Jisc

18/07/2018

Cyber Security Posture Survey 2018 Research Findings

John Chapman, Head of Security Operations Centre
Jessica Francis, Research Manager Product & Improvement
Lola Harre, Research Manager Product & Improvement

Summary of Key Findings I

Cyber security staffing

- Similar to 2017, **cyber security staffing is more prevalent in HE than FE.**

Within HE:

  - The **proportions reporting to have a strategic cyber security lead** (2018 60% vs 2017 56%) and **computer security incident** response team (2018 63% vs 2017 50%) **has risen since 2017**.
  - Although those reporting dedicated security staff has gone down (2018 65% vs 2017 69%), there has been a **substantial rise in Information Security Officer** (2018 80% vs 2017 31%) and **Security Analyst** (2018 76% vs 2017 36%) **positions**, suggesting a recruitment drive in this space.

Within FE:

  - The **proportion reporting they have a strategic cyber security lead has risen** to 35% from 28%, however only 2% indicate they have dedicated cyber security posts.
  - Organisations reporting they have **staff available 24x7 to respond to security incidents has declined** to 4% from 10%.

- In organisations where there is no strategic lead for cyber security, Directors or Heads of IT are most likely to have this responsibility. It was also fairly common across both sectors for multiple individuals to have responsibility for cyber security.

Cyber security budgets

- **Those reporting to have a specific cyber security budget (excluding staffing costs) appears to be rising** over time:
  - For HE, 43% said they had a budget in 16/17 compared to 62% for 18/19, indicating it is increasingly being seen as essential expenditure by universities.
  - For FE, a slight rise is also noted from 27% in 16/17 to 33% for 18/19.
- The mean cyber security budget for HE does appear to have fallen slightly since 17/18 (-9%), as well as a more significant drop in FE (-34%). However, small sample sizes, outliers, and more individuals reporting budgets in 18/19 but not previous years may have influenced the reliability of these figures.

Summary of Key Findings II

Current Cyber security provision

- **Within HE, perceptions of cyber security protection remain fairly negative:**
  - Only 15% score their organisation as 8+ when asked how well protected they are, the same proportion as in 2017.
  - Overall HE organisations achieve a mean score of 5.9/10 in terms of protection level, a slight improvement on last year.
  - Cultural issues, lack of resources/budget and absence of policy are often cited as key reasons for lower scores.
- **Similar to 2017, FE organisations remain more optimistic than HE about their cyber security protection:**
  - 43% score their organisation 8+ and a mean score of 7.1/10, up slightly on 2017.
  - However, **lower proportions of FE organisations are interested in ranking their security posture against their peers (73%), compared to 2017 (86%),** indicating this has become less important for them.
- **HE are more likely to be working towards or have achieved cyber security certifications, but there is growth evident in FE:**
  - Much higher proportions of FE organisations are working towards Cyber Essentials (29% 2018 vs 3% 2017) and Cyber Essentials Plus (14% 2018 vs 3%) 2017), indicating that they are increasingly seen as a must-have certification.
- **Use of third party penetration testing services by the FE sector has risen (41% reported non use in 2017 vs only 14% in 2018)**
  - 33% use the Jisc service, which is comparable to the proportions using other penetration services. Sec-1 is the most frequently mentioned service.
- **Use of third party services to gain insight/intelligence has risen since 2017 both within HE (66% 2018 vs 46% 2017) and FE (49% 2018 vs 31% 2017:**
  - For HE, CISP and NCSC are the most often mentioned providers with newsletters/mailing lists also proving popular.
  - For FE, Sophos gets the most mentions.

Summary of Key Findings III

Cyber security threats and products

- Phishing & social engineering, Ransomware/Malware and lack of awareness/accidents remain the top three threats reported by both HE and FE, indicating **human error remains a key problem** (All threats listed):
  - Patch management and BYOD are new entrants to the top 10 this year for HE.
  - For FE, budgets/insufficient funding, lack of staff/resources and complacency are new to top 10.
- Interest in specific cyber security services and products has shifted:

For HE:

- Cyber Essentials training, advice and guidance and security assessment/posture analysis remain in the top 5 by % of interest. Interest in Password Managers and a managed log aggregation service replace GDPR training and phishing simulation in popularity.
- The biggest growth in interest since 2017 has been for Digital forensics, moving from 10th place (40% interested in 2017) to 6th this year (56% of interest), suggesting it is higher up HE members agendas.
- With the deadline passed, interest in GDPR training has declined since 2017, with higher proportions having participated in training this year (49% vs 12% in 2017). However this evolving space could lead to further interest in the future.
- Decreasing interest in phishing simulation is also evident, likely driven by higher proportions of institutions having this already (34% 2018 vs 18% 2017).

For FE:

- Cyber Essentials Training, advice and guidance and vulnerability assessment remain in the top 5 this year by % of interest. Security assessment/posture analysis and Intrusion detection system (managed internally) replace GDPR training and phishing simulation as top products of interest.
- Similar to HE, GDPR and Phishing simulation have seen decreases in interest.
- Services with the largest increases in interest are security assessment/posture which is now in top place (76% interested in 2018 vs 59% in 2017) ,high assurance networks (43% 2018 vs 31% 2017) and off-site DNS hosting (24% 2018 vs 10% 2017).

Summary of Key Findings IV

Cyber security training

- The **proportions reporting compulsory staff security awareness training appear to have increased since 2017**, as has student training in FE. This suggests that organisations are increasingly acknowledging human error/lack of awareness as security risks. Has GDPR driven this shift?
- The proportions of HE organisations indicating they have compulsory student training has decreased, although optional training has increased. This might suggest changing approaches to engaging students in information security.

Feedback on Jisc Services

- Overall, **feedback on Jisc security services was positive**.
- For HE, many different services were requested but only Managed SOC received more than one mention.
- Rather than specific security products, **many requests from FE relate to Jisc providing guidance or advice, as well as intelligence** on current performance, to help the sector make more informed decisions.

Background
Objectives
Methodology

Background & research objectives

Background

In order to successfully provide the relevant cyber security services, products and support to members, it is important Jisc understands organisations' current provision and needs as well as the potential threats and prevalent issues going forwards.

Following the running of the Jisc Cyber security posture survey in 2017, the team were keen to repeat the process in 2018 in order to understand organisations security posture in light of the fast changing and increasingly critical area of cyber security.

Business Objective

Prioritise planned security services for members and identify additional gaps for development.

Core Research Objectives

- Understand organisations' current cyber security staffing provisions
- Understand the budgets allocated by organisations to cyber security and any changes over time
- Explore organisations' perceptions of current protection levels and areas for improvement
- Understand cyber security certifications, training, and current provision of services within organisations'
- Explore perceptions of future cyber security threats
- Explore perceptions of Jisc's cyber security offer
- Explore reactions to potential service areas and to Jisc providing products in these areas

Methodology and sample

15 minute online survey was sent to security contacts including Information Security Managers, Network Managers, CIO's, IT Directors and Chief information Security Officers within HE and FE.

118

Completes

(2017 n=81)

Survey In Field:

27th March- 14th May 2018

Type of Organisation*	2018		2017	
	Completes	%	Completes	%
HE	65	55%	52	64%
FE	49	42%	29	36%
Other (Arts and Heritage, Research)	4	3%		

* This document includes analysis of HE and FE response only.

Jisc

Notes on data

- This document covers analysis of HE and FE response only. Other organisations have not been included due to small sample size. Responses are available as part of the raw dataset.
- Due to the low response rate from FE institutions to the 2017 survey, year-on-year comparisons of this sector should be treated with caution.
- Where the same individual answered the survey twice, their second response was deleted from the dataset.
- Where the same institution submitted multiple surveys, the most senior or relevant staff member’s response was included.

Cyber security staffing

Jisc

Cyber security staffing summary

	Have a strategic cyber security lead	Have dedicated cyber security posts	Have staff available 24x7 to respond to security incidents	Have a computer security incident response team*	Have a security operations centre*
HE (2017)	60% (56%)	65% (69%)	23% (21%)	63% (50%)	8% (8%)
FE (2017)	35% (28%)	2% (3%)	4% (10%)	33% (34%)	6% (7%)

- Similar to 2017, cyber security staffing is more prevalent in HE than FE.
- Within HE:
  - The proportion of those who have a strategic cyber security lead, staff available 24x7, and computer security incident response team has risen since 2017. However those reporting to have dedicated cyber security posts within their organisation has declined since 2017, and the rate of security operations centres has remained static.
- Within FE:
  - The proportion of organisations reporting they have a strategic cyber security lead has risen slightly to 35%, however only 2% indicate they have dedicated cyber security posts.
  - Those FE organisations reporting they have staff available 24x7 to respond to security incidents has declined since 2017.

*Note that these roles typically refer to the same team and so there may be some overlap of these values.

Q4a. Do you have a strategic lead for cyber security at your organisation? (e.g. CISO, CIO or other lead role). Q6. Do you have any dedicated cyber security posts in your organisation. Q7. Please tell us how many dedicated cyber security posts you have at each role (or equivalent) below? Q12. Do you have staff available 24x7 to respond to security incidents? Please tell us about this below. Q9. Do you have a Security Operations Centre? Q10. Do you have a computer Security Incident Response Team?

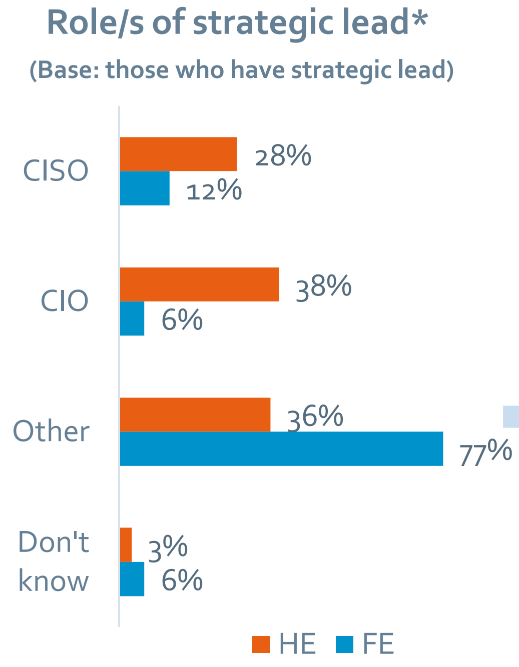
Presence of strategic cyber security lead

60% Have strategic cyber security Lead (HE)

(2017 56%)

35% Have strategic cyber security Lead (FE)

(2017 28%)



HE other responses

- Information Security Manager/IT Security Manager n=2
- CISO as part of Shared Service and CIO n=1
- Cyber security Manager n=1
- Digital Services, IT n=1
- Director of EFM and IT n=1
- Head of Information Assurance n=1
- Head of Information Security n=1
- Head of ITS n=1
- Head of Strategy Architecture and Assurance n=1
- Information Assurance n=1
- Registrar n=1
- Security and compliance n=1
- Steering Board, chaired by Finance Director n=1

FE other responses

- Head of IT/IT Director n=4
- Director n=1
- Director of Network and Information Systems n=1
- IT Manager n=1
- Operational Middle Manager n=1
- Assistant Principal for Digital n=1
- Vice Principal- Business Excellence n=1

60% of HE organisations surveyed have a strategic cyber security lead, with the majority in CISO and CIO positions. For FE, those with a strategic cyber security lead stands at 35%, with this often forming part of an IT or network director role.

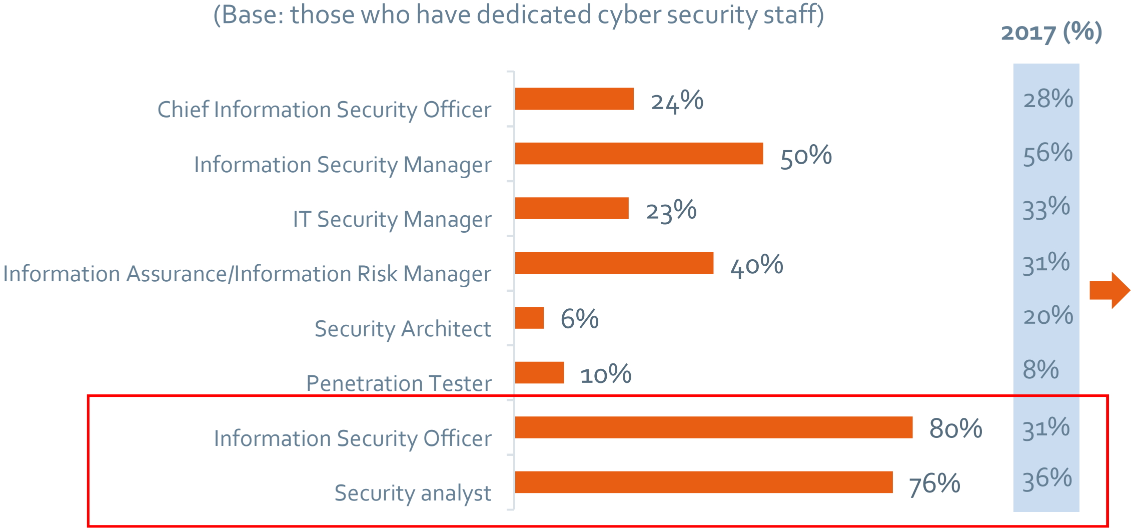
Q4a. Do you have a strategic lead for cyber security at your organisation? (e.g. CISO, CIO or other lead role) Q5. What role does your strategic lead for cyber security have? * results not comparable to 2017 as question changed to multicode from single code

Dedicated cyber security staff

65% have dedicated cyber security staff (HE)
(2017 69%)

2% have dedicated cyber security staff (FE)
(2017 3%)

% who have staff in role
(Base: those who have dedicated cyber security staff)



Only one FE organisation indicated they have dedicated cyber security staff in the role of **Digital Governance Manager**

Other roles within HE:
Head of Service Assurance, Service Assurance Staff, Head of CERT, 27x4 Managed Server/DC Manager Service, Graduate Intern, vacant role for Information Security Officer, cyber security partial part of other roles (networks, infrastructure), Information Governance Post, DPO and Records manager sit within IT/information security, incidence response team.

The proportion of HE organisations reporting they have dedicated cyber security staff has declined since 2017. However for those who do, there has been a substantial rise in Information Security Officer and Security Analyst positions, suggesting a recruitment drive in this space. FE remains stable, with only 2% reporting that they have dedicated cyber security staff.

Q6. Do you have any dedicated cyber security posts in your organisation. Q7. Please tell us how many dedicated cyber security posts you have at each role (or equivalent) below?

Institutions without a strategic cyber security lead

Those responsible for cyber security, where there is no strategic lead for cyber security:

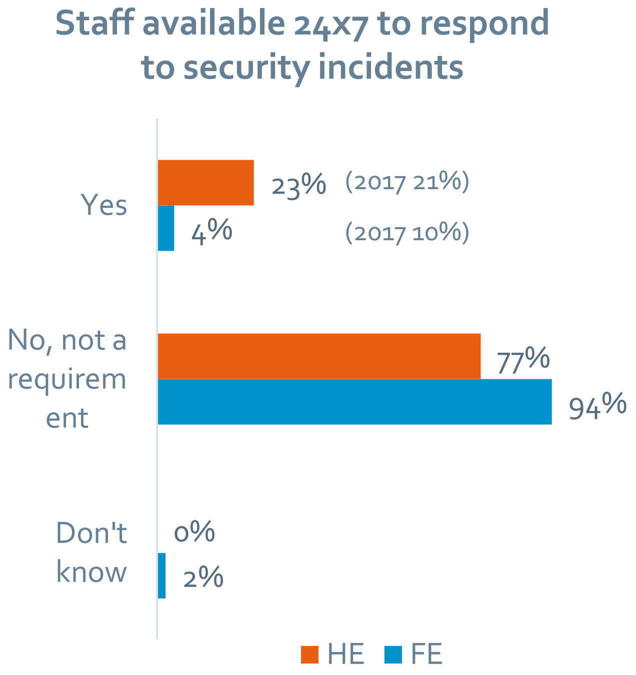
HE	
Director/Head of IT/ICT	n=8
IT Security Manager	n=2
Head of Information Management Tech	n=1
Head of Systems and Support Services, Information Services	n=1
Information Security Manager	n=1
IS&T Manager	n=1
IT Manager	n=1
IT Services Manager	n=1
IT Network Manager	n=1
Technology Services Manager	n=1
Network Security Officer	n=1
Multiple Individuals	**n=4**

FE	
Director/Head of IT/ICT	n=7
IT Manager/IT Systems/Services Manager	n=6
IT Network Manager	n=3
Another College	n=1
IT Department	n=1
IT Infrastructure Manager	n=1
Head of Network Services	n=1
Technology Services Development Manager	n=1
Network Support Officer	n=1
Head of Systems & Halls	n=1
Network & Comms Manager	n=1
VP	n=1
Multiple Individuals	**n=7**

In organisations where there is no strategic lead for cyber security, Directors or Heads of IT are most likely to have this responsibility. Within both HE and FE, it was also fairly common for multiple individuals to have responsibility for cyber security.

Q11. Who is currently responsible for cyber security at your organisation?

Staff available 24x7 to respond to security incidents



Cover varies from formalised response teams to more informal processes:

"Currently by goodwill, but working towards formalised measures – our end game is a 24/7 SOC which is being developed over time but constrained by investment…"

"24x7 "Best Efforts" support for incidents and emergencies"

"Yes, sort of- a major incident rota is in place where senior staff carry a 'hot phone', that will be called in the event of any major incident"

"General helpdesk who are all security trained"

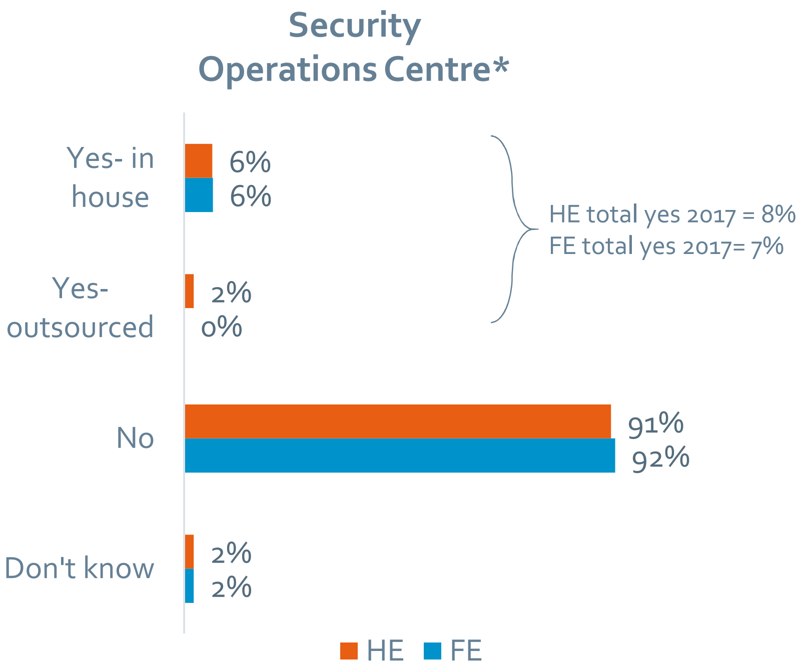
"We have a 24/7 service provided by NorMAN and an on-call duty rota for responding managers on-site"

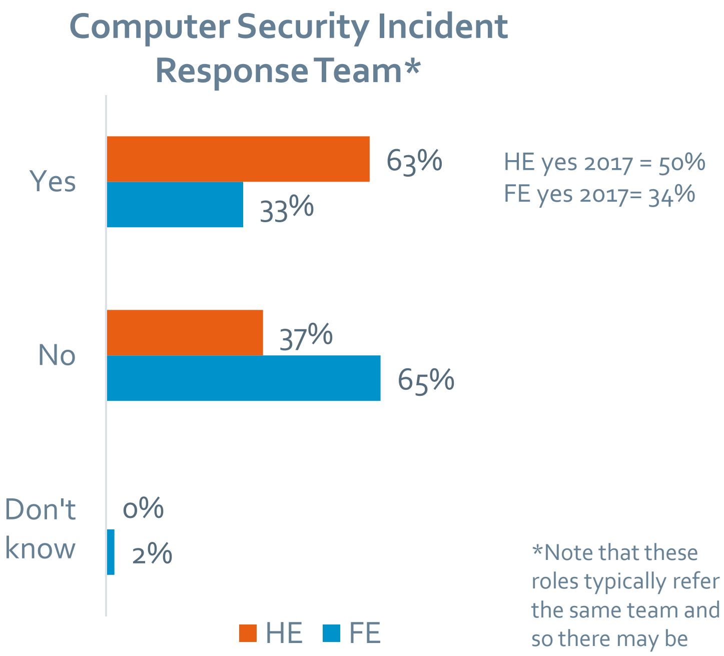
"calls routed through helpdesk, breach policy and risk management policy/procedures list for emergency callout"

Close to a quarter of HE organisations surveyed (23%) indicated that they have staff available 24x7 to respond to security incidents, though cover varies in formality and set-up. Within FE this is much less common with only 4%, down from 10% in 2017.

Q12. Do you have staff available 24x7 to respond to security incidents? Please tell us about this below.

Other cyber security staffing and provision





*Note that these roles typically refer to the same team and so there may be some overlap of these values.

Within HE, the proportions reporting a Security Operations Centre (8%) are unchanged, while those reporting Computer Security Incident Response teams (63%) have risen since 2017. This indicates that formalised teams to address cyber security are becoming more prevalent. Rates for FE are lower and have remained largely static since 2017.

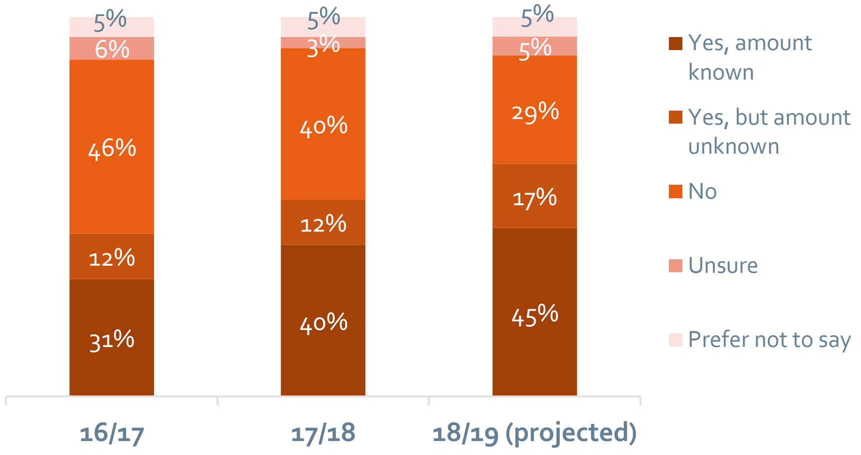
Q9. Do you have a Security Operations Centre? Q10. Do you have a computer Security Incident Response Team?

Cyber security budgets

Cyber security budget summary

Existence of specific cyber security budget (excluding staffing costs)

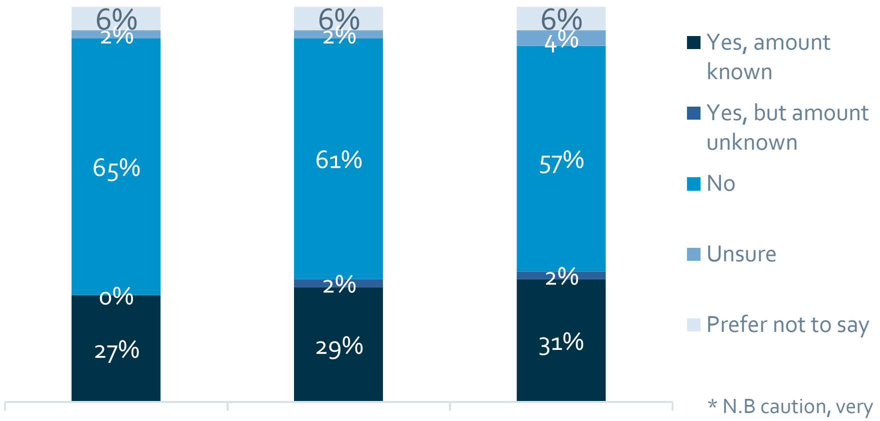
HE



MEAN BUDGET (Base: those amount known)*		
£116,250	£155,385	£142,069

-9%

FE



MEAN BUDGET (Base: those amount known)*		
£12,692	£27,857	£18,333

-34%

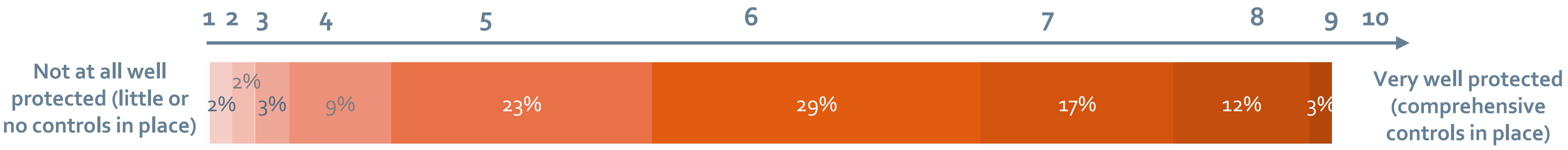
* N.B caution, very small sample size. Figures likely to be heavily impacted by outliers and more individuals reporting budgets in 18/19 than previous years.

For HE, the proportion of those reporting they have a specific cyber security budget (excluding staffing costs) has risen from 43% in 16/17 to 62% for 18/19, indicating it is increasingly seen as an essential expenditure. For FE, a slight rise is also noted from 27% to 31%. However, projected cyber security budgets for 18/19 show a decline of 9% for HE and 34% for FE. Note that these figures are based on small sample sizes, and so reliability may be impacted by outliers and the fact that more individuals have reported budgets in 18/19 but not previous years.

Q13. Do you have a specific cyber security budget (not including staffing costs)/. Please select one answer per row.? N.B. Prefer not to say and unsure excluded.

Cyber security provision

Cyber security protection perceptions HE



Mean score= 5.9 (2017 5.8)

(2017 % 8+= 15%)

➢ Rationale 1-4

- ➢ Lack of budget
- ➢ Work in progress
- ➢ Focus has been on GDPR
- ➢ Basic protections, but more to do
- ➢ Lacking staff resources
- ➢ Slow to get things in place
- ➢ Inconsistent operational procedures & monitoring
- ➢ Infosec not taken seriously- researchers reluctant to give away control
- ➢ Poor internal monitoring & controls
- ➢ Limited mobile management & BYOD
- ➢ Lack of policies

➢ Rationale 5-7

- ➢ Staff awareness biggest challenge
- ➢ Some controls in place, but more needed. Lack of maturity
- ➢ Lack of resources/time/budget
- ➢ Reactive rather than proactive
- ➢ No cohesive policy
- ➢ In process of putting a programme in place
- ➢ Behind where we would like to be
- ➢ Good external protection & policies, weaker internal protection
- ➢ Current protections & procedures not aligned to any standard
- ➢ Under resourced for threat level & environment complexity
- ➢ Good technical measures in place. Process, culture or organisational issues reduce overall effectiveness

➢ Rationale 8-10

- ➢ Good/many controls
- ➢ Strong policy
- ➢ Track record of incidence avoidance & handling
- ➢ Central control
- ➢ Extensive monitoring
- ➢ Have Cyber Essentials Plus
- ➢ Regular testing & auditing
- ➢ Made significant improvements and have dedicated team
- ➢ Infrastructure designed with 'security first' principle
- ➢ Training for all staff

92%

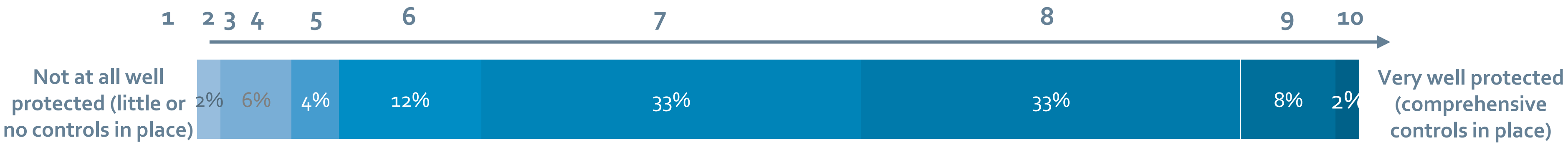
(2017 94%)

feel useful to rank institutions security posture against peers

Within HE, perceptions of cyber security protection remain fairly negative with only 15% scoring their organisation as 8+, and a mean score of 5.9. Cultural issues, lack of resources/budget and absence of policy are often cited as key reasons for lower scores.

Q14. Thinking about cyber security, how well do you feel your institution is protected? Q15. Please tell us why you gave a score of xx? Q27.Would it be useful for you to see how your institution's security posture ranks against your peers?

Cyber security protection perceptions FE



Mean score=**7.1** (2017 6.9) (2017 % 8+= 34%)

Rationale 1-4	Rationale 5-7	Rationale 8-10
➢ No dedicated cyber security team ➢ Limited resources ➢ Limited systems and controls in place currently	➢ In process of improving controls ➢ More could be doing ➢ Lack time and resources ➢ Lack of budget ➢ Threats are continually evolving ➢ Appropriate controls given size/type of organisation ➢ Good external security, but internal security could be improved ➢ Sensible measures in place within budget ➢ Need to improve end user training ➢ More monitoring needed	➢ Comprehensive set of controls ➢ Focus on cyber security over last 18 months ➢ Processes, systems, testing and training all undertaken ➢ Strong focus on security ➢ Could make staff more aware ➢ More testing could be done ➢ Working towards Cyber Essentials Certification ➢ Trialling AI threat systems ➢ Security embedded into design

73%

(2017 86%)

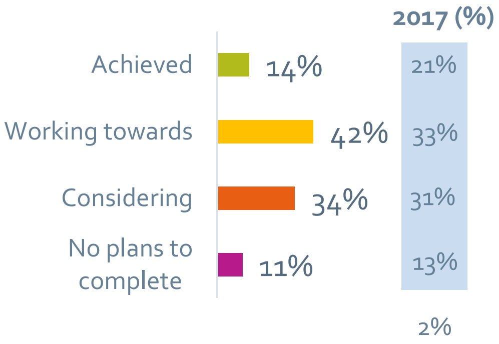
feel useful to rank institutions security posture against peers

Similar to 2017, FE organisations remain more optimistic than HE about their cyber security protection, with 43% scoring their organisation 8+ and a mean score of 7.1, up slightly on 2017. However, lower proportions of FE organisations are interested in ranking their security posture against their peers, compared to 2017, indicating this has become less important for them.

Q14. Thinking about cyber security, how well do you feel your institution is protected? Q15. Please tell us why you gave a score of xx? Q27.Would it be useful for you to see how your institution's security posture ranks against your peers?

Cyber security certifications HE

Cyber Essentials



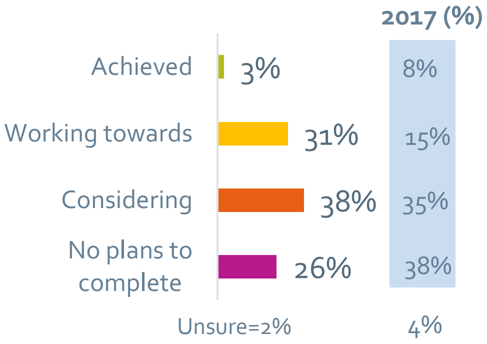
Year first achieved:

2018 n=3

2017 n=5

2016 n=1

Cyber Essentials Plus

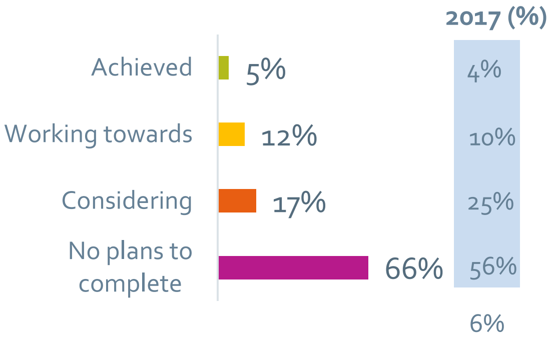


Year first achieved:

2018 n=1

2017 n=1

ISO27001



Year first achieved:

2017 n=2

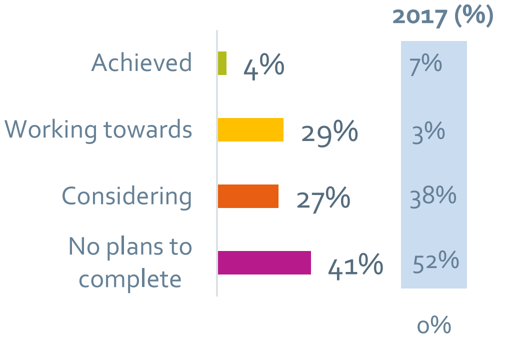
2014 n=1

Lower proportions of the HE organisations surveyed this year have achieved the Cyber Essentials and Cyber Essentials Plus certifications compared to 2017, although significant proportions are working towards both these qualifications currently. Slightly higher proportions report having achieved ISO27001 compared to 2017.

Q16. Does your institution have any of the following security certifications? Q17. In which year did your institution first achieve the x certification? Q18. What's the scope of your institution's x certification?

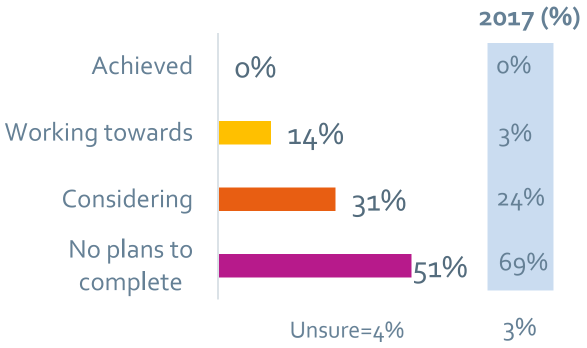
Cyber security certifications FE

Cyber Essentials

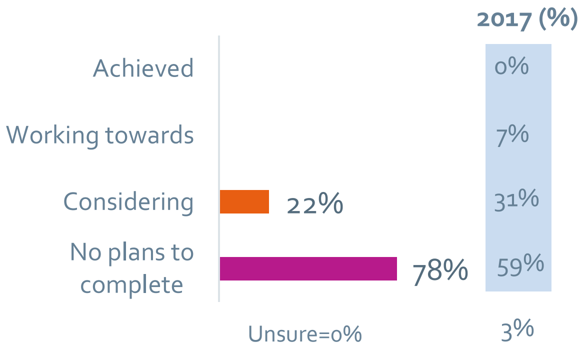


Year first achieved:
2018 n=1 2017 n=1

Cyber Essentials Plus



ISO27001



Much higher proportions of FE organisations are working towards Cyber Essentials and Cyber Essentials Plus compared to 2017, indicating it is increasingly seen as a must-have certification. No FE organisation this year reported working towards or achieving ISO27001.

Q16. Does your institution have any of the following security certifications? Q17. In which year did your institution first achieve the x certification? Q18. What's the scope of your institution's x certification?

Other cyber security training doing/considering

HE

Payment Card Industry Data Security Standard (PCI DSS)
multiple mentions

NHS Information Governance Toolkit (NHS IGT)
multiple mentions

Service Organization Control 2 (SOC2)

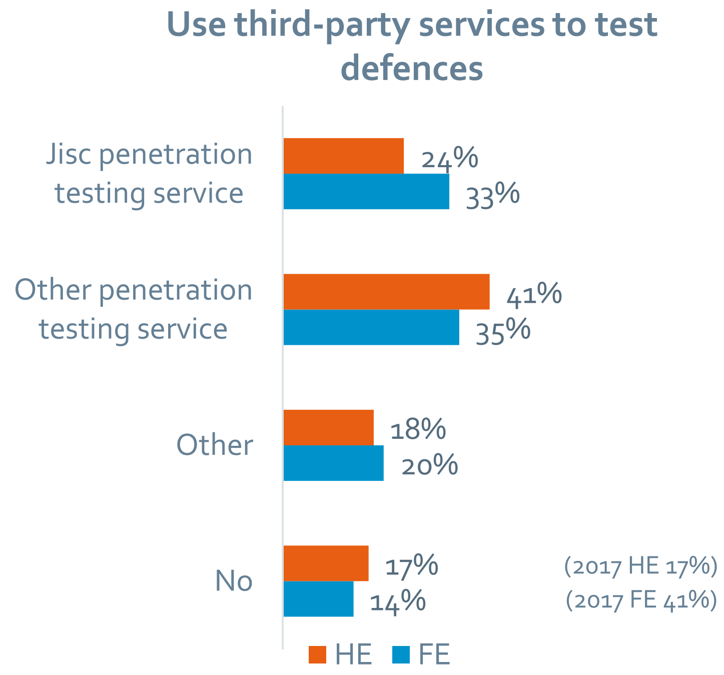
FE

Certified Ethical Hacker (CEH)

In terms of other cyber security training, PCI and NHS IGT training were the most likely to be mentioned by HE organisations. CEH was the only training mentioned by FE.

Q16d. Please tell us which other security certifications you have achieved already/are working towards/considering??

Use of third party services to test defences



Other penetration testing services used (supplier mentions)	
HE	FE
➢ Nessus n=2 ➢ Sec-1 n=2 ➢ 7safe n=1 ➢ Barclays n=1 ➢ Blackberry n=1 ➢ CGI n=1 ➢ Khipu n=1 ➢ Greenbone n=1 ➢ KPMG n=1 ➢ Red Team n=1 ➢ ECSC n=1 ➢ PWC n=1	➢ Sec-1 n=3 ➢ AppCheck n=1 ➢ C-ways n=1 ➢ Deloitte n=1 ➢ Infosec n=1 ➢ Practical Networks n=1 ➢ NCC n=1

24% of HE organisations surveyed use the Jisc penetration service and 41% report using another penetration service, with a number of providers mentioned. Within FE, use of third party services has risen since 2017. 33% use the Jisc service, comparable to the proportions using other penetration services, where Sec-1 is the most mentioned.

Q25. Do you use any third-party services to test your defences?

Use of third party services to gain insight/intelligence

66% HE (2017 HE 46%)

49% FE (2017 FE 31%)

use third-party services to gain insight/intelligence about current or emerging threats

Third party services used for insight (more than one response)	
HE	**FE**
➢ CISP n=11	➢ Sophos n=4
➢ NCSC n=8	➢ CISP n=3
➢ Newsletters/mailing lists n=7	➢ Sonicwall n=3
➢ Jisc n=4	➢ Jisc n=2
➢ Forums n=3	➢ Mailing lists n=2
➢ CISCO n=2	
➢ NHS n=2	
➢ Blogs n=2	
➢ Social media n=2	
➢ Khipu n=2	
➢ Microsoft n=2	

Use of third party services to gain insight/intelligence has risen since 2017 in both HE and FE. For HE, CISP and NCSC are the most popular providers with newsletters/mailing lists also proving popular. For FE, Sophos gets the most mentions.

Q26. Do you use any third-party services to gain insight/intelligence about current or emerging threats?

Cyber security threats and priorities

Cyber security threats

Top Threat Summary

(top 5 mentions-coded open end responses)

HE		FE	
Phishing and social engineering	n=26	Lack of awareness/accidents	n=13
Lack of awareness/accidents	n=11	Ransomware/malware	n=9
Ransomware/malware	n=6	Phishing/social engineering	n=9
Lack of secure processes/coordination/ policies/compliance	n=4	External attack	n=4
Attack from inside	n=3	DDoS	n=3

Similar to 2017, phishing and lack of awareness and accidents are the top threats listed by HE organisations, indicating that human error remains a key problem. Ransomware and Malware come in third. The results are similar for FE but with lack of awareness/accidents topping the list.

Q28. What do you feel are the three current biggest cyber security threats to your institution?

Cyber security threats

Top Three Threats Summary

(top 10 mentions- coded open end responses)

HE

Phishing & social engineering	n=41
Ransomware/malware	n=25
Lack of awareness/accidents	n=20
Patch management	n=15
Data breach/loss/leak	n=13
BYOD	n=10
Complacency/lack of responsibility /resistance from staff	n=7
Lack of secure processes/coordination /policies/compliance	n=7
External attack	n=7
Lack of oversight/monitoring of systems	n=6

FE

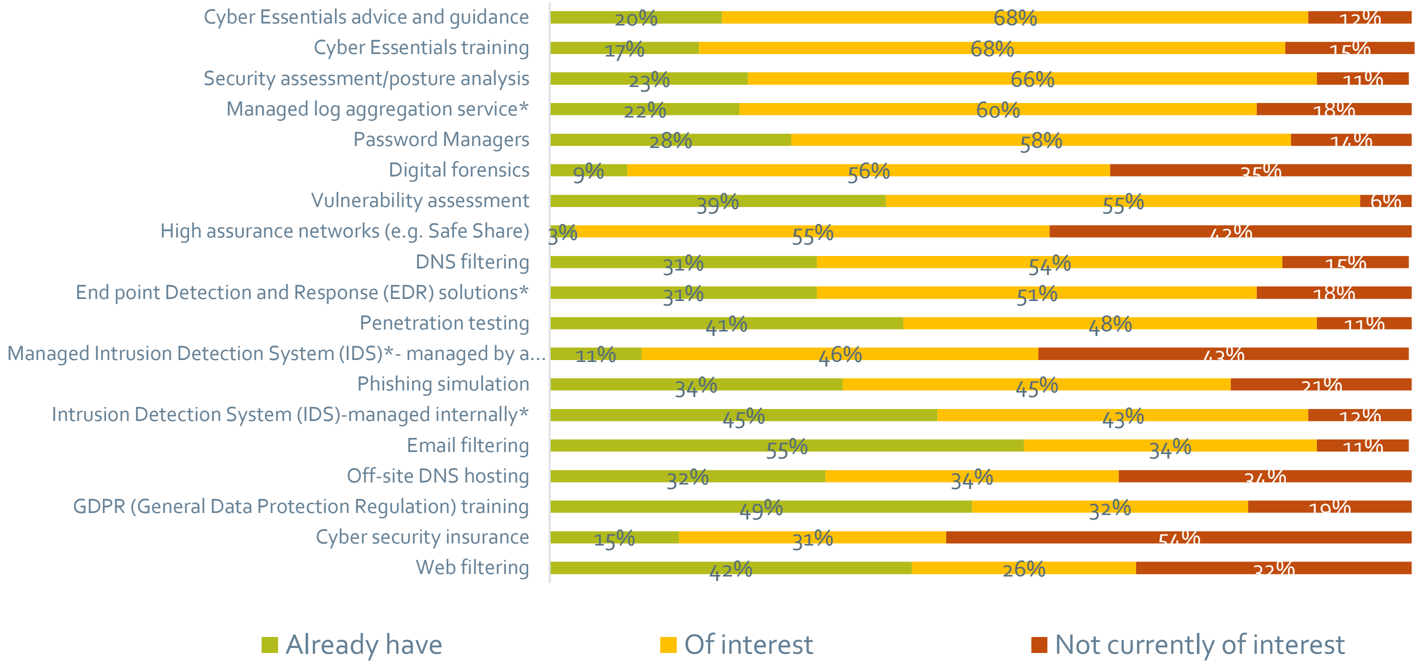
Ransomware/malware	n=31
Lack of awareness/accidents	n=19
Phishing & social engineering	n=17
DDoS	n=12
Hacking	n=9
Data breach/loss/leak	n=9
External attack	n=8
Budget/insufficient funding	n=7
Insider attack/threat	n=5
Lack of staff/resources	n=4
Complacency/lack of responsibility /resistance from staff	n=4

When looking at all threats listed, Phishing and social engineering top the list for HE and Ransomware/malware for FE and the top 3 threats listed for both sectors remain consistent with results from 2017. Patch management and BYOD are new entrants to the top 10 this year for HE. For FE, budgets/insufficient funding, lack of staff/resources and complacency are new for FE, indicating the constant squeeze on this sector.

Q28. What do you feel are the three current biggest cyber security threats to your institution?

Interest in Products/Services- HE

Interest- ordered by % "of interest"



Top 5 2017 (% total interested):**

1.GDPR training = 81%
2. Security posture analysis = 67%
3. Cyber Essentials training =62%
4. Cyber advice and guidance =58%
5. Phishing simulation =56%

*New categories in 2018

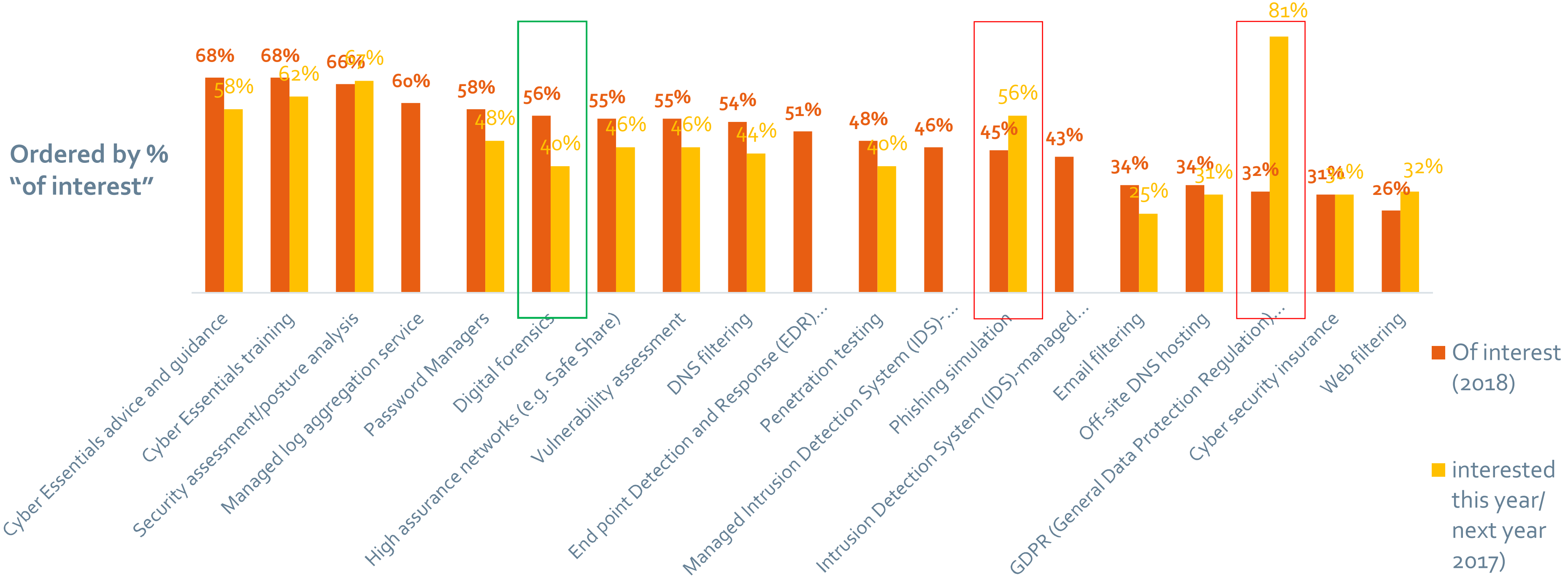
** answer options structured slightly differently in 2017:
Already have,
yes this year,
yes next year,
not currently of interest

By % of interest, Cyber Essentials training, advice and guidance and security assessment/posture analysis continue to top the list for HE. Interest in Password Managers and a managed log aggregation service replace GDPR training and phishing simulation to complete the top 5 in 2018.

Q29. Which of the following products or services would be of interest to you?

2018 vs 2017 Interest in Products/Services- HE

Ordered by % "of interest"

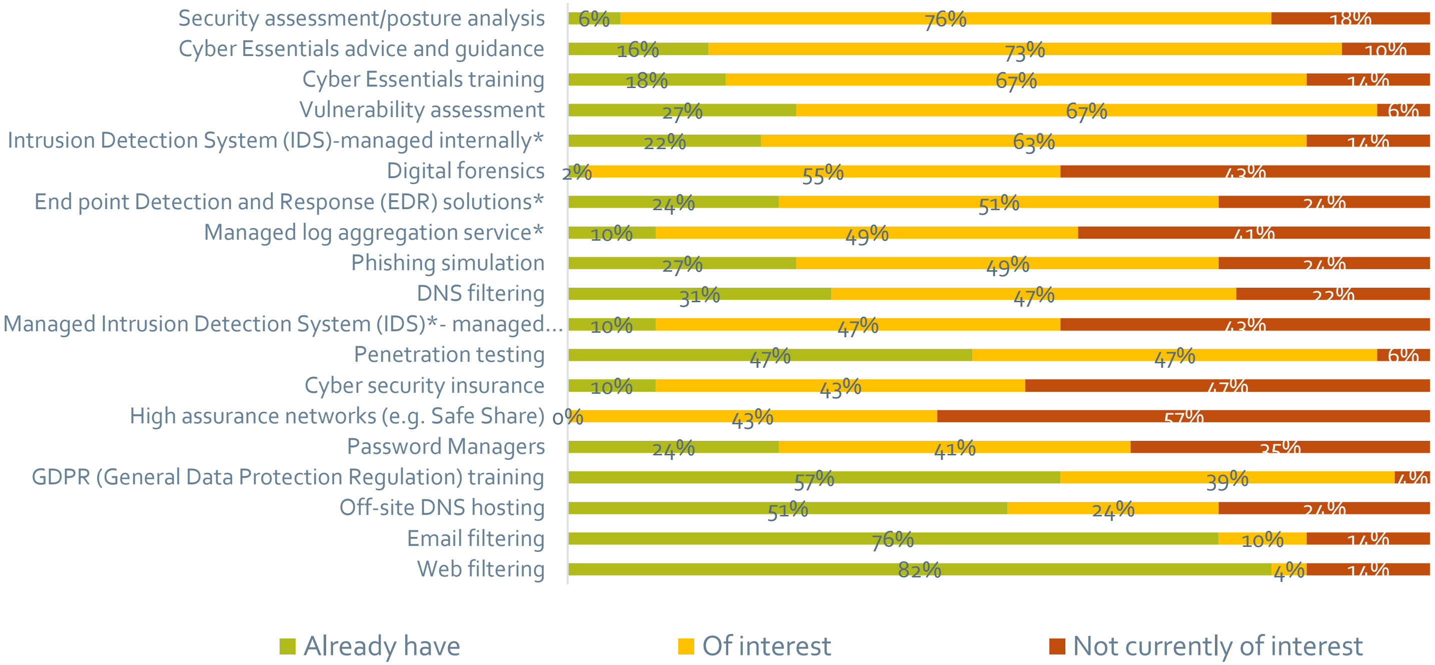


The biggest growth in interest since 2017 is for Digital forensics (6th place from 10th place), suggesting this is higher up HE members' agendas. Conversely, and not surprisingly, with the deadline passed interest in GDPR training has declined since 2017, with much higher proportions having already participated in training this year (49% vs 12% in 2017). There also seems to have been a decrease in interest in phishing simulation, which is likely driven by the fact that higher proportions of institutions already have this (34% vs 18% in 2017).

Q29. Which of the following products or services would be of interest to you? ** answer options structured slightly differently in 2017- Already have, yes this year, yes next year, not currently of interest

Interest in Products/Services- FE

Interest- ordered by % "of interest"



Top 5 2017 (% total interested):**

1. Cyber Essentials Training 83%
2. GDPR training 69%
3. Cyber advice and guidance 69%
4. Vulnerability Assessment 66%
5. Phishing Simulation 66%

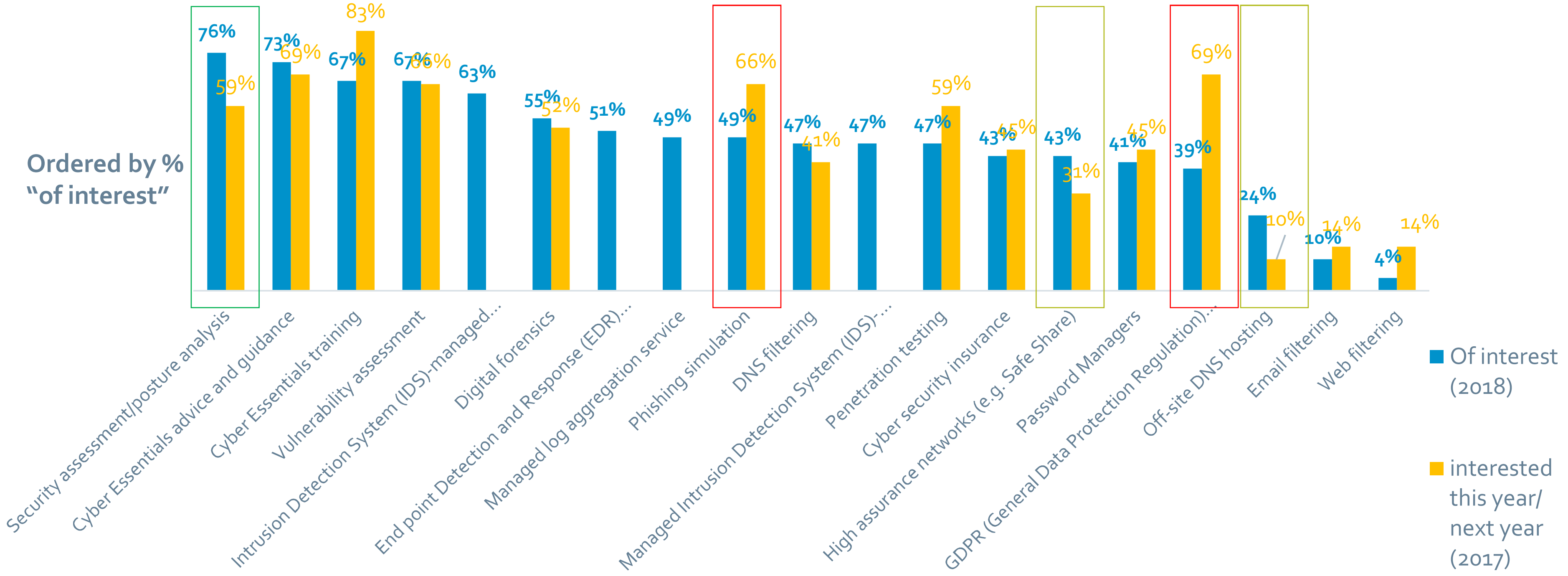
*New categories in 2018

** answer options structured slightly differently in 2017:
Already have,
yes this year,
yes next year,
not currently of interest

Cyber Essentials Training, advice and guidance, and vulnerability assessment remain in the top 5 for FE this year. Security assessment/posture analysis and Intrusion detection system (managed internally) have replaced GDPR training and phishing simulation as key products of interest.

Q29. Which of the following products or services would be of interest to you?

2018 vs 2017 Interest in Products/Services- FE



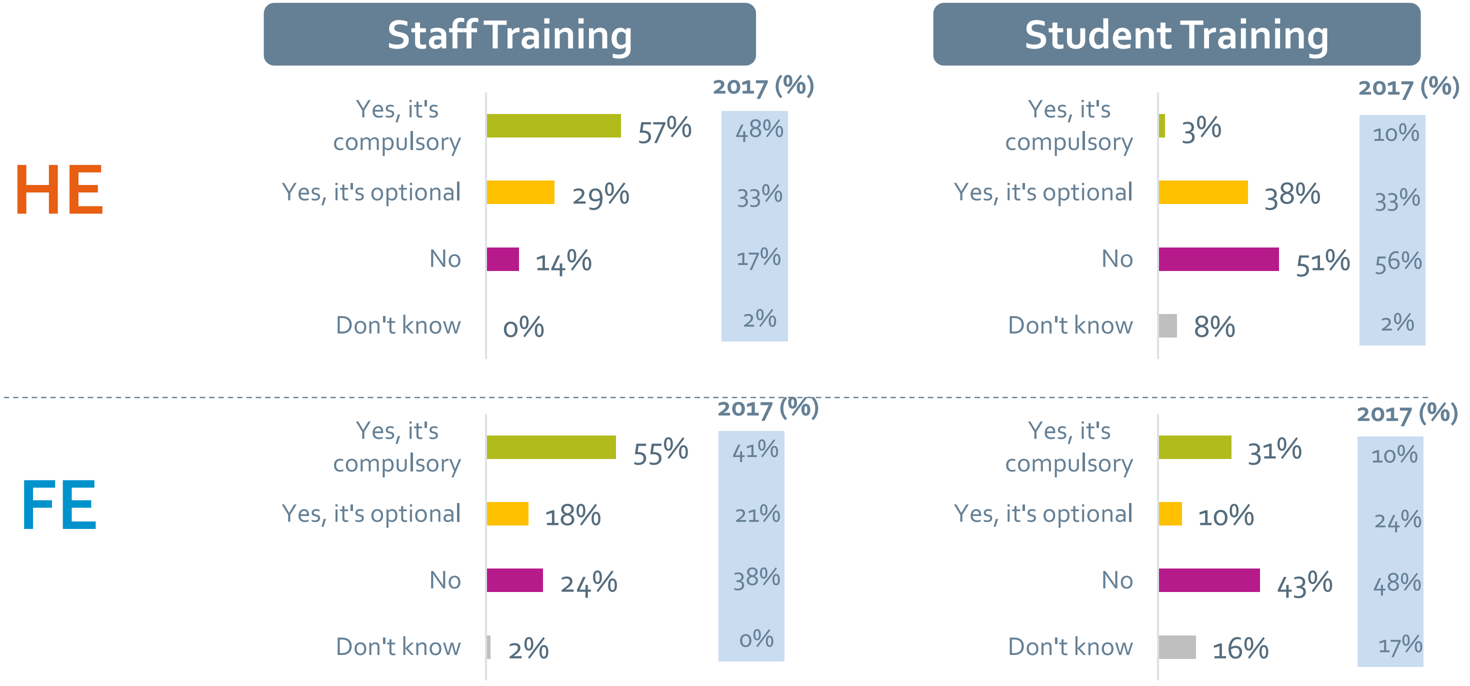
Ordered by % "of interest"

GDPR and Phishing simulation have seen decreases in interest, comparable to that in HE, which are most likely driven by increases in those who already have undertaken these services (GDPR 10% 2017 vs 58% 2018, Phishing 10% 2017 vs 28%). Services that have seen the largest increases in interest are security assessment/posture, which is now in top place, high assurance networks, and off-site DNS hosting.

Q29. Which of the following products or services would be of interest to you? ** answer options structured slightly differently in 2017- Already have, yes this year, yes next year, not currently of interest

Cyber security training

Information security awareness training



The proportions reporting compulsory staff security awareness training have increased since 2017, as has student training in FE. This suggests that organisations are increasingly acknowledging human error/lack of awareness as security risks. Has GDPR driven the need to address this? Interestingly, the proportions of HE organisations indicating they have compulsory student training have decreased, although optional training has increased. This might suggest changing approaches to engaging students in information security.

Q22. Do your staff undergo any information security awareness training? Q23. Do you students undergo any information security awareness training?

Types of information security training undertaken

HE

Training- subject not specified	n=16
UCISA training/package*	n=16
Information Security	n=15
GDPR/data protection	n=11
Phishing simulation/training	n=7
Cyber security	n=3
Jisc training	n=3
(security toolkit, online modules, security provision)	
Malware	n=2
Cyber Security Essentials	n=1
Records management	n=1
Safeguarding	n=1
Prevent	n=1
KnowBe4 online courses	n=1
Online security	n=1
Identity theft	n=1

FE

Training-subject not specified	n=14
Data protection/GDPR	n=7
Phishing	n=5
Basic IT training	n=3
Information security	n=3
eSafety	n=2
UCISA	n=1
Cyber security	n=1

* Some duplication with other categories e.g. information security.

UCISA's training packages were frequently mentioned by HE, as were GDPR, phishing, and information security training for both sectors

Q24. Please describe the type of information security awareness training undertaken by staff and/or students.

Contact

John Chapman

Head of Security Operations Centre

John.Chapman@jisc.ac.uk

jisc.ac.uk
0203 697 5800
We provide digital solutions for UK education and research
Embedding technology
Five steps to the strategic adoption of technologies in colleges