outside of these areas, organisations report limited experience of cyber security incidents and identify staff time as the most common impact of cyber security incidents. However, proactive management and monitoring of cyber threats continues, reflected by the numbers of organisations using third party services to gain insight/intelligence on current/emerging threats.

Background & Methodology

Background I

The cyber security landscape continues to be a challenging and changing environment with a large amount of varied attacks impacting universities and colleges including an increase in ransomware attacks causing severe disruption. And, according to the NCSC, interest from state-backed actors continues to be a threat to research in the UK[1].

Cyber security, therefore, remains a key priority area for Jisc and one that has gained even more importance during the Coronavirus (COVID-19) pandemic. At this time, it is vital that we have a good understanding of our members' needs, expectations and current provision, in order to provide relevant cyber security products and support.

This survey has been run in a similar format for the last three years. This year's survey aims to get an up-to-date picture from both HE and FE organisations on their cyber security posture and priorities, and to track any changes over time.

The findings will be used to inform effective roadmap development and product planning at Jisc over the coming years.

Business objective: To understand more about HE and FE organisations' cyber security posture and priorities, so Jisc can effectively prioritise security products and support for our members and identify additional gaps for development

Research Objectives:

- Understand organisations' current cyber security staffing
- Understand organisations' current cyber security provision
- Explore organisations' perceptions of current protection levels and areas for improvement/key risk areas
- Understand what certifications and training organisations deploy
- Explore perceptions of future cyber security threats
- Explore reactions to potential new product areas and Jisc's provision in these areas

[1] See https://www.ncsc.gov.uk/blog-post/trusted-research and https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

Background II

The results of this research were shared through our CISO forum, our HE IT Leaders Focus Group, the AoC Technology Special Interest Group, and with ucisa Trustees and Leadership Council as part of a review process. This has allowed us to:

- Gather expert opinion on the findings, further informing our understanding of cyber security priorities and the context surrounding the survey responses
- Demonstrate up-to-date knowledge of our membership, positioning Jisc as experts in the field
- Collaborate with our members on cyber security, so they feel valued and listened to

This report includes commentary from the peer review process.

As with previous years surveys, we also plan to present the key findings from the survey at the Jisc cyber security conference 2020.

Method and sample

An online survey was sent to Jisc security contacts including CIOs, IT Directors, Head of IT, Chief Information Security Officers, Network Managers and Security Managers within HE and FE

100
Completes
(2019 n=122)

Type of organisation	2020 sample		2019 sample	
HE	51	31% (51/164)	64	38% (64/167)
FE	47	13% (47/367)	55	18% (55/310)
Other*	2		3	

Notes on the data:

- This document covers analysis of HE and FE responses only (n=98)
- This report aims to give an institutional view. Where the same organisation submitted multiple survey responses, only the most senior or most relevant staff member's response was included. 19 duplicate responses were removed from the dataset
- 'Other' organisations in 2020 were research and commercial organisations
- Organisations have been classified using information in the Jisc CRM

Sample breakdown by FE/HE organisation type

98

Completes from HE and FE

N= 51 HE

Type of organisation	N=	%
Large (> 20,000 students)	11	22%
Small (< 20,000 students)	40	78%
No info available	/	/

N= 47 FE

Type of organisation	N=	%
Large (> 10,000 learners)	20	43%
Small (< 10,000 learners)	25	53%
No info available	2	4%

Where information was available, organisations were classified by size based on number of total students*. Where relevant, differences in responses have been pulled out based on size classifications, however sample sizes are small and so any differences in response are indicative only

*Data Sources: HE student numbers= HESA 17/18, FE Student numbers= Department of Education

COVID-19

Impact of COVID-19

This year's survey was distributed in June/July 2020, as universities and colleges were faced with the challenges of the COVID-19 pandemic. Both HE and FE saw additional work to support the rapid virtualisation of their organisations and to support the impact of staff and students working remotely, for example expanding VPN capacity and managing the security of devices remotely.

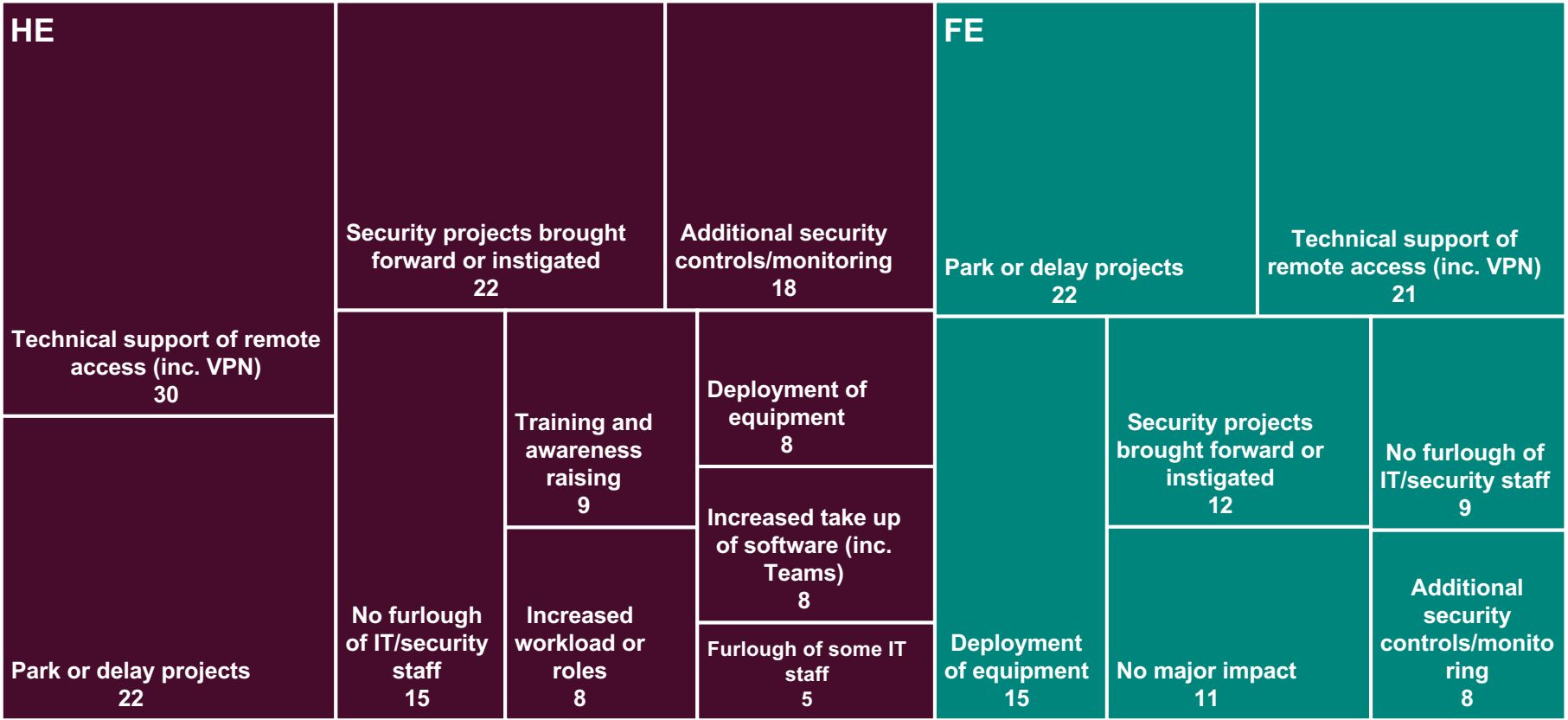
While some IT projects were delayed due to campus closure or changing priorities, both FE and HE organisations reported that security related projects, including implementation of MFA, had been brought forward or instigated. With cyber security seen as a priority, minimal staff had been furloughed and additional security controls or monitoring had been necessary. There are mentions of increased awareness raising and training for staff and students.

We have put in place a number of enhancements to our security posture in light of the covid-19 pandemic including cloud management of client devices, removal of legacy email protocols, enhanced application and desktop virtualisation, spike licensing of VPN. We have also commissioned a further round of enhancements for the next 6 months. HE Institution

We have started to put in extra controls because of Covid 19 and home working, but predominantly on college devices. Updated our procedures on use of personal mobile devices. Increased investment in malware and phishing protection. A number of our projects have been delayed due to Covid where external contractors are required onsite. FE College

Q9. In terms of cyber security, what impact has COVID-19 had within your organisation?

Summary of COVID-19 impact: >5 mentions

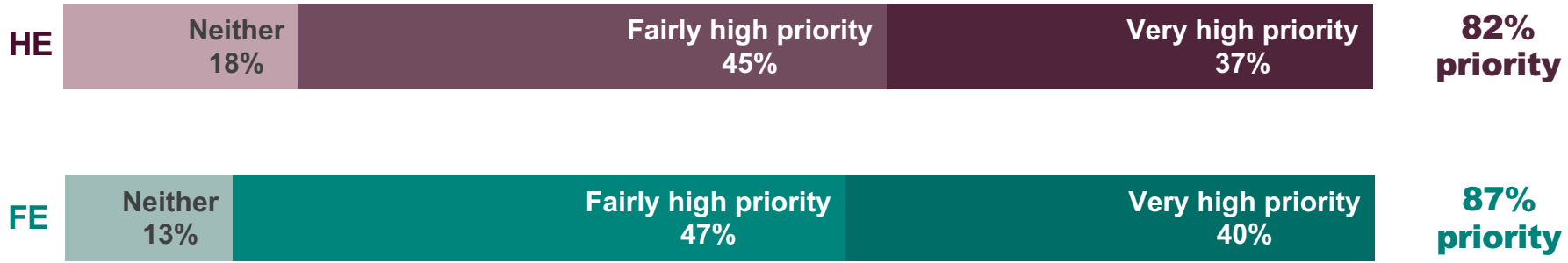


Q9. In terms of cyber security, what impact has COVID-19 had within your organisation?

Cyber security governance, structure & operations

Priority given to cyber security

82% of HE and 87% of FE institutions indicate that priority is given to cyber security within their institution. For those that indicate cyber security is neither a high nor low priority, the question is why not? Although we do not have open-ended responses to expand on the level of priority given, the majority of those who chose 'neither' rated overall cyber security protection within their institution in the 5-7 range or lower on a scale of 1-10 (see slide 30). Their comments indicate that costs and resource, organizational culture, limited understanding of security by staff and students, and a need to implement additional products and processes are issues that need to be addressed.



Q10.What level of priority is given to cyber security within your organisation?

Cyber security on risk register

Nearly all HE (88%) and FE (87%) institutions indicate that cyber security appears on their risk register. If we exclude 'don't know' answers, this rises to 96% for HE and 95% for FE. In comparison to 2019, the number of FE institutions answering 'yes' has risen by 9 percentage points (from 78% in 2019) suggesting that this is gaining stronger strategic and operational importance within this sector.

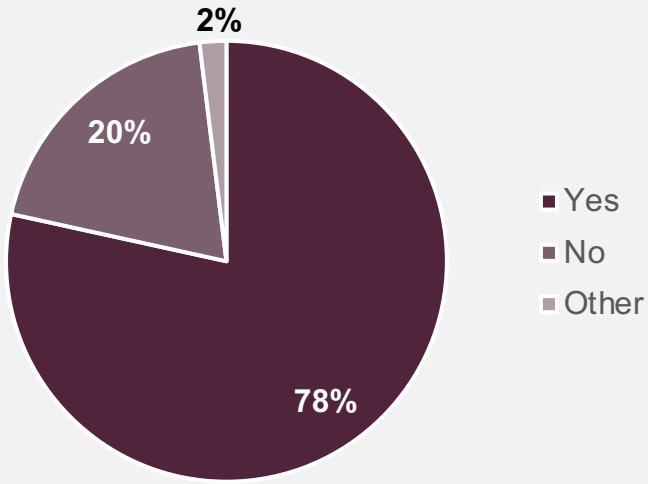
HE	FE
88%	**87%**
cyber security appears on organisations risk register	cyber security appears on organisations risk register
82% large HE 90% small HE	95% large FE 80% small FE

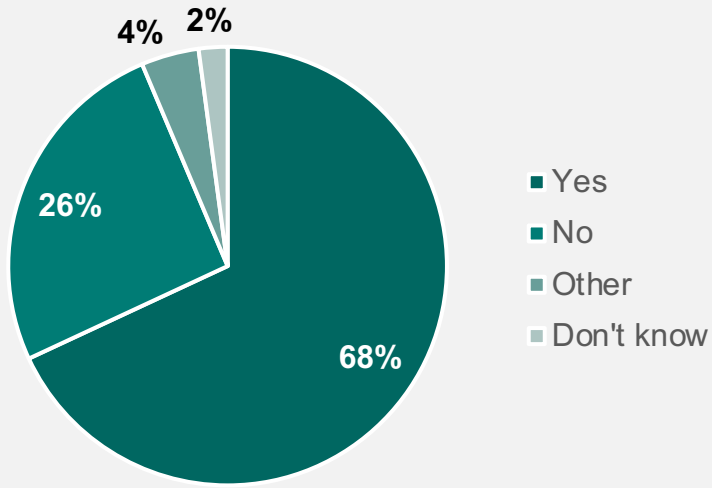
Q11. Does cyber security appear on your organisations risk register?

Reporting to executive management

Over ¾ of HE institutions (78%) and over ⅔ of FE colleges(68%) institutions indicate that they regularly report cyber security risks and resilience to their executive board. For the three who selected 'other', one respondent was a member of the senior management team and met regularly with the team to discuss, one reported to the risk management team, and one reported on an occasional basis.

% regularly report cyber security risks to executive board





Q12. Do you or a colleague regularly report on cyber security risks and resilience to your executive board?

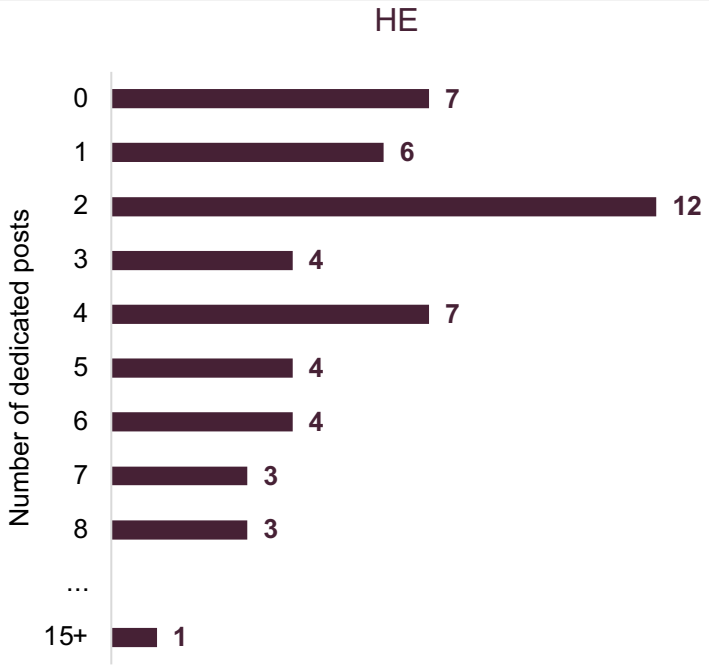
Cyber security staffing summary

Type of organisation	Have dedicated cyber security roles within organisation	Have staff available 24x7 to respond to security incidents	Have dedicated team performing incident response or active security monitoring (Yes total)
	2020	2020	2020
HE	**86%** (73% 2019)	**22%** (16% 2019)	**59%** (44% 2019)
FE	**28%** (11% 2019)	**11%** (9% 2019)	**25%** (18% 2019)

Q13. Do you have any dedicated cyber security roles in your organisation?
Q16. Do you have a dedicated team that performs incident response or active security monitoring…?
Q18. Do you have staff available 24x7 to respond to security incidents?

Number of dedicated cyber security posts

44 (86%) HE and 13 (28%) FE organisations indicate that they have dedicated cyber security posts. In HE, the majority of those with dedicated roles have two posts within the institution, while those in FE are most likely to have one dedicated post.



In FE, one organisation responded 'don't know' and one declined to answer. n=45

Q14. How many dedicated cyber security posts do you have at each role?

Dedicated cyber security roles

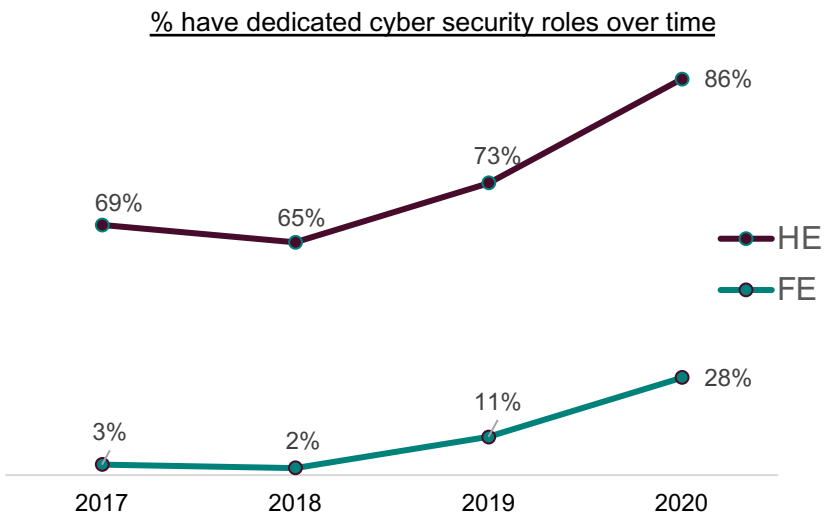
In the last year, the proportion of HE and FE organisations reporting they have dedicated cyber security roles in their organisation has increased by 13 percentage points in HE to 86% and 17 percentage points to 28% in FE.

HE

86% have dedicated cyber security roles

FE

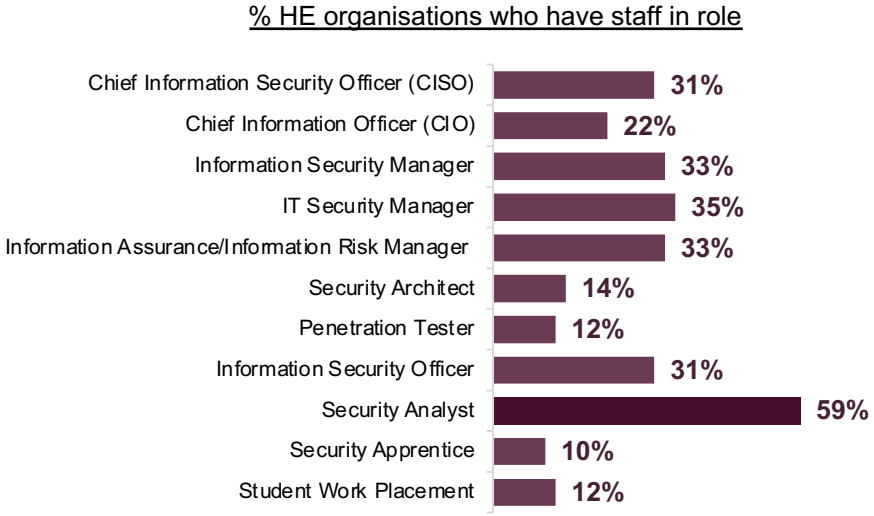
28% have dedicated cyber security roles



Q13. Do you have any dedicated cyber security roles in your organisation? These roles can be staff on the payroll, contract staff or third parties providing a cyber security function for your organisation

Dedicated cyber security roles HE

Within HE, Security Analyst, IT Security Manager, Information Security Manager, Information Assurance, and Information Risk Manager are most common. Comments suggest that some roles are combined within institutions (e.g. engineer and analyst roles overlap), or the responsibilities are subsumed within other roles (e.g. Network Analysts).



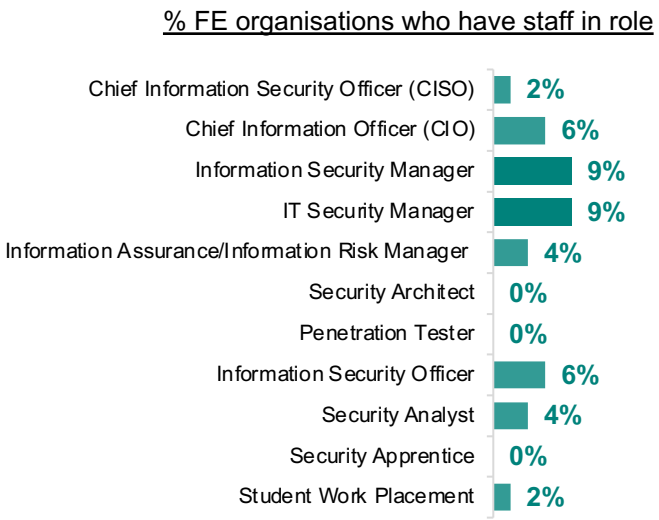
Other dedicated cyber security roles:

- CISO via Scottish shared service
- CIO is the CISO
- Cyber Security Manager
- Cyber Security Specialist
- Head of Information Security
- SOC Apprentice
- Head of Strategy Architecture and Cyber Security
- Information Security Engagement Lead/Officer
- Faculty Information Security Coordinator
- Cyber Security Technician
- Cyber Security Programme/Project Manager

Q14. How many dedicated cyber security posts do you have at each role (or equivalent) below?
Q15. Are there any other dedicated cyber security posts within your organisation?

Dedicated cyber security roles FE

Fewer FE colleges have dedicated security roles (11%), but the year-on-year data suggest that they are becoming more common at manager level, particularly Information Security Manager (4% in 2019) and IT Security Manager (5% in 2019).



Other dedicated cyber security roles:

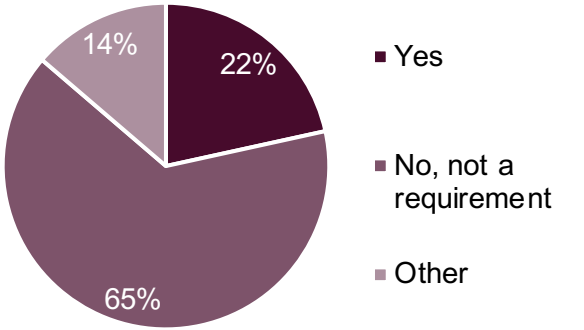
- CISO via Scottish shared service
- Data Protection/Risk Manager
- ICT Security Engineer

Q14. How many dedicated cyber security posts do you have at each role (or equivalent) below?
Q15. Are there any other dedicated cyber security posts within your organisation?

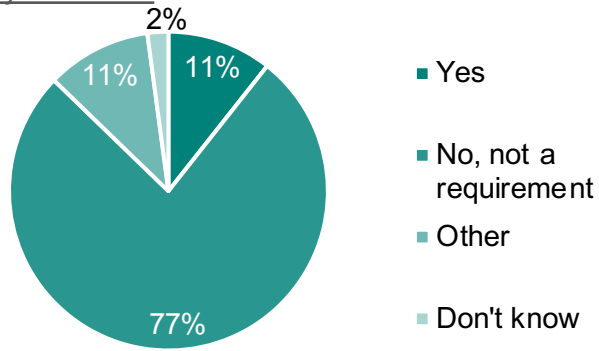
Availability of staff to respond 24/7

In HE, 22% of organisations have staff available 24/7 to respond to security incidents, rising to 36% in larger institutions. A further 14% have another form of provision. 11% of FE organisations indicate that they have staff available 24/7, with a further 11% having another form of provision. Analysis of open comments suggest this question has been interpreted in different ways, with some seeing this as a dedicated 24/7 team, others stating 'on-call' rotas, and some indicating that staff are contactable. Availability of staff to respond to incidents is likely to be more widespread than these data suggest, although formalised 24/7 arrangements may be less common.

% have staff available 24/7 to respond to security incidents



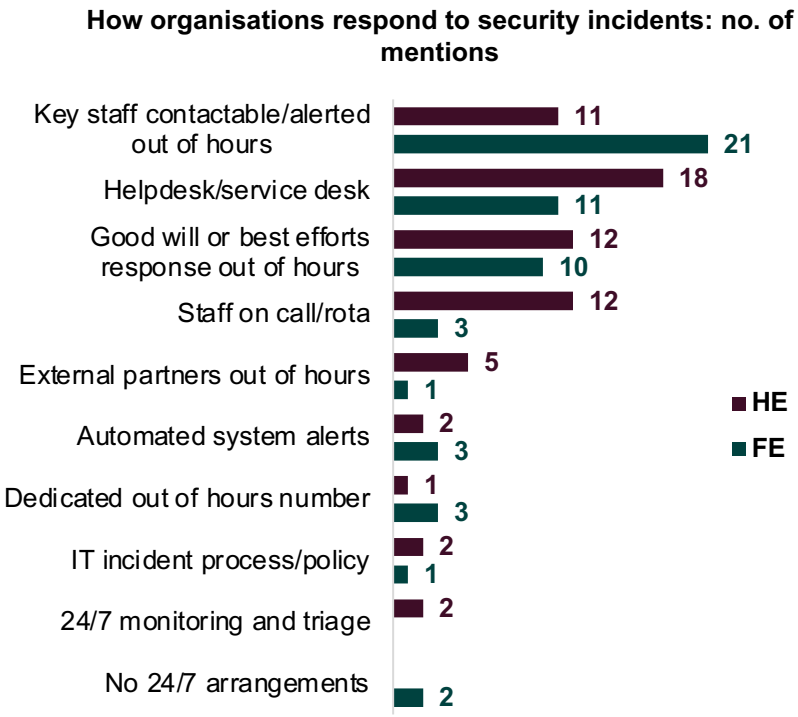
	Large HE	Small HE
Yes	36% large HE	18% small HE
No, not a requirement	55% large HE	67% small HE
Other	9% large HE	15% small HE



	Large FE	Small FE
Yes	5% large FE	12% small FE
No, not a requirement	80% large FE	76% small FE
Other	15% large FE	8% small FE

Q18. Do you have staff available 24/7 to respond to security incidents?

Response to security incidents



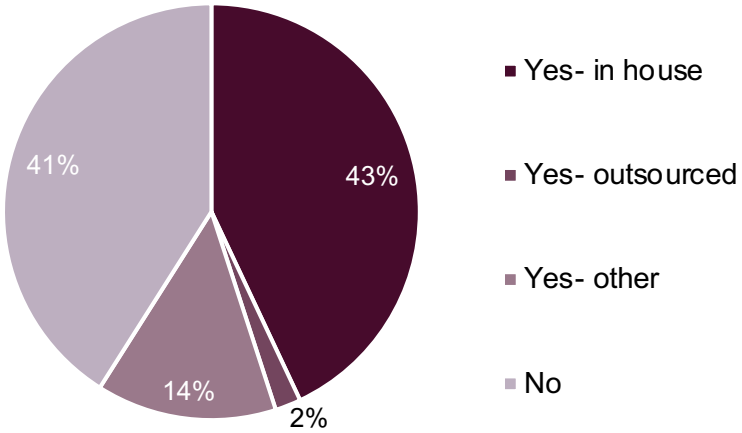
- **In HE, security incidents are most likely to be routed through an IT helpdesk, and forwarded to staff on call out of hours.**
- **FE comments also refer to IT helpdesks, but incidents are more likely to be escalated to key security staff that are contactable out of hours on a less formal basis.**
- **There is variation in how organisations refer to staff availability. Comments suggest that the key distinction made is around whether the organisation has a formalised on-call process with staff on a rota, or whether key staff are alerted or contactable out of hours but not "contractually required" to do so. 6 of the 11 HE institutions who indicate they have staff available 24/7, refer to having staff on-call in the comments.**
- **For both HE and FE, a large number of comments mention out of hours response being on a best-efforts or voluntary basis, with institutions relying on good will. For the 21 comments in FE that refer to staff being contactable out of hours, 6 of these mention this being a good will arrangement.**

Q19. Please tell us more about how you respond to security incidents

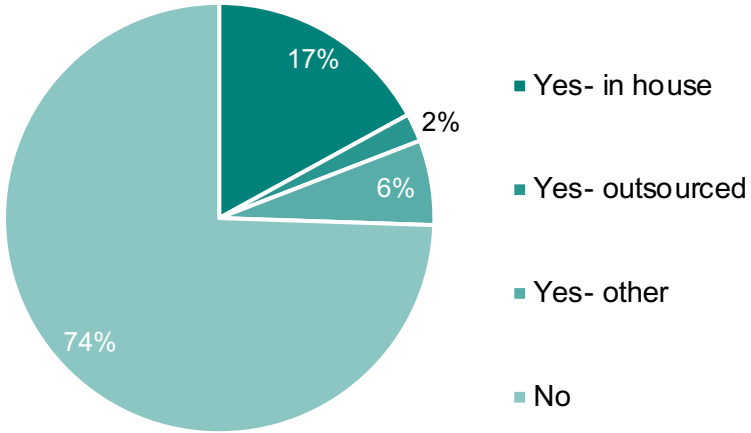
Dedicated CSIRT and SOC Teams

43% of HE organisations claim to have an in-house CSIRT or SOC team, with a further 2% outsourcing this. The proportion of FE organisations with a CSIRT or SOC team in house is lower at 17%.

% HE who have CSIRT or SOC team



% FE who have CSIRT or SOC team



Q16. Do you have a dedicated team that performs incident response or active security monitoring, such as a Computer Security Incident Response Team (CSIRT) or Security Operations Centre (SOC)?

Operation of dedicated CSIRT and SOC Teams

As also identified in 2019, while 43% of HE and 17% of FE organisations report in-house CSIRT or SOC teams, comments suggest that some organisations have staff that respond to incidents as part of other security roles. In 2020, the proportion of organisations with a dedicated CSIRT/SOC team is again likely to be lower than indicated on the previous slide.

HE

Kept on a retainer for call off when needed

Incident response is handled in house, as is some of the monitoring, but the SOC is outsourced.

Composed of Head of IT, Security Architect, Data Protection officer, Systems Team Lead. Alerts via WhatsApp and Microsoft Teams

Dedicated Cyber Security team who conduct CSIRT activities alongside the Governance, Risk and Compliance and Strategic aspects of Cyber Security

A CSIRT team has just been formed to deal with organisation wide security incidents, the exact details of how this will function is still being determined.

Existing information security team undertakes this exercise and we have developed incident response plans and guidance

FE

It's in house and within IT team - they monitor and deal with issues and run training - including externally we have used purplephish to raise staff level of awareness to risks

Outsourced to IT support provider.

CSIRT, involving members of the Digital Services team and our CISO. We have yet to run a TTX [Incident Response Tabletop Exercise] yet though

"The in-house CSIRT team is made up of the IT Services manager, Lead Security officer, IT Security Officer, Infrastructure & User / Systems Support Officer and Team Leader. We response to internal incidents - but mainly to Jisc / Janet notifications

managed within existing IT resource.

Q17. Please tell us more about how this team operates and, if outsourced, who to.

Implementation of SIEM

47% of HE institutions indicate they have implemented a SIEM system, an increase of 19 percentage points from 2019 (28%). Splunk and LogRhythm are the most commonly used. Amongst FE, the proportion who indicate they have implemented a SIEM is lower at 11% with a range of different suppliers used. As with 2019, inclusion of some non SIEM systems suggests some confusion about what constitutes this type of system.

HE

47%

(45% adjusted*)

Implemented a Security Information and Event Management System (SIEM)

Systems implemented:

- Splunk (5)
- LogRhythm (3)
- AlienVault (2)
- ELK Stack (2)
- Azure Sentinel trial (2)
- Rapid7 InsightIDR (2)
- Foresite (1)
- LogPoint (1)
- *Greenbone** (1)
- Cybanetix (1)
- Exabeam (1)
- IBM Qradar (1)
- MS ATA (1)
- MS Azure Security Center (1)

FE

11%

(9% adjusted*)

Implemented a Security Information and Event Management System (SIEM)

Systems implemented (1 mention each):

- *Sophos and Fortigate**
- ELK Stack
- AlienVault
- Azure Sentinel
- Manageengine Eventlog Analyzer

Q20. Have you implemented a Security Incident and Event Management system (SIEM)? Which SIEM have you implemented? *Not SIEM systems - adjusted figure also provided with these removed

Value of SIEM

Those with a SIEM are somewhat positive about their experience, although four HE institutions expressed dissatisfaction. For those who feel they get value from their SIEM, this is driven by costs, functionality, responsiveness, rapid/timely reporting of threats, ease of use/automation of workflows, and vendor support. Those that do not feel they get value cite a lack of effectiveness and problems with implementation.

HE

62%*

Feel get value from SIEM

Clarity of information, real-time responsiveness, agility.

Fantastic support from the vendor, ease of use, highly tunable and has proven valuable in investigations.

It gives us centralised log collection, which wasn't available previously. We also get user and entity behaviour analytics, which helps to reduce the workload on the security team.

FE

40%* (2 out of 5)

Feel get value from SIEM

*small sample of SIEM users

Excellent results with one 1 week of install and refinement. Information which was now available to IT Services.

Q21. Do you feel you get value from your SIEM?
Q21a. What factors have influenced this assessment of your SIEM?

Rationale for not implementing SIEM

In both HE and FE the most common reason indicated in the comments was that they are considering or are in the process of implementing a SIEM, indicating the growing importance of these systems. Cost and resource implications are given as key reasons for not implementing, particularly in FE, along with the need to focus on other priorities and the lack of time or resource.

HE

- Being considered or in progress n=11
- Lack of resource/time n=6
- Other priorities take precedence n=5
- Cost/lack of budget n=4
- Procedures/elements in place n=2
- Lack of expertise and training n=1

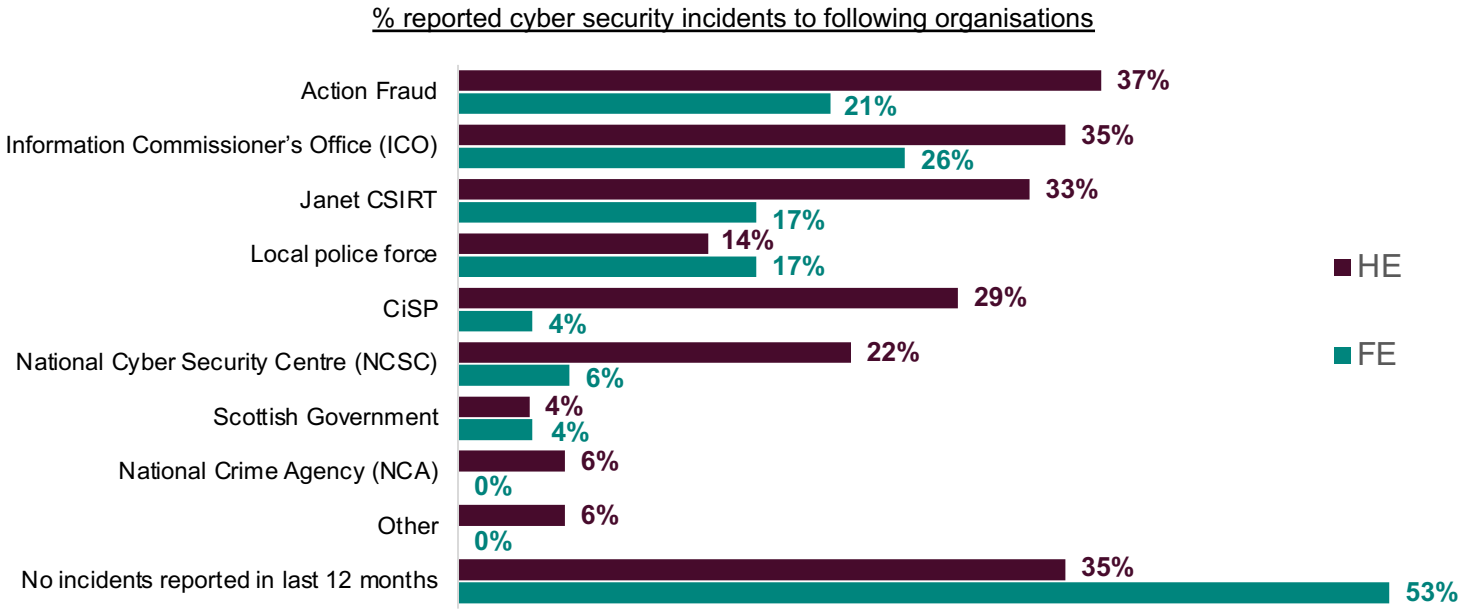
FE

- Being considered or in progress n=11
- Cost/lack of budget n=10
- Lack of resource/time n=8
- Procedures/elements in place n=5
- Other priorities take precedence n=4
- Lack of expertise and training n=1
- Unaware of systems n=1

Q20b. Please tell us why your organisation has not implemented a SIEM?

Reporting of cyber security incidents

Organisations were most likely to report incidents to Action Fraud, ICO and Janet CSIRT, with FE also reporting to the local police force. HE were more likely to report incidents, with over half of responding FE colleges (53%) reporting no incidents within the last 12 months, in comparison to 35% of HE institutions. Only 2 (18%) large HE organisation reported no incidents in the last 12 months.



Q22. In the last 12 months have you reported cyber security incidents to any of the following external organisations?

Cyber security posture

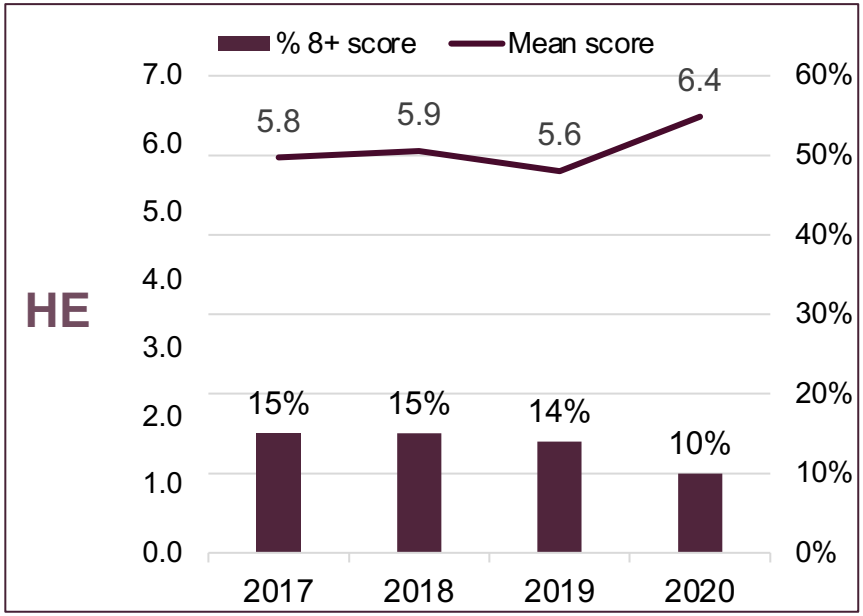
Cyber security protection perceptions

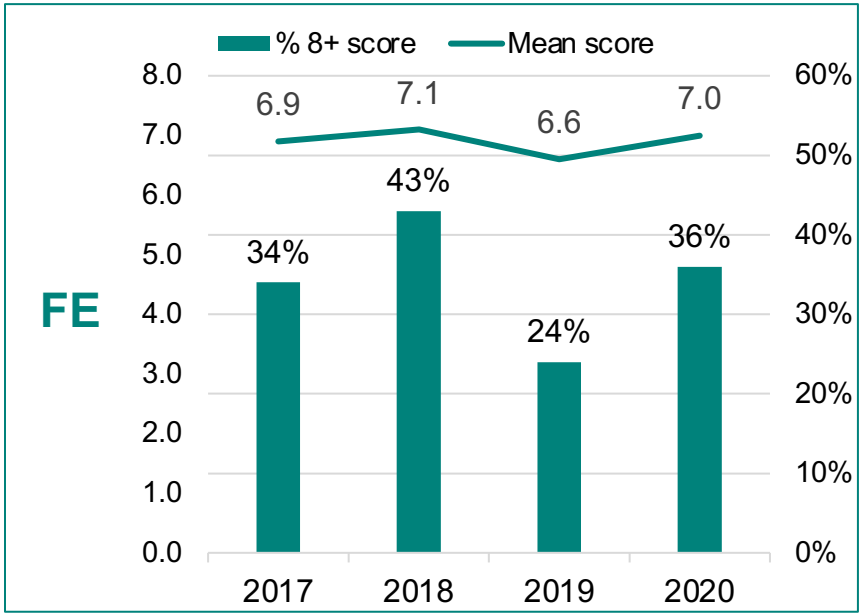
Within HE, perceptions of cyber security protection are not high, with only 10% (5 institutions) scoring their organisation as 8+ and a mean score of 6.4/10. The majority of HE organisations rate their protection at '7', reflecting comments that additional measures/processes and better awareness amongst staff/students are needed to feel fully protected. Perceptions are more positive in FE with 36% scoring their organisation as 8+, and a mean score of 7.0.

Q23. Thinking about cyber security, how well do you feel your organisation is protected?

Cyber security protection perceptions over time

Whilst perceptions of cyber security protection have risen in FE, they have dipped slightly in the last year in HE; 10% scored 8+ in 2020 compared to 14% in 2019 on a 10 point scale of how well protected they feel their organisation is. However, both HE and FE have seen a rise in their overall mean score in 2020, indicating that work to implement appropriate systems and processes is having an impact on perception.





Q23. Thinking about cyber security, how well do you feel your organisation is protected?

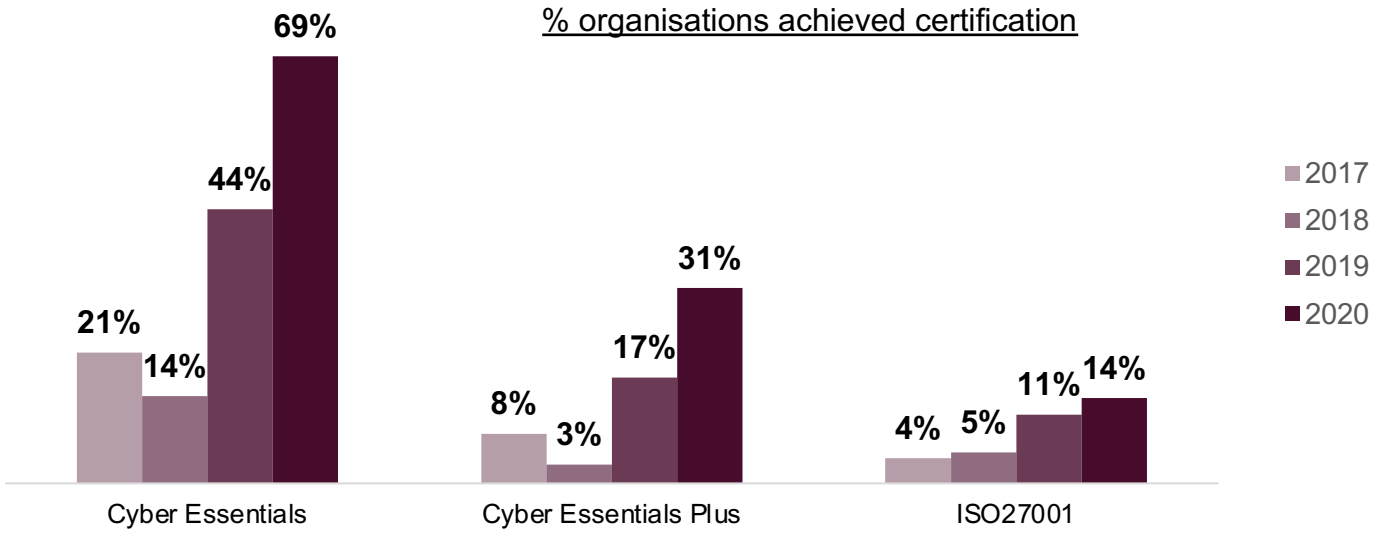
Protection perception rationale

	Rationale scores 1-4	Rationale scores 5-7	Rationale scores 8-10
HE	• Based on accreditation or results of audits/assessments (1) • Understanding and awareness of staff students (1) • Culture/prioritisation within organisation (1) • More work to do – generic (1) • Costs and lack of resource (1) • Need to implement additional processes or products (1)	• Measures in place but need to implement additional processes or products (e.g. MFA/SIEM) (15) • Understanding and awareness of staff/students (10) • Culture/prioritisation within organisation (8) • Appropriate systems and processes in place (6) • Costs and lack of resource (5) • Continuous monitoring and improvements (5) • More work to do – generic (4) • Based on accreditation or results of audit/assessments (3) • Fast moving landscape/new threats (3) • Legacy technology (2)	• Appropriate systems and processes in place (4) • Continuous monitoring and improvement (3) • Good understanding and awareness of staff/students (1) • More work to do – generic (1)
FE	• More work to do - generic (1) • Costs and lack of resource (1)	• Measures in place but need to implement additional processes or products (e.g. MFA/SIEM) (8) • Costs and lack of resource (6) • More work to do – generic (5) • Understanding and awareness of staff/students (4) • Appropriate systems and processes in place (4) • Culture/prioritisation within organisation (2) • Need to complete accreditation (2) • Based on accreditation or results of audit/assessments (2) • Continuous monitoring and improvements (1) • Legacy technology (1) • Results of pen testing (1)	• Appropriate systems and processes in place (11) • Continuous monitoring and improvements (8) • Improving understanding and awareness of staff/students (3) • Culture/prioritisation within organisation (3) • Costs and lack of resource (3) • Based on accreditation or results of audit/assessments (3) • Results of pen testing (2) • More work to do – generic (1)

Q24. Please tell us why you gave your organisation a score of x?

Cyber security certifications in HE over time

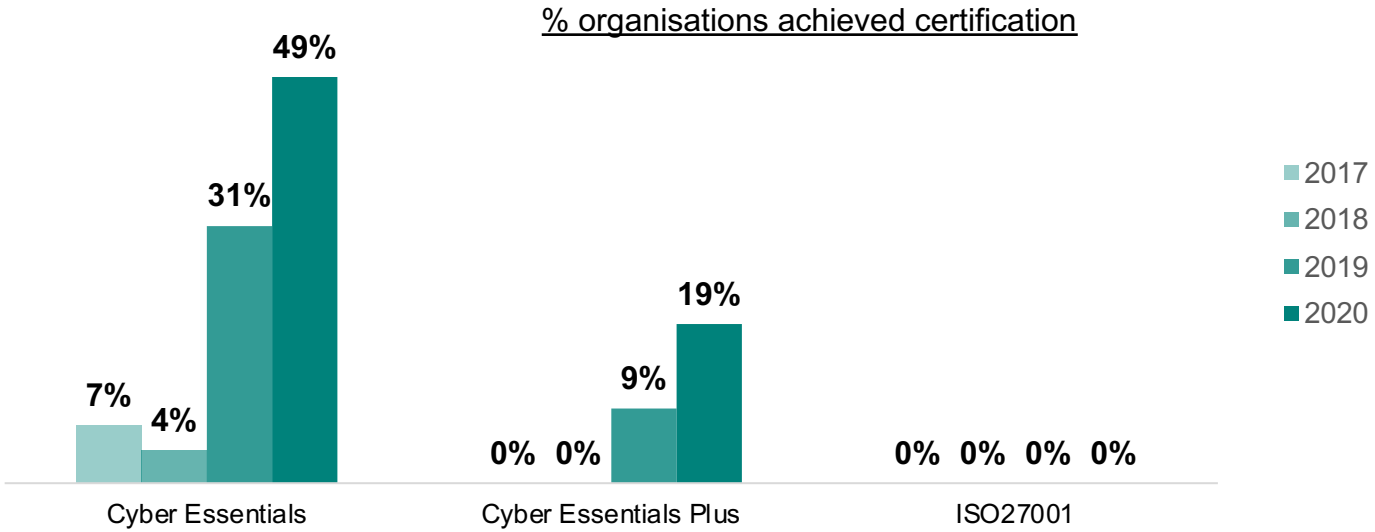
For the third year, there have been increases in the proportion of HE organisations achieving all three cyber security certifications, indicating their continued importance for members. While only 14% have completed ISO27001, a further 24% were considering completing this, suggesting we may see a rise in 2021.



Q25. Does your organisation have any of the following security certifications?

Cyber security certifications in FE over time

Both Cyber Essentials and Cyber Essentials Plus have seen a large rise in completion levels in the last year amongst FE organisations. For the second year in a row, we have seen a jump in Cyber Essentials certifications, which is likely to lead to continued interest in the Plus certification, especially as 36% indicate they are currently working towards this and a further 30% are considering.

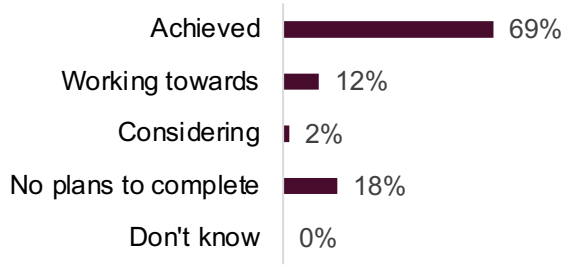


Q25. Does your organisation have any of the following security certifications?

Certifications - Cyber Essentials

Over 80% of responding institutions in HE and FE have achieved or are working towards Cyber Essentials certification. For these organisations, the scope of the certification tends to cover the entire organisation. This large increase is likely due to government, funding or contractual obligations mandating Cyber Essentials certification.

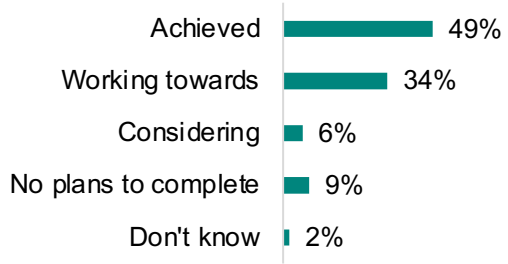
HE



Scope of certification (> 1 response):

- Entire organisation n=18
- Managed services/devices/desktop n=2
- Specific commercial department/s n=2
- Research/specific research centres n=3

FE



Scope of certification (> 1 response):

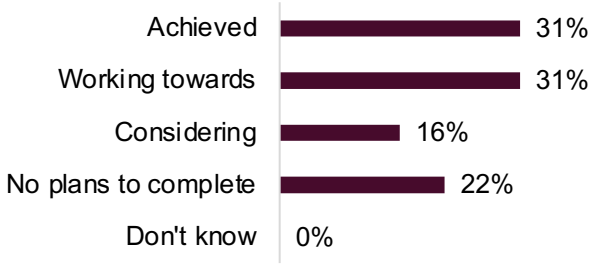
- Entire organisation n=29
- Managed services/devices n=2
- Staff network n=2

Q25. Does your organisation have any of the following security certifications?
Q26. If you have or are working towards Cyber Essentials, what is the scope of your certification?

Certifications - Cyber Essentials Plus

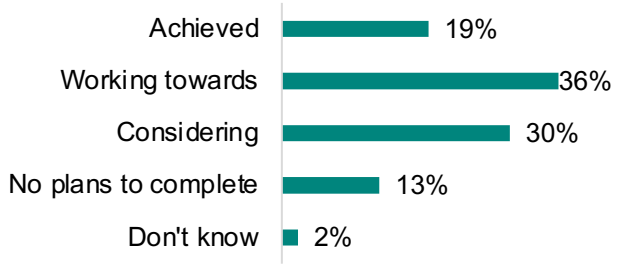
Over half of responding institutions in HE and FE have achieved or are working towards Cyber Essentials Plus. Similarly, these organisations are looking to cover the entire organisation.

HE



Scope of certification (> 1 response):
- Entire organisation n=16
- Restricted subset n=4
- Managed services/desktop n=3

FE



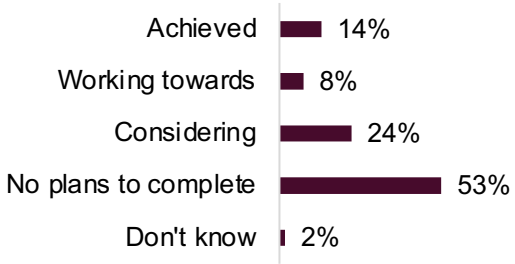
Scope of certification (> 1 response):
- Entire organisation n=22
- Managed services/devices n=2
- Staff network n=2

Q25a. Does your organisation have any of the following security certifications?
Q27. If you have or are working towards Cyber Essentials Plus, what is the scope of your certification?

Cyber security certifications - ISO27001

For ISO27001, the scope tends to be more variable, either covering the whole organisation, data centres/safe havens or specific departments. The proportions considering or working towards certification currently indicates that ISO27001 certification completions could continue to grow in popularity, although around half of responding institutions in both sectors have no plans to complete at present.

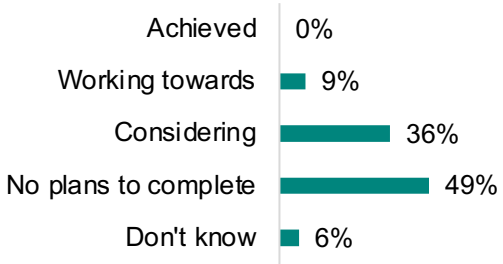
HE



Scope of certification (> 1 response):

- Entire Organisation n=3
- IT services/departments n=3
- Data centre/data safe haven n=2
- Specific department n=2

FE



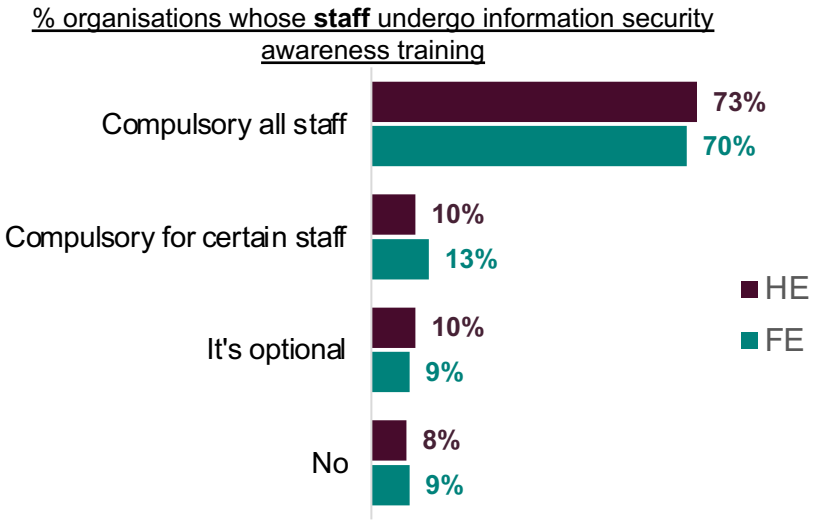
Scope of certification (> 1 response):

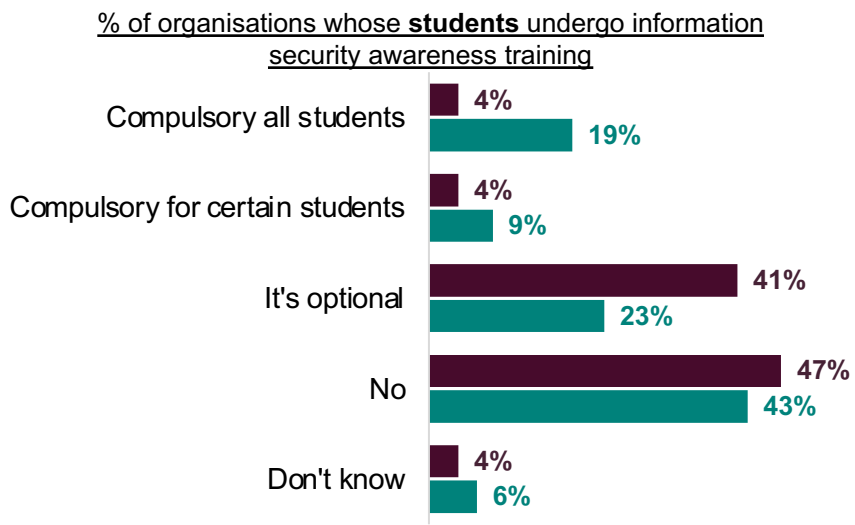
- Entire organisation n=2

Q25b. Does your organisation have any of the following security certifications?
Q28. If you have or are working towards ISO27001, what is the scope of your certification?

Information security training

Compulsory staff training remains more common than student training for both HE and FE with 73% of HE and 70% of FE organisations implementing this. Comments suggest that new starters, senior staff, and key infrastructure/business support staff are more likely to receive this in organisations where it is not compulsory. As in 2019, FE organisations (19%), are more likely to run compulsory student training than HE (4%). Students in cyber or computing disciplines receive this training where it is not compulsory for all.



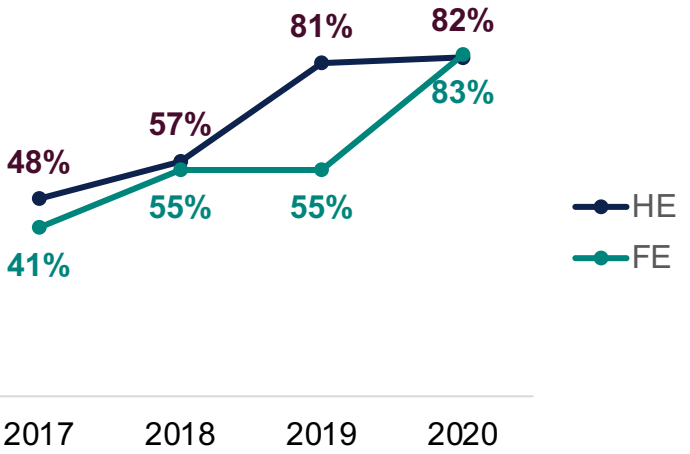


Q29. Do your staff undergo information security awareness training? Q29a. Please state what type of staff this is compulsory for.
Q30. Do your students undergo information security awareness training? Q30a. Please state what type of students this is compulsory for.

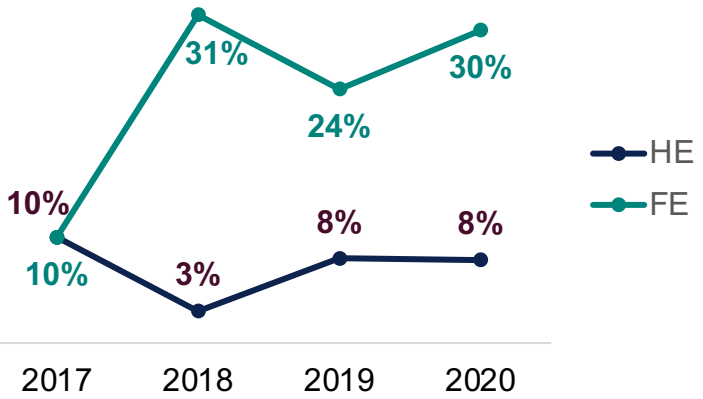
Cyber security training over time

The proportion of organisations who indicate they have some form of compulsory staff training has risen in both sectors, particularly in FE, suggesting this is now a key priority for mitigating human error/risk. Compulsory student training has consistently been more common in FE than HE since 2017.

% organisations who have compulsory information security awareness training for staff



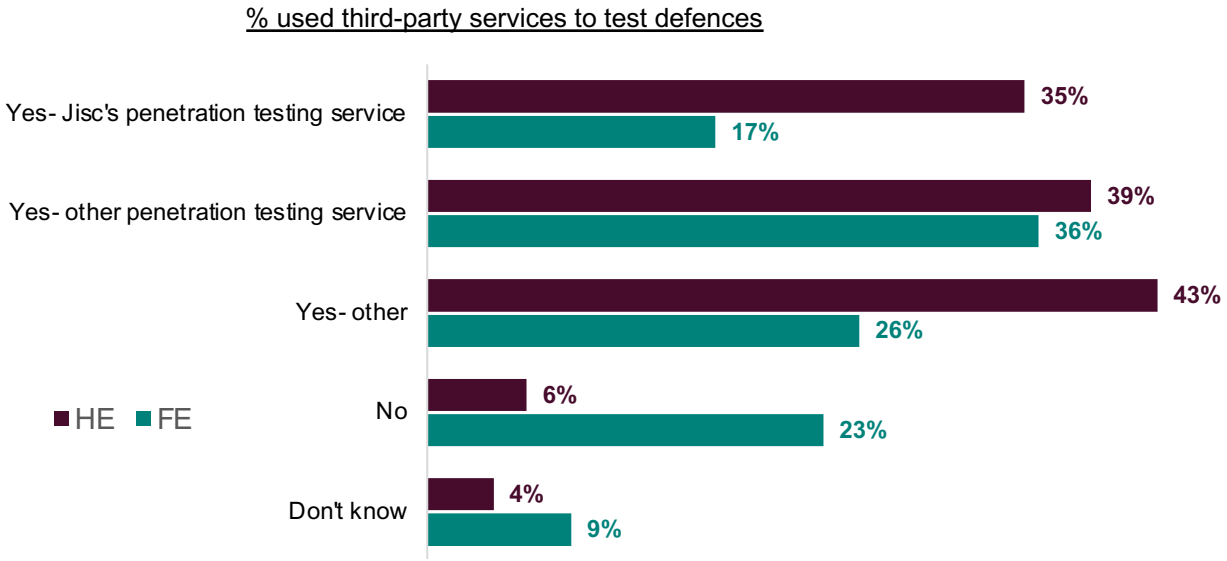
% organisations who have compulsory information security awareness training for students



Q29. Do any of your staff undergo information security awareness training?
Q30. Do any of your students undergo information security awareness training?

Tools or services used to test defences

Almost all HE organisations (90%) use third-party services to test their defences, with almost three-quarters (74%) using some form of penetration testing. At 68%, these tools are less commonplace in FE organisations, although over half (53%) report using penetration testing.



Q32. Do you use any tools or services to test your defences?
Q32a. Please tell us which other penetration testing services you use.

Providers used to test defences

Some did not specify providers, but comments suggest that a range of suppliers are used to test defences and no single company dominates, which is a similar picture to 2019.
Suppliers with more than 1 mention include Appcheck and Nessus in HE and Khipu in FE.

Other penetration testing services used (supplier mentions)

HE	FE
• Unspecified vendor n=9 • AppCheck n=3 • Khipu n=1 • Nessus n=1 • 4ARMED n=1 • Sapphire n=1 • Red-Team n=1 • Sec-1 n=1 • ECSC n=1 • Outpost24 n=1 • NCC Group n=1	• Khipu n=3 • Unspecified vendor n=2 • Nessus n=1 • Nettitude n=1 • Bank PCI n=1 • Kali n=1 • OpenVAS n=1 • Pentest People n=1 • Orange Cyberdefence n=1 • Hacker Guardian n=1 • Barrier n=1 • GFI LANGuard n=1 • Deloitte n=1

Other tools or service used to test defences (supplier mentions)

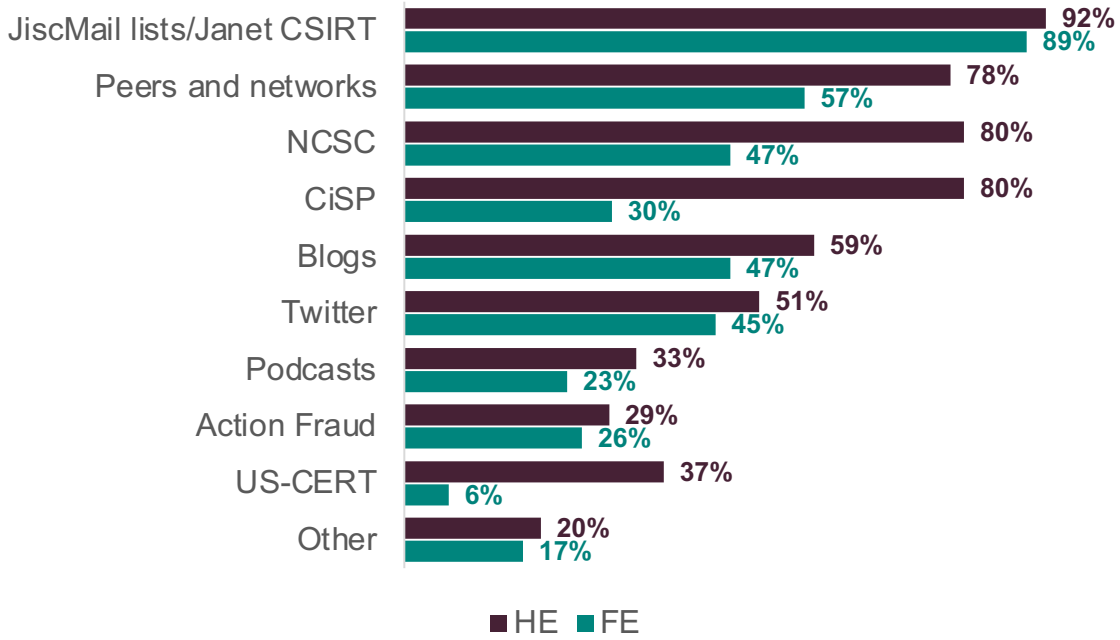
HE	FE
• Nessus n=5 • AppCheck n=2 • Unspecified vendor n=1 • Kali n=1 • Qualys n=1 • Red Team n=1 • In house n=1 • Tenable.io n=1	• Unspecified vendor n=4 • Khipu n=2 • In-house n=1 • Bank PCI n=1 • Shodan n=1 • NCSC n=1 • Greenbone n=1 • Nessus n=1

As can be seen from the tables, some responses mentioned penetration testing service vendors and some named vulnerability scanning solutions instead. This indicates a lack of understanding of the difference between penetration testing and vulnerability scanning.

Q32a. Please tell us which other penetration testing services you use.
Q32b. Please tell us what other tools or services you use to test your defences.

Third party services used to keep updated

JiscMail lists/Janet CSIRT, peers/networks and NCSC top the list in terms of sources used for insight/intelligence. CiSP is also a popular source of intelligence within HE, while social media channels such as blogs and twitter are popular in FE. As in 2019, knowledge sharing amongst peers play an important role in in detecting and reacting to emerging threats for both sectors.



Other sources mentioned HE

- News sites/lists n=5
- HEFESTIS CISO Share n=3
- Local networks n=2
- Supplier briefings n=2
- Reddit n=1
- National Trading Standards n=1

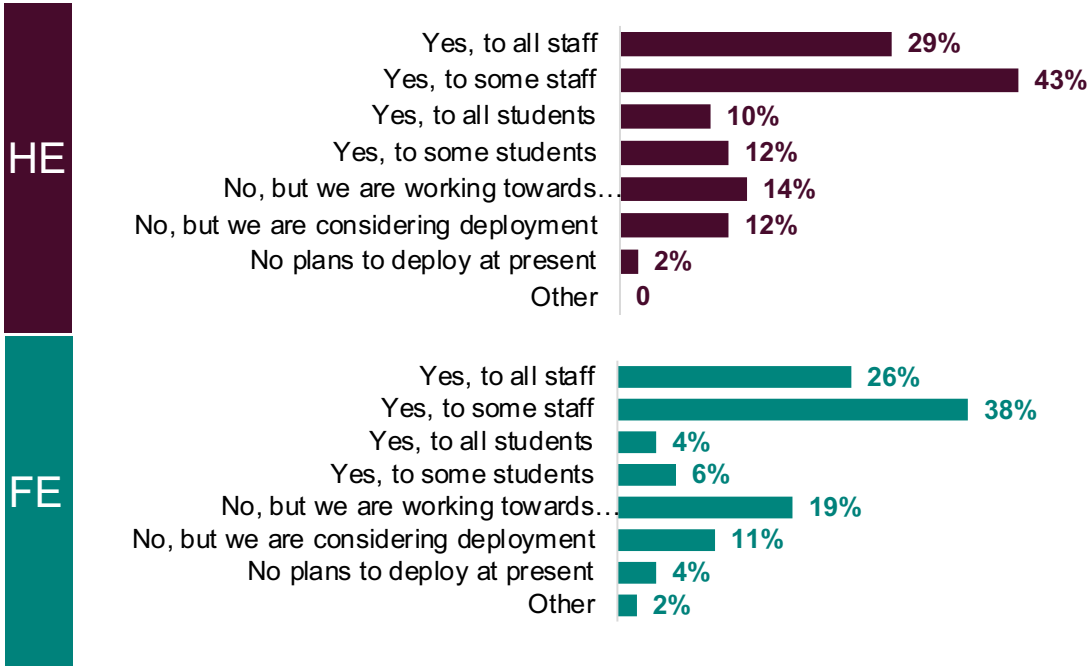
Other sources mentioned FE

- Email alerts n=2
- News sites/lists n=3
- Local networks n=2
- EduGeek n=1
- Reddit n=1

Q33. Do you use any of the following to keep updated on security news, threats or intelligence?

Multifactor authentication

Both HE and FE are more likely to deploy multifactor authentication (MFA) to staff. 72% of HE and 64% of FE indicate some form of MFA deployment for staff, dropping to 22% (HE) and 10% (FE) for students. Reasons for non-deployment include disruption to users, time/resource, platform integration issues and prioritisation of other work. However, implementing MFA will help protect against phishing campaigns, which are recognised as a top threat.



HE: Reasons for non deployment

- Other priorities n=2
- Cost/resources n=2
- Resistance and disruption to users n=1
- Failure of previous project n=1

FE: Reasons for non deployment

- Issues with platform integration n=2
- Time and resources, including Covid overload n=1
- Disruption to users n=1

Q34. Have you deployed multifactor authentication within your organisation?
Q34b. Please tell us why you haven't deployed mutifactor authentication.

Multifactor authentication

Comments suggest that MFA for remote access and Office 365 are the the most common, with Azure the most mentioned product. Where it has not been rolled out to all, IT and those with admin accounts were the most likely to have MFA and comments suggest that wider roll out is planned or already in discussion.

	Yes to all staff/students	Yes to some staff	Yes to some students
HE	• Deployed on some systems (2) • Azure MFA (3) • MFA for 365 (4) • Required for remote access (4) • Duo (2)	• Deployed to IT staff/admins (6) • Considering or rolling out for remote access (4) • Considering or rolling out MFA for 365 (4) • Considering rolling out to all users (2) • Considering rolling out to students (2) • Role-based access levels (1) • Deployed to professional services staff (1) • Rolling out Azure MFA (1) • In-house system (1) • Deployed on some systems (1)	• Mandatory MFA for students planned (2) • Optional for students (1) • No plans to make mandatory (1)
FE	• Required for remote access (4) • Azure MFA (3) • MFA for 365 (5)	• Deployed to IT staff/admins (11) • Considering rolling out to all staff (6) • Deployed to senor staff/management (2) • No plans to roll out to students (2) • Azure MFA (1) • MFA for 365 (1) • Duo (1) • Deployed to finance staff (1) • Deployed to teaching staff (1)	• Currently optional for students (2)

Q34a. Please tell us more about your deployment

Cyber security threats and concerns

Cyber security concerns – summary

As in 2018 and 2019, phishing/social engineering is the top concern identified by both HE and FE, with 36 HE institutions and 35 FE organisations ranking this at no.1. Ransomware/malware and unpatched security vulnerabilities are ranked second and third by both HE and FE. For those who indicate 'other', human error and accidental data breaches by staff are most mentioned, again reflecting the responses from 2019. This suggests that implementing controls against phishing alongside training and awareness raising with staff/students is still a key priority for organisations.

Top cyber security concerns (frequencies and rank based on a weighted score – top three ranked)

Rank HE	Threat	1	2	3	Weighted score
1	Phishing/social engineering	36	8	3	127
2	Ransomware/malware	5	23	11	72
3	Unpatched security vulnerabilities	6	11	15	55
4	Intellectual property theft	1	3	7	16
5	Denial of Service attacks	1	1	6	11
6	Other	1	2	2	9
7	Internal attacks	0	2	3	7
8	IoT based attacks	0	0	3	3

Rank FE	Threat	1	2	3	Weighted score
1	Phishing/social engineering	35	8	1	122
2	Ransomware/malware	7	24	8	77
3	Unpatched security vulnerabilities	2	5	13	29
4	Internal attacks	3	5	9	28
5	Denial of Service attacks	0	2	7	11
6	Intellectual property theft	0	1	5	7
7	Other	0	2	2	6
8	IoT based attacks	0	0	2	2

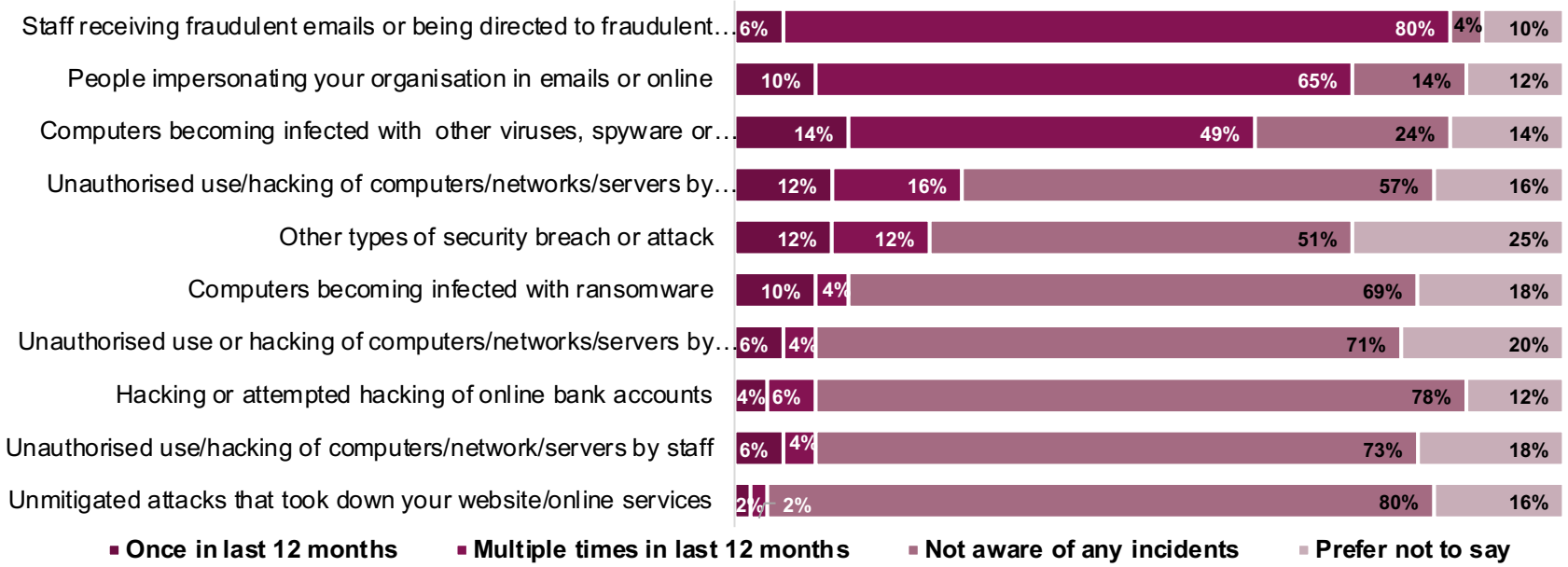
Q35. What do you feel are the three most significant cyber security threats to your organisation?
Q36 If your top threats aren't listed, please add up to three additional cyber security threats.

Jisc

Cyber security incidents

Experience of cyber security incidents - HE

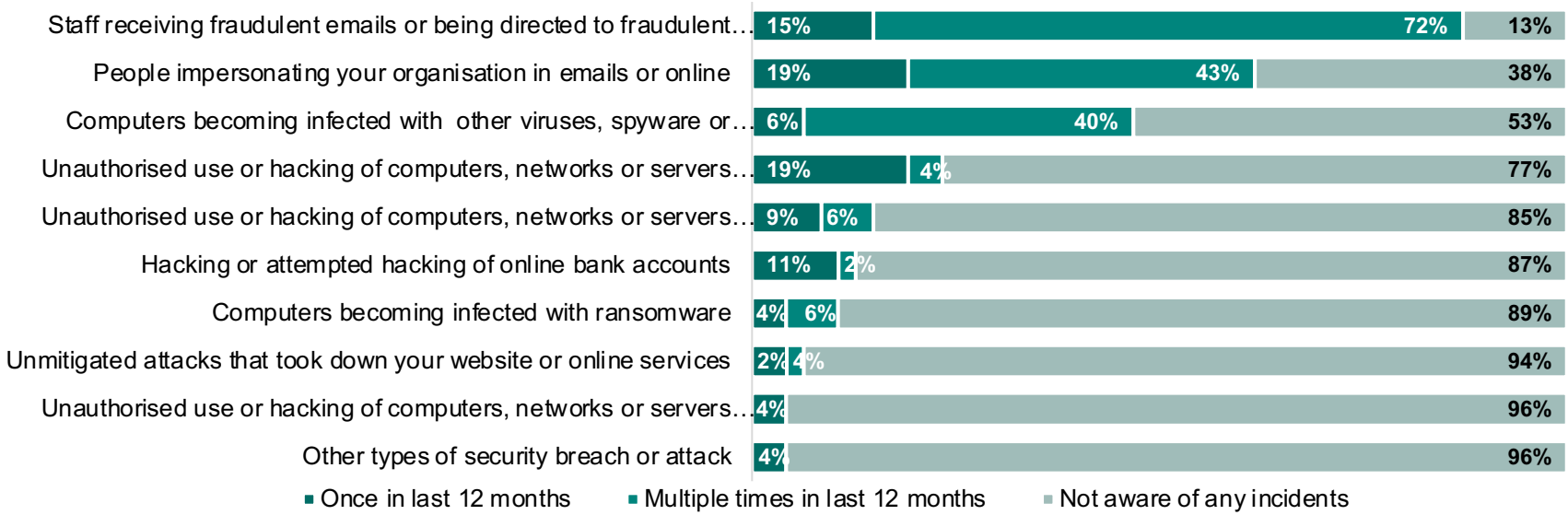
Alongside its identification as a key concern, phishing is also the most reported security incident by HE respondents. 86% report incidence of staff receiving fraudulent emails or being directed to fraudulent websites, while 75% report people impersonating their organisation in emails or online. Over half (63%) report computers becoming infected with viruses or spyware.



Q37: In the last 12 months, has your organisation experienced any of the following incidents?

Experience of cyber security incidents - FE

For FE, the top three reported incidents mirror the HE experience. 87% report occurrences of staff receiving fraudulent emails or being directed to fraudulent websites in the last 12 months, while over half (62%) report people impersonating their organisation in emails or online. Computer infection with viruses or spyware is also reported by almost half of organisations.

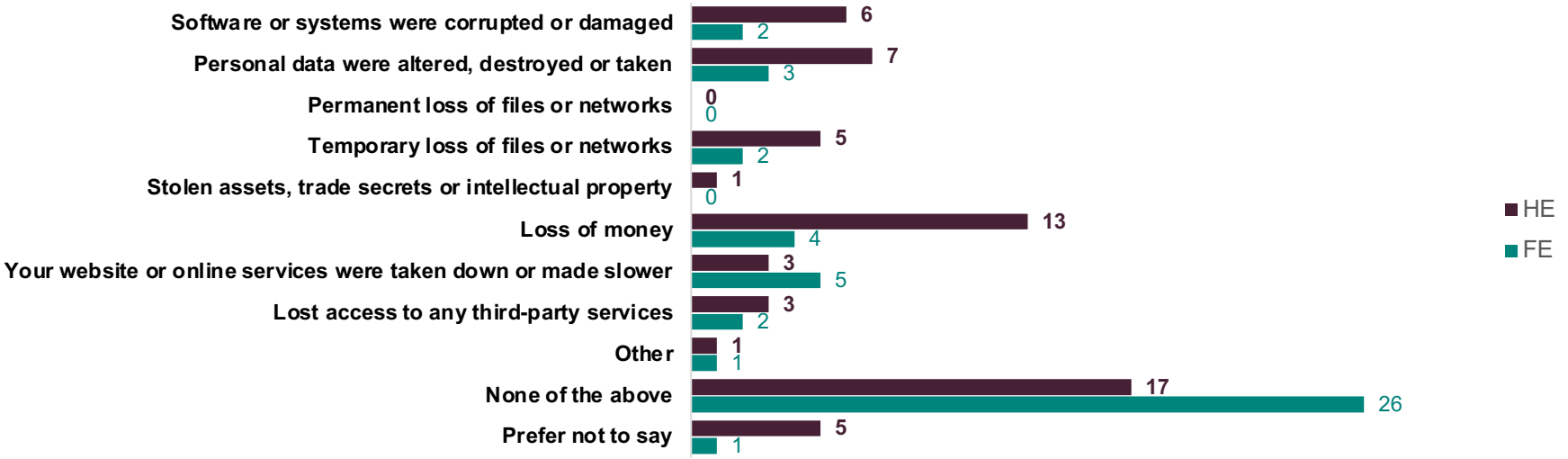


Q37: In the last 12 months, has your organisation experienced any of the following incidents?

Outcomes of security incidents

Few organisations reported major outcomes, although loss of money, corruption of software and personal data breaches were highlighted by some. Many declined to answer or reported 'none of the above', which could be due to defences working well, or could be that the respondents were unaware of the outcomes. Understanding the true outcomes and impacts of cyber security incidents could benefit from further exploratory research.

Outcomes of cyber security incidents (absolute numbers reported due to low responses)



Q38. Did any of the incidents that your organisation experienced in the last 12 months lead to the following?

Impacts of incidents

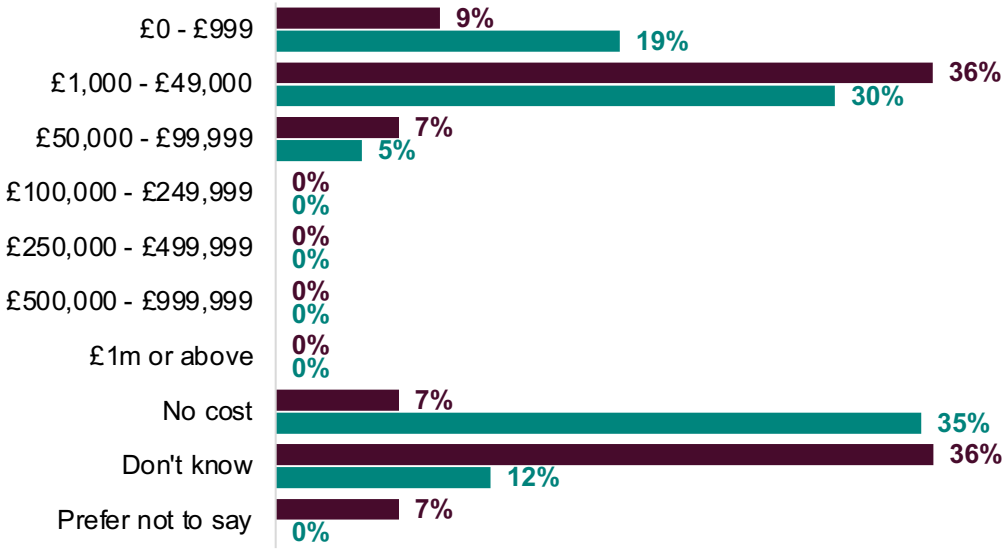
Staff time required to deal with incidents is the biggest reported impact for both HE and FE, with FE also reporting an increased need to invest in security controls.

Impacts of cyber security incidents (absolute numbers reported due to low responses)

Q39. Did your organisation experience any of the following impacts as a result of these incidents in the last 12 months?

Financial impact of incidents

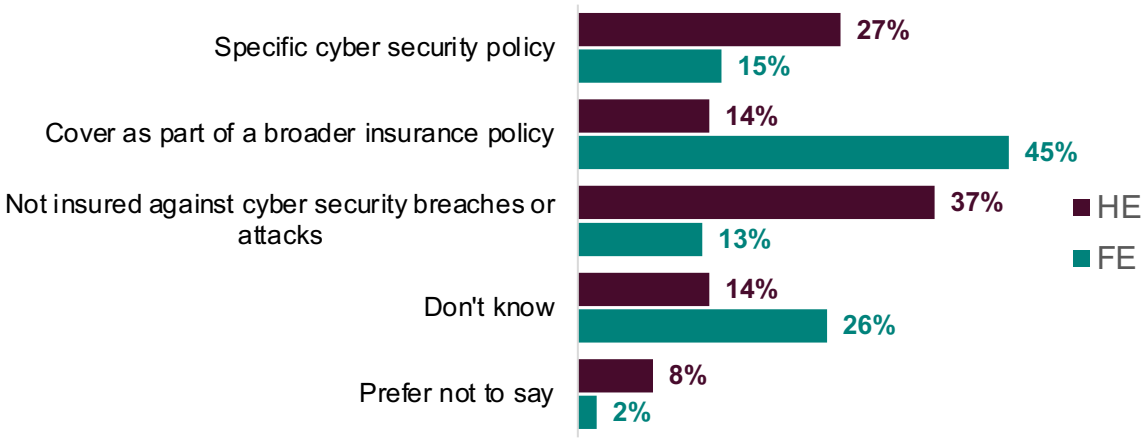
Both HE and FE indicate that cyber security breaches and attacks over the last 12 months have cost their organisation less than £100,000, with most responses in the £1,000 to £49,000 bracket. Over one third of FE responses (35%) indicate no incurred cost, while 36% of HE institutions do not know the financial costs. Responses suggest that organisations do not see a significant financial cost to their organisations, however interviews carried out subsequent to this survey, and from assisting with investigations, we believe the true financial impact is not being accurately captured. This will form part of a further piece of research.



Q40. Approximately, how much do you think the cyber security breaches or attacks you have experienced in the last 12 months have cost your organisation financially?

Cyber security insurance

41% of HE institutions indicate some form of cyber security cover and are more likely to have specific cyber security insurance (27%) than FE colleges (15%). However, more FE colleges indicate having some form of cyber security insurance overall (60%) but are more likely to have this as part of a broader insurance policy (45%). HE are more likely to have no insurance against cyber security breaches at 37%, with only 13% of FE respondents indicating no cover.



HE: Insurance companies mentioned

- Arthur J. Gallagher n=2
- UMAL n=1
- CFC n=1
- Ascent n=1
- Beazley UK n=1

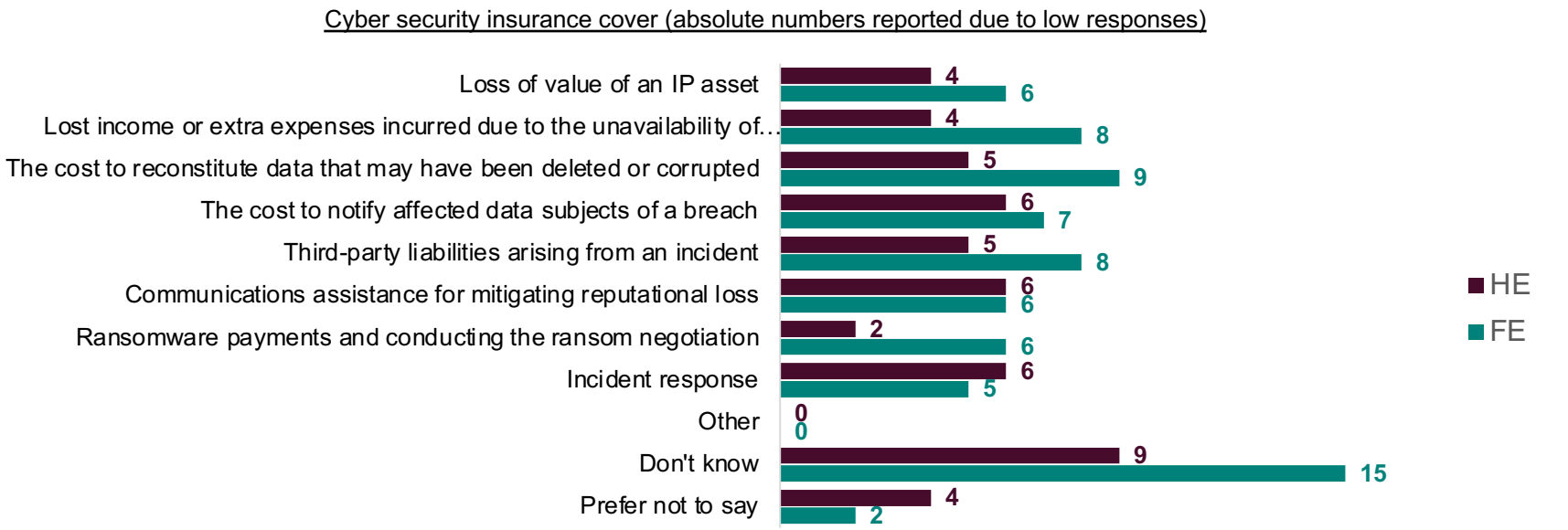
FE: Insurance companies mentioned

- Marsh Cyber Insurance n=2
- Zurich n=1
- UMAL n=1
- Hettle Andrews n=1
- FE Protect n=1
- Chubb n=1

Q42. Insurance: which of the following best describes your situation?
Q43. If you know who your insurer is for cyber security cover, please tell us.

Cyber security insurance cover

Insurance policies appear to cover a broad range of issues, but most respondents are unaware of the details or would prefer not to say.



Q44. Which of the following are provided under this insurance policy as far are you are aware?

Cyber security insurance claims

Insurance claims for cyber security breaches do not appear to be common, although more are reported in HE than in FE. 13 (62%) HE institutions indicate they have not made any insurance claims, with 2 making claims in the current academic year and one in the previous academic year.
25 (89%) FE organisations have not made any claims in the last two years, and none report making any claims.

HE (n=21)*

62% (13 out of 21)
Have not made a claim in the last two years

14% (3 out of 21)
Have made a claim in the last two years

*Small sample

FE (n=28)*

89% (25 out of 28)
Have not made a claim in the last two years.
None have made claims.

*Small sample

Q45. Have you made any insurance claims for cyber security breaches under this insurance?

Feedback on Jisc products/services

Products/services of interest - summary

Audits and assessment services, and threat sharing were top of the list of services with the highest interest levels for HE, highlighting the increased priority placed on cyber security within institutions and the continued importance placed on proactive monitoring and management of threats. There is also interest in SIEM as a managed service and NTA/NDR platforms.

FE, also report interest in cyber risk and resilience audit, and indicate a focus on increasing cyber defence with phishing simulation, penetration testing and vulnerability assessment also showing high levels of interest. SIEM products are clearly of interest to FE, with both SIEM on premise and SIEM as a managed service appearing in the top 5.

HE Top 5 interested in:
1. MISP Threat Sharing 43%
2. Cyber risk and resilience audit (BS31111) 37%
3. SIEM managed service 33%
4. Security assessment/posture analysis 31%
5. NTA/NDR platforms 31%

FE Top 5 interested in:
1. Cyber risk and resilience audit (BS31111) 53%
2. SIEM on premise 51%
3. Penetration testing 49%
4. SIEM managed service 47%
4. Phishing simulation 47%
4. Vulnerability assessment 47%

Q46. Which, if any, of the following products or services would be of interest to your organisation?

Products/services used and of interest - HE

Products/services	Have	Interested	Not interested
Critical services protection	5 (10%)	15 (29%)	12 (24%)
Cyber Essentials advice & guidance	16 (31%)	9 (18%)	14 (27%)
Cyber Essentials certification	21 (41%)	14 (27%)	5 (10%)
Cyber risk and resilience audit (BS31111)	4 (8%)	**19 (37%)**	14 (27%)
Cyber security financial x-ray	4 (8%)	7 (14%)	22 (43%)
Data Loss Prevention	9 (18%)	15 (29%)	13 (25%)
DNS allow lists and deny lists	10 (20%)	14 (27%)	11 (22%)
DNS RPZ / DNS Firewall	13 (25%)	10 (20%)	12 (24%)
Email filtering	22 (43%)	4 (8%)	12 (24%)
EDR solutions	12 (24%)	13 (25%)	11 (22%)
GDPR training	22 (43%)	4 (8%)	12 (24%)
IDS – managed internally	13 (25%)	10 (20%)	13 (25%)
Managed firewall – 3rd party	11 (22%)	4 (8%)	20 (39%)

Products/services	Have	Interested	Not interested
Managed IDS – 3rd party	3 (6%)	10 (20%)	22 (43%)
MISP Threat Sharing	4 (8%)	**22 (43%)**	9 (18%)
MFA solution	23 (45%)	9 (18%)	8 (16%)
NTA/NDR platforms	6 (12%)	**16 (31%)**	14 (27%)
Off-site DNS hosting	6 (12%)	7 (14%)	23 (45%)
Password managers	5 (10%)	19 (37%)	13 (25%)
Penetration testing	14 (27%)	15 (29%)	11 (22%)
Phishing simulation	12 (24%)	12 (24%)	13 (25%)
Security assessment/posture analysis	10 (20%)	**16 (31%)**	10 (20%)
SIEM managed service	7 (14%)	**17 (33%)**	14 (27%)
SIEM on premise	7 (14%)	14 (27%)	18 (35%)
Vulnerability assessment	19 (37%)	12 (24%)	7 (14%)
Web filtering	17 (33%)	10 (20%)	12 (24%

Q46. Which, if any, of the following products or services would be of interest to your organisation?

Products/services used and of interest - FE

Products/services	Have	interested	Not interested
Critical services protection	5 (11%)	8 (17%)	21 (45%)
Cyber Essentials advice & guidance	16 (34%)	19 (40%)	6 (13%)
Cyber Essentials certification	15 (32%)	21 (45%)	4 (9%)
Cyber risk and resilience audit (BS31111)	3 (6%)	**25 (53%)**	10 (21%)
Cyber security financial x-ray	0	15 (32%)	18 (38%)
Data Loss Prevention	11 (23%)	11 (23%)	13 (28%)
DNS allow lists and deny lists	10 (21%)	14 (30%)	11 (23%)
DNS RPZ / DNS Firewall	13 (28%)	11 (23%)	12 (26%)
Email filtering	22 (47%)	7 (15%)	9 (19%)
EDR solutions	10 (21%)	9 (19%)	14 (30%)
GDPR training	20 (43%)	5 (11%)	11 (23%)
IDS – managed internally	14 (30%)	11 (23%)	8 (17%)
Managed firewall – 3rd party	5 (11%)	5 (11%)	27 (57%)

Products/services	Have	interested	Not interested
Managed IDS – 3rd party	2 (4%)	6 (13%)	25 (53%)
MISP Threat Sharing	5 (11%)	15 (32%)	11 (23%)
MFA solution	15 (32%)	11 (23%)	11 (23%)
NTA/NDR platforms	7 (15%)	17 (36%)	9 (19%)
Off-site DNS hosting	13 (28%)	5 (11%)	18 (38%)
Password managers	11 (23%)	16 (34%)	11 (23%)
Penetration testing	14 (30%)	**23 (49%)**	4 (9%)
Phishing simulation	7 (15%)	**22 (47%)**	8 (17%)
Security assessment/posture analysis	7 (15%)	16 (34%)	9 (19%)
SIEM managed service	1 (2%)	**22 (47%)**	12 (26%)
SIEM on premise	4 (9%)	**24 (51%)**	8 (17%)
Vulnerability assessment	9 (19%)	**22 (47%)**	7 (15%)
Web filtering	24 (51%)	6 (13%)	7 (15%)

Q46. Which, if any, of the following products or services would be of interest to your organisation?

Feedback on Jisc's existing services- HE

We received positive comments about the Jisc offer and our staff, with particular mentions for CSIRT, penetration testing, and DDoS mitigation.

Always very good, good people, visionary and effective at identifying solutions required by clients.

We use the Jisc Penetration Testing services extensively and have always been very impressed at the service...

Baseline ISP service is very good, basic DDoS protection is valuable.

Good all round security offering. Approachable and efficient staff. Industry standard technology.

A number of suggestions for development were made, including:

- Awareness of how services can be utilised
- Sharing of information/data across the sector
- Improve value for money of additional services, or include in the subscription
- A request to scan institution public IP ranges as a standard process and provide reports

Q47. Do you have any feedback on Jisc's existing cyber security services?

Feedback on Jisc's existing services - FE

We received positive comments about services, with particular mentions for the CSIRT team, Cyber Essentials, and Jisc's knowledge and responsiveness. However comments around Jisc's speed of getting services to market suggest some confusion about our offer, including what is available and what is outsourced to third parties. Additional liaison or marketing activities could be beneficial in this sector.

Really pleased to see cyber security essentials certification included in the Jisc support

Amazing service. great staff and so responsive.

Jisc do a great job and the team are very knowledgeable when contacted.

The CSIRT Team when we have used them, or when they have picked up attacks on our IPs have been absolutely amazing... A service we far too often take for granted but appreciate massively!

Key themes on areas for development:

- Perception of Jisc's speed of getting services to market, and awareness of our offer
- Cost, and inclusion of advanced cyber security services within the subscription charge

Q47. Do you have any feedback on Jisc's existing cyber security services?

Other products/services interested in Jisc providing

A range of responses were received and are summarised below

HE

- Regular threat bulletins
- Outsourced 24/7 SOC
- CISO advisory services
- Training for Penetration testing in house
- Managed SIEM
- NIST Framework
- BS 31111 audit and assessment
- ISO27001 CE+ Certification services
- Comparison metrics against business
- Secure hubs for research activities
- Managed SIEM/SOC options - either consuming or contributing data/intelligence
- Managed SOC (x2)
- Help with achieving ISO27001

FE

- Contracts with, e.g. Cisco and Fortinet to improve affordability for the sector.
- SOC managed service
- Improve costs/affordability of the frameworks already in place

Q49. Are there any additional cyber security related frameworks, products or services you are interested in Jisc providing?

Lisa Charnock
Research analyst
lisa.charnock@jisc.ac.uk

John Chapman
Head of security operations centre
john.chapman@jisc.ac.uk