22/06/2017

Cybersecurity Posture Survey 2017 Research Findings

Jessica Francis, Research Manager Product & Improvement

John Chapman, Cybersecurity Compliance Manager

Summary of Key Findings I

Cybersecurity staffing:

- **Cybersecurity staffing and provision is more prevalent in HE than FE**. HE organisations are more likely to have dedicated cybersecurity posts (HE 72%, FE 3%), a strategic lead for cybersecurity (HE 55%, FE 30%) and staff available 24x7 to respond to security incidents (HE 20%, FE 10%) than FE organisations
- Where organisations have a **strategic cybersecurity lead, their role/job title varies**. **CISO and CIO are the most common**, with Heads of IT , COO & information Security Managers also likely to be fulfilling this role
- In HE, **Information Security Manager (47%), IT Security Manager (36%) & Information Security Officer (36%)** are the most **common dedicated Cybersecurity roles**. Only 6% of institutions with dedicated cybersecurity staff have Penetration Tester role/s
- In **FE organisations, where there are no dedicated cybersecurity staff or leads**, the **Heads of IT are the most likely to take responsibility for cybersecurity** as part of their role, followed by IT Managers or IT Network Managers

Cybersecurity budgets:

- **Within HE, rises have been seen in cybersecurity budget provision and the amount of money dedicated to this area**:
  - 40% had a specific cybersecurity budget in 2015/2016 vs a projected 58% in 2017/2018
  - The mean amount assigned to cybersecurity has risen by 132% from 16/17 to to a projected figure of £797,500 for 17/18
- **Within FE, the proportion of organisations with a dedicated cybersecurity budget has remained fairly stable at around 23-26%**
- **For both HE & FE, vulnerability management/self-testing is the key mechanism used to measure the effectiveness of their security** spending (HE 58%, FE 70%)
- For HE, this is followed by improved compliance (55%), reduction in attack surface (51%) & meeting strategic objectives (51%)
- For FE, this is followed by reduction in attack surface (50%) and reduction the number of breaches/compromises (43%)
- Speed and accuracy of response are only selected by 23% of HE/FE organisations as a measure to evaluate effective spending

Summary of Key Findings II

Current Cybersecurity Provision:

- **For HE institutions, perceptions of current Cybersecurity protection are not particularly positive**:
    - Institutions score a mean of 5.8 with only 14% scoring 8 or more when asked how well protected they are
    - Nearly all HE institutions surveyed (94%) indicate it would be useful to rank their security posture against their peers
- **FE organisations surveyed are more positive, although there is still room for improvement:**
    - Organisations score a mean of 6.8 with 33% of organisations scoring 8 or more
    - Less interest from FE in ranking institutions security posture against their peers, although still 87% felt it would be useful
- **HE organisations are more likely to have or be working towards cybersecurity accreditations than FE organisations:**
    - Cyber Essentials is the most popular security certificate for HE; 20% having achieved this already, 38% working towards this and 29% considering. This is in contrast to the ISO27001 certification where 57% indicate they have no plans to complete
    - Whilst only 10% of FE organisations have achieved or are working towards the Cyber Essentials, 40% are considering it
- **HE organisations are more likely than FE organisations to use third party services:**
    - 82% of HE and 57% of FE organisations use third party services to test their defences
    - 51% of HE and 30% of FE organisations use third-party services to gain insight/intelligence about current or emerging threats

Cybersecurity priorities:

- **For HE, the top cybersecurity priorities are protection & prevention, end user training/awareness and risk reduction**
- **For FE, these are protection & prevention, detection & response and risk reduction**
- **Most mentioned cybersecurity threats for both HE & FE relate to social engineering including phishing and human error**, driven by a lack of awareness/ignorance of the subject. Malware/Ransomware & Insider attacks were also commonly mentioned
- **HE are most interested in GDPR training, Cyber Essentials advice/guidance & Cyber Essentials training** as products/services
- Product priorities differ for **FE; Vulnerability assessment, phishing simulation and Cyber Essentials advice/guidance are most popular this year**

Summary of Key Findings III

Cybersecurity Training:

- Within both **HE and FE**, staff are more **likely to undertake information security awareness training than students:**
  - Only 8% of HE respondents and 10% FE respondents indicated student training in this area was compulsory, compared to 46% (HE) and 43% (FE) for staff
- **Information and data security training are the most commonly mentioned types of training undertaken across both HE and FE**
- Anti-phishing training is most consistently requested across HE & FE as a need going forwards, as well as GDPR within HE and training specifically aimed at staff in FE

Background
Objectives
Methodology

Background & Research Objectives

Background

Jisc identified a need to better understand institutions' security posture in light of the fast changing and increasingly critical area of cybersecurity.

In order to successfully provide the relevant 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.

Business Objective

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

Core Research Objectives

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

Methodology & Sample

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

95

completes

Survey In Field:

30th March - 6th June 2017

Type of Organisation	Number of completes	% of total completes
HE	65	68%
FE	30	32%

N.B results are reported by sector, but caution must be applied to FE results due to low base size

Cybersecurity Staffing

Cybersecurity Staffing Summary

	Have a strategic cybersecurity lead	Have dedicated cybersecurity posts	Have staff available 24x7 to respond to security incidents	Have a computer security incident response team	Have a security operations centre	Ask for specific security accreditations as part of person spec for security roles
HE	55%	72%	20%	51%	6%	29%
FE	30%	3%	10%	33%	7%	0%

- ➢ Cybersecurity staffing and provision is more prevalent in HE than FE:
    - ➢ 72% of HE organisations surveyed indicated they have dedicated cybersecurity posts within their organisation compared to only 3% of FE
    - ➢ Just over half (55%) of HE organisations indicate they have a strategic lead for cybersecurity vs 30% of FE organisations.
- ➢ Within both HE and FE the presence of a security operations centre was rare (6% and 7% respectively) and only 20% of HE and 10% of FE organisations surveyed said they have staff available 24 x 7 to respond to security incidents

Q4a. Do you have a have a strategic lead for cybersecurity at your organisation? (e.g. CISO, CIO or other lead role). Q5a. Do you have any dedicated cybersecurity posts in your organisation? Q10. Do you have staff available 24x7 to respond to security incidents? Q8. Do you have a Computer Security Incident Response Team? Q7.Do you have a Security Operations Centre? Q6. Do you ask for specific security accreditations as part of the person spec for any of your security roles? i.e. security+, CISSP.?

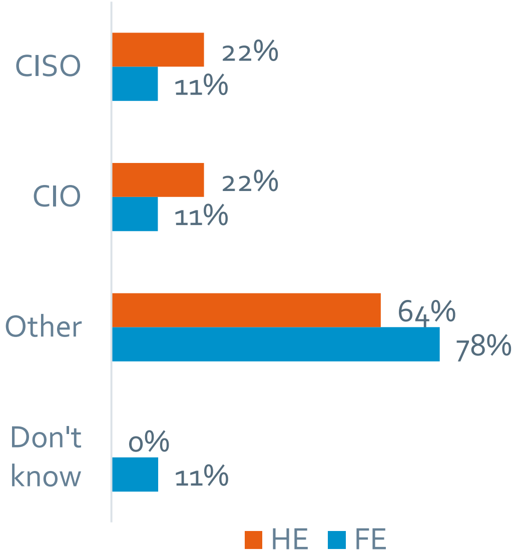
Presence of Strategic Cybersecurity Lead

55% Have strategic cybersecurity Lead (HE)

30% Have strategic cybersecurity Lead (FE)

Role/s of Cybersecurity Lead

(Base: those who have strategic lead)



HE other responses
COO n=3
Director of IT/IT services n=3
Information Security Manager n=3
Enterprise Architect n=2
Head of Information Security/services n=2
Assistant Director of IT n=1
CIO n=1
Head of Digital Architecture n=1
Head of Heritage & Information Governance n=1
Head of IT Governance n=1
SIRO n=1
University Registrar n=1

FE other responses
Director of IT/Head of n=4
COO n=1
Director & Finance & Corporate Services n=1
Smoothwall/Sophos n=1

For those organisations who indicated they have a strategic cybersecurity lead, their role/job title varied. CISO and CIO were the most common, with Heads of IT, COO & information Security Managers also most commonly fulfilling this role

Q4a. Do you have a strategic lead for cybersecurity at your organisation? (e.g. CISO, CIO or other lead role) Q4b. What role does your strategic lead for cybersecurity have?

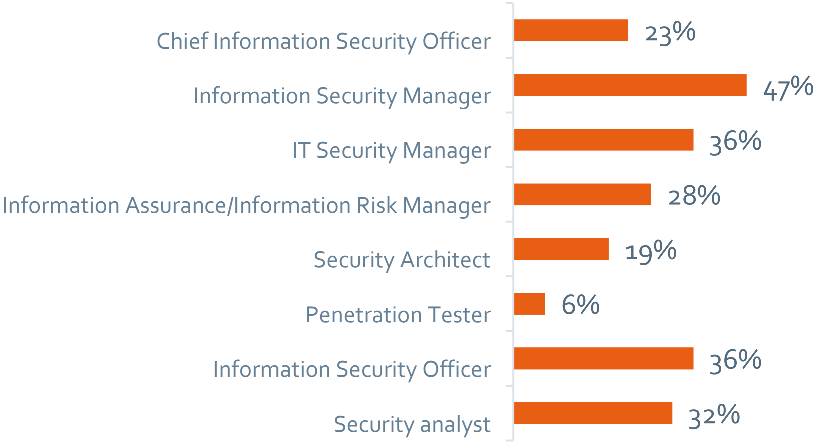
Dedicated Cybersecurity Staff

72% have dedicated cybersecurity staff (HE)

3% have dedicated cybersecurity staff (FE)

% who have staff in role

(Base:those who have dedicated cybersecurity staff)



Other roles: Security Engineer, Data Protection Officer, IT Security & ID Management Team, Information Compliance Advisor, Network Development Officer, Security Group Leader, Senior Network & Security Officer, Information Governance Manager. Cybersecurity part of other roles.

Only one FE organisation indicated they have dedicated cybersecurity staff in the role of **Senior Network & Security Officer**

Information Security Manager (47%), IT Security Manager (36%) and Information Security Officer (36%) were the most common roles found in HE that are dedicated to Cybersecurity. Conversely only 6% of HE organisations that have dedicated cybersecurity staff have those in a Penetration Tester role.

Q5a. Do you have any dedicated cybersecurity posts in your organisation? Q5b. Please tell us how many dedicated cybersecurity posts you have at each role (or equivalent) below? Q5J. Are there any other dedicated cybersecurity posts within your organisation? Please tell us which posts there are and number of roles that fit within this.

Institutions Without Dedicated Cybersecurity Staff

Those responsible for cybersecurity (where no dedicated staff)

HE	
CIO	n=2
Director of IT/ICT	n=2
COO	n=1
Infrastructure Engineer	n=1
Network & Server Engineer	n=1

FE	
Director/Head of IT/ICT	n=6
IT manager	n=3
IT Network Manager	n=3
Head of Computer services	n=1
Senior Infrastructure & Service Technician	n=1
Head of Information Systems	n=1
Head of Technical Services	n=1
Data Protection Officer	n=1
IT Support Team	n=1

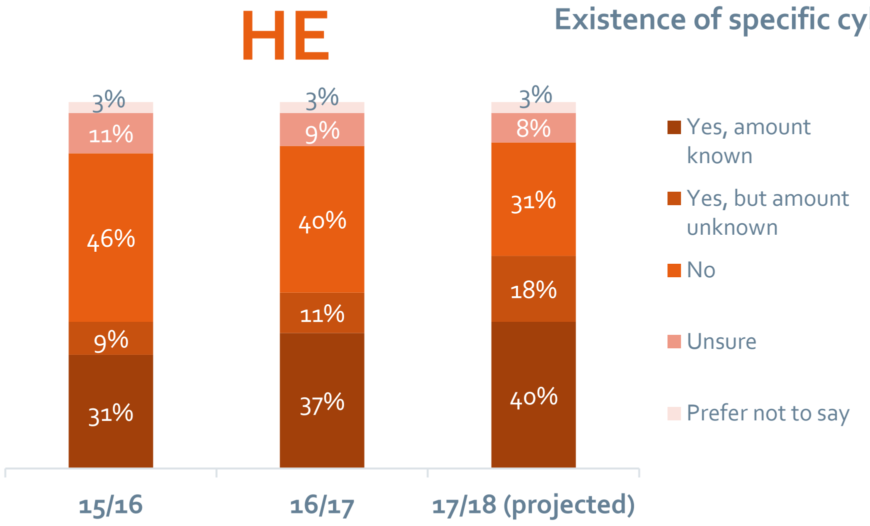
In FE organisations where there are no dedicated cybersecurity staff or leads, the Heads of IT are the most likely to take responsibility for cybersecurity as part of their role, followed by IT Managers or IT Network Managers

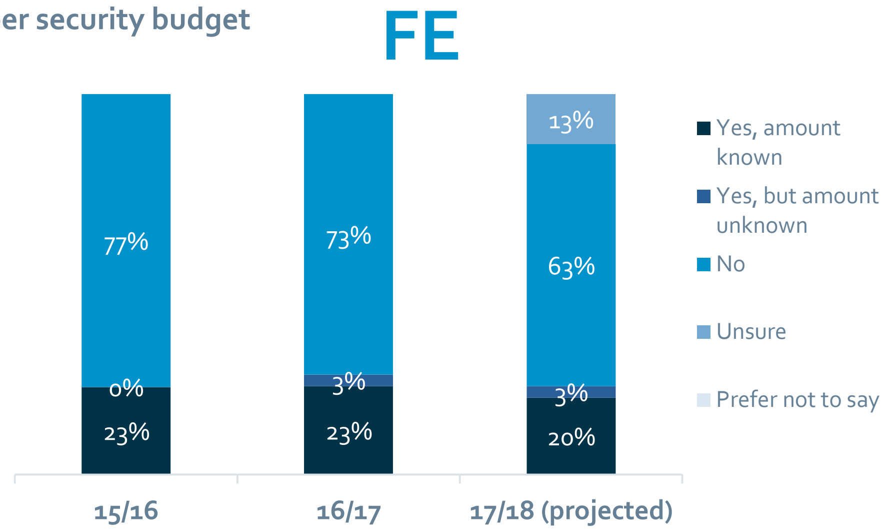
Q9. Who is currently responsible for cybersecurity at your institution?

Cybersecurity Budgets

Cybersecurity Budget Summary

Existence of specific cyber security budget





MEAN BUDGET (Base: those amount known)*		
£374,250	£343,750	£797,500

132%

MEAN BUDGET (Base: those amount known)*		
£12,143	£35,714	£25,000

* N.B caution, very small sample size

The proportion of HE organisations indicating they have a specific budget for cybersecurity (whether amount known or not) has risen from 40% in 2015/2016 to a projected 58% in 2017/2018. With FE this has remained fairly stable at around 23-26%.The mean budget assigned to cybersecurity in HE has risen by 132% from what is being spent in 2016/2017 to what is projected to be spent in 2017/2018.

Q11a. Do you have a specific cybersecurity budget (not including staffing costs)/. Please select one answer per row.? N.B. Prefer not to say and unsure excluded.

Measuring Effectiveness of Security Spending

HE

- 58% Vulnerability management/self-testing
- 55% Improved compliance
- 51% Reduction in attack surface
- 51% Meets strategic objectives
- 49% Reduction in no. breaches/compromises
- 23% Speed & accuracy of response
- 9% Other

Mean=3 measures selected

Measures used to evaluate effectiveness of security spending

FE

- 70% Vulnerability management/self-testing
- 50% Reduction in attack surface
- 43% Reduction in no. breaches/compromises
- 37% Improved compliance
- 27% Meets strategic objectives
- 23% Speed & accuracy of response
- 10% Other

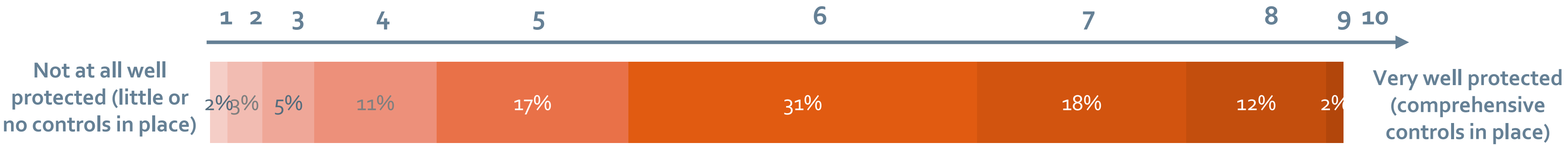
Mean=2.6 measures selected

- ➢ Vulnerability management/self-testing is the key mechanism for which both HE (58%) and FE organisations (70%) measure the effectiveness of their security spending.
- ➢ For HE, this is followed by improved compliance (55%), reduction in attack surface (51%) and meeting strategic objectives (51%)
- ➢ For FE, this is followed by reduction in attack surface (50%) and reduction the number of breaches/compromises (43%)
- ➢ For both FE and HE, speed and accuracy of response are only selected by 23% of organisations as a spending effectiveness measure

Q11d. How do you measure the effectiveness of your security spending? .

Cybersecurity Provision & Priorities

Cybersecurity Protection Perceptions HE



Mean score= 5.8

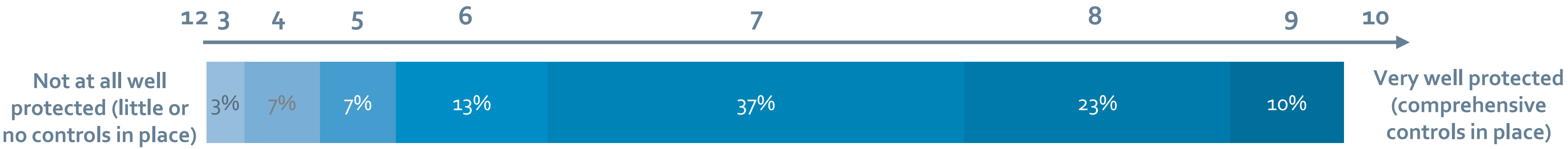
Rationale 1-4	Rationale 5-7	Rationale 8-10
➢ No security accreditations ➢ Culture of doing bare minimum ➢ Low on Senior Management priority list/not enough support ➢ At start of cybersecurity programme ➢ Limited staff/resources ➢ No joined up approach ➢ Audit results	➢ Starting from a low position, but improvements being made ➢ Some measures & GDPR helped impetus ➢ Legacy security tools/infrastructure ➢ Procurement barriers ➢ Apathy/reluctance from S. Management ➢ Inconsistent application of controls ➢ Struggling to keep up with change/risks ➢ Lack of investment ➢ Staff shortage/recruitment issues ➢ Low staff awareness	➢ Taken seriously & proactive approach ➢ Appropriate controls in place for type of organisation ➢ Staff are biggest threat ➢ Low incident count ➢ Processes, tech & training in place ➢ React quickly to problems ➢ Regular audits undertaken ➢ Invested heavily in areas

94% feel useful to rank institutions security posture against peers

Perceptions of current Cybersecurity protection are not particularly high amongst HE institutions with only 14% of those surveyed giving a score of 8 or more and a mean score of 5.8 emerging. Nearly all HE institutions surveyed (94%) indicated that it would be useful to rank their security posture against their peers.

Q13a. Thinking about cybersecurity, how well do you feel your institution is protected? Q13b. Please tell us why you gave a score of xx? Q21.Would it be useful for you to see how your institution's security posture ranks against your peers?

Cybersecurity Protection Perceptions FE



Mean score=6.8

Rationale 1-4	Rationale 5-7	Rationale 8-10
➢ Adhoc implementation of controls ➢ Cultural barrier; seen as making day-to-day business harder ➢ Legacy IT systems ➢ Lack of dedicated staff	➢ Insufficient in-house skill & expertise ➢ Budget constraints ➢ More could be done ➢ Systems in place, but no vulnerability/penetration testing ➢ Lack of monitoring activity ➢ New threats/vectors always emerging ➢ Doing well within the constraints ➢ Controls in place, but not formalised ➢ Some systems and controls in place	➢ Proactive, despite lack of dedicated team ➢ Recent audit positive, working towards ISO27001 ➢ Systems & policies in place, but no dedicated person ➢ Regular internal audits conducted ➢ All staff given training ➢ Can always do better!

87%
feel useful to rank institutions security posture against peers

FE organisations surveyed are more positive with 33% of organisations rating their protection as 8 or more and a mean score of 6.8. Lower proportions in this sector, albeit still 87% felt it would be useful to rank their organisations security posture against their peers.

Q13a. Thinking about cybersecurity, how well do you feel your institution is protected? Q13b. Please tell us why you gave a score of xx? Q21.Would it be useful for you to see how your institution's security posture ranks against your peers?

Cybersecurity Priorities

	HE					FE				
	% 1-4	% 5-6	% 7-8	% 9-10	mean	% 1-4	% 5-6	% 7-8	% 9-10	Mean
Discovery & forensics	31%	26%	29%	14%	5.8	23%	27%	37%	13%	6.1
Design/development	20%	28%	35%	17%	6.4	17%	23%	40%	20%	6.7
Security program or project management	18%	29%	32%	20%	6.3	27%	40%	27%	7%	5.6
Security staff training & certification	29%	17%	40%	14%	6	27%	23%	40%	10%	5.8
Governance/policies	14%	8%	38%	40%	7.7	3%	10%	53%	33%	7.9
End user training & awareness	8%	18%	26%	48%	7.9	7%	7%	33%	53%	8.3
Risk reduction	8%	15%	29%	48%	7.8	3%	13%	30%	53%	8.4
Compliance & audit	11%	17%	37%	35%	7.6	0%	17%	47%	37%	7.9
Detection & response	15%	12%	26%	46%	7.7	0%	10%	37%	53%	8.5
Protection & prevention	11%	9%	26%	54%	8.1	0%	7%	20%	73%	9.1

For the HE organisations, when looking at mean scores and % scoring 9/10, the top three priorities emerged as Protection & Prevention, End User training/awareness and risk reduction. For FE, these were Protection & Prevention, Detection & Response and Risk Reduction.

Q12d. How important do you feel the following cybersecurity areas are to your institution? Please select one answer per element.

Other Cybersecurity Areas of Importance

HE

Compliance- GDPR

Information management

Intelligence

Threat vector definition

Research certification

Response management

Phishing

Risk & assurance

Robust risk management governance & reporting

Staff & student awareness training

Lack of strategic priority given to cybersecurity

Lack of representation at senior level

Testing during project transition

FE

Budget constraints

Compliance- GDPR

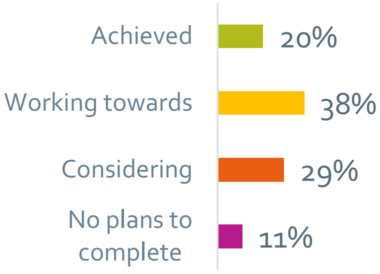
Limited funding

Q12k. Are there any other cybersecurity areas that are important to your institution?

Jisc

Cybersecurity Certifications HE

Cyber Essentials

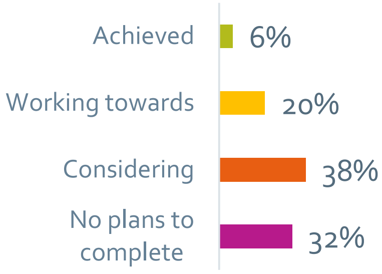


Unsure=2%

Year first achieved:

2017 n=4 2016 n=6
2015 n=2 2014 n=1

Cyber Essentials Plus

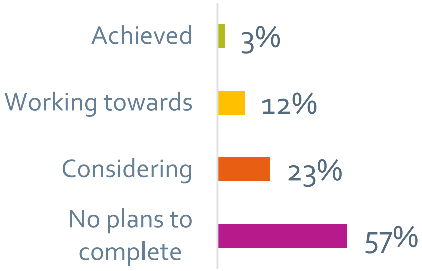


Unsure=3%

Year first achieved:

2017 n=2 2016 n=2

ISO27001



Unsure=5%

Year first achieved:

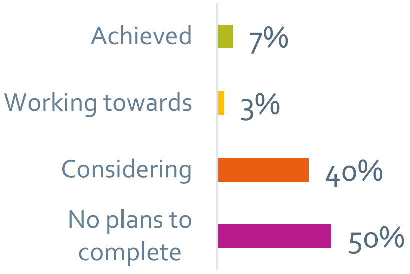
2017 n=1
2014 n=1

Cyber Essentials is the most popular security accreditation amongst HE organisations within the survey, with 20% having achieved this already, 38% working towards this and 29% considering. Only 11% have no plans to complete. This is in contrast to the ISO27001 certification where 57% indicate they have no plans to complete.

Q14a. Does your institution have any of the following security certifications? Q14. In which year did your institution first achieve the x certification? Q14. What's the scope of your institution's x certification?

Cybersecurity Certifications FE

Cyber Essentials

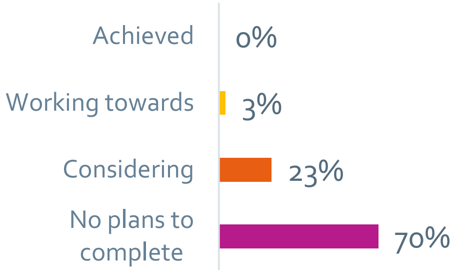


Unsure=0%

Year first achieved:

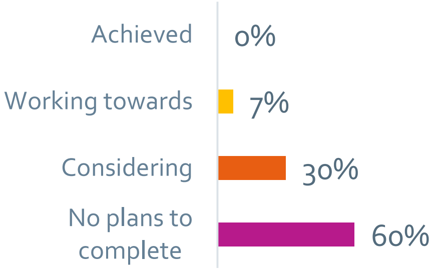
2017 n=2

Cyber Essentials Plus



Unsure=3%

ISO27001



Unsure=3%

Results suggest FE organisations within the survey are less likely to have security certifications or be working towards them, although 40% are considering a Cyber Essentials security certification

Q14a. Does your institution have any of the following security certifications? Q14. In which year did your institution first achieve the x certification? Q14. What's the scope of your institution's x certification?

Use of Third Party Services

82% HE

57% FE

use third-party services to test defences

Third party services used to test defences (more than one response)	
HE	FE
➢ Penetration testing n=42 ➢ Vulnerability assessment n=9 ➢ Audit n=2 ➢ Phishing/spam email test n=2	➢ Penetration testing n=10 ➢ Phishing/spam email test n=2 ➢ Vulnerability assessment n=2

51% HE

30% FE

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=12 ➢ Cisco n=2 ➢ Security blogs n=3 ➢ Mailing lists n=3 ➢ Janet CSIRT/Jisc n=3	➢ Newsfeeds/internet community resources/websites n=2 ➢ Sonicwall n=2

HE organisations are more likely than FE organisations to use third party services:

- ➢ 82% of HE institutions and 57% of FE organisations use third party services to test their defences
- ➢ 51% of HE institutions and 30% of FE organisations use third-party services to gain insight/intelligence about current or emerging threats

Q19. Do you use any third-party services to test your defences? Q. Do you use any third-party services to gain insight/intelligence about current or emerging threats?

Cybersecurity Perceptions

Cybersecurity Threats

Top Threat Summary

(top 5 mentions)

HE

Phishing/spear phishing/whaling/social engineering	n=25
Ignorance/lack of awareness/accidents	n=18
Attack from inside	n=6
Ransomware/malware	n=4
Complacency/lack of responsibility	n=2
Legacy systems/hardware	n=2

FE

Phishing/social engineering	n=23
Ignorance/lack of awareness/accidents	n=11
Ransomware/malware	n=7
Compliance	n=2
Data loss	n=2
Malware	n=2

When looking at the top threats listed, the most significant areas for both HE and FE appear to be those related to social engineering such as phishing and human error driven by a lack of awareness and ignorance of the subject area.

Q22. What do you feel are the three current biggest cybersecurity threats to your institution?

Cybersecurity Threats

Top Three Threats Summary

(top 10 mentions)

HE

Ignorance/lack of awareness/accidents	n=37
Phishing/spear phishing/whaling/social engineering	n=34
Ransomware/malware	n=11
Data loss/sharing/vulnerability	n=10
Attack from inside	n=10
Complacency/lack of responsibility/resistance	n=9
Lack of staff/resource	n=8
Lack of secure processes/co-ordination/policies	n=8
DDOS	n=5
Legacy software/hardware	n=4

FE

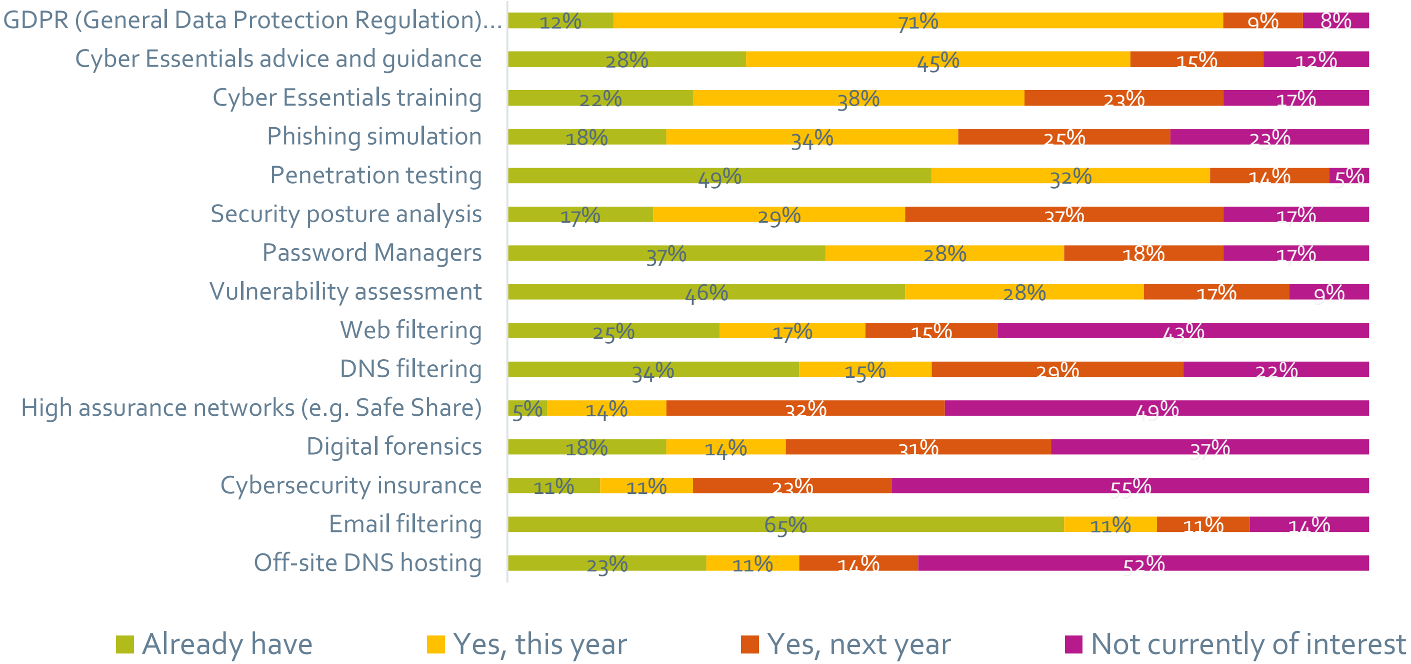
Lack of awareness/accidents	n=15
Ransomware/malware	n=13
Phishing/social engineering	n=12
Internal attack	n=4
Hacking	n=3
External attack	n=3
Compliance	n=3
USB keys	n=2
Poor patching	n=2
DDOS	n=2
Data loss	n=2
Legacy hardware/software	n=2

Again when looking at the total responses for the biggest current cybersecurity threats, lack of awareness and human error, social engineering relating threats and ransomware/malware issues come in the top three mentions for both HE and FE

Q22. What do you feel are the three current biggest cybersecurity threats to your institution?

Interest in Products/Services- HE

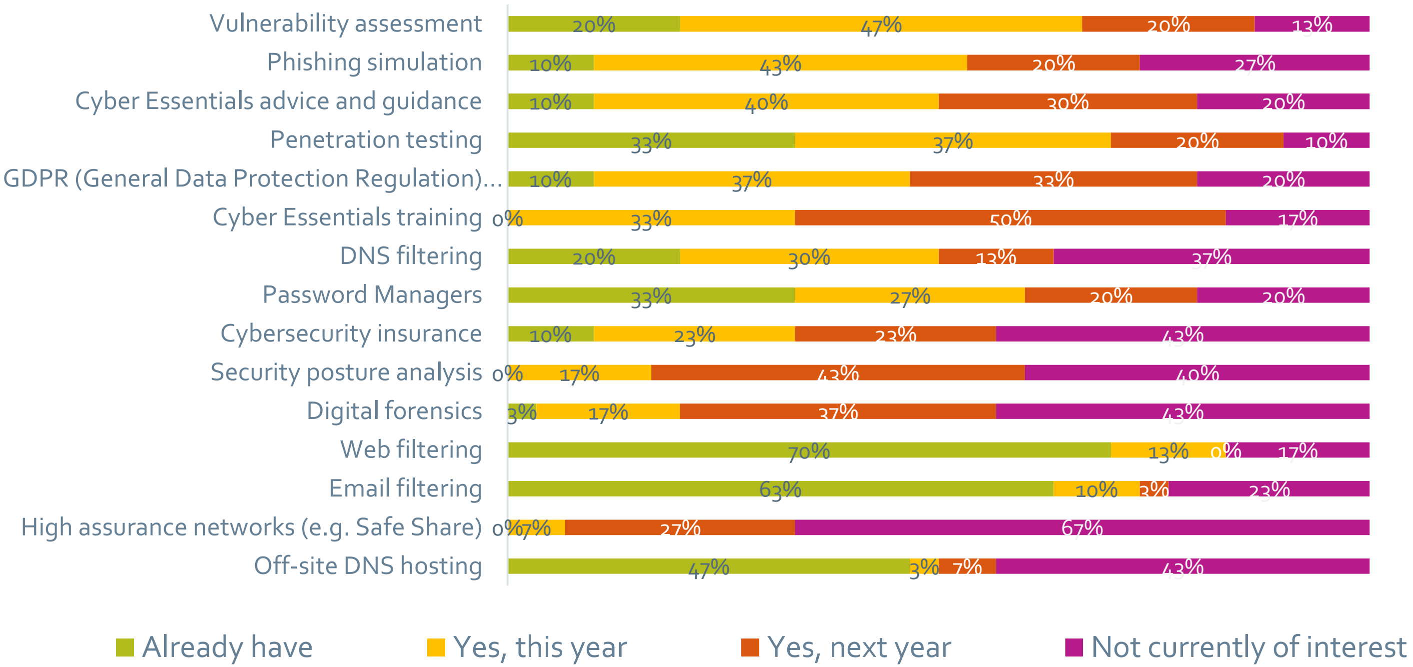
Interest- ordered by % “Yes, this year”



Looking at the proportions who indicated they are interested in these products/services this year, GDPR training, Cyber Essentials advice and guidance and Cyber Essentials training are the most popular for the HE institutions surveyed.

Q23. Which of the following products or services would be of interest to you?

Interest in Products/Services- FE

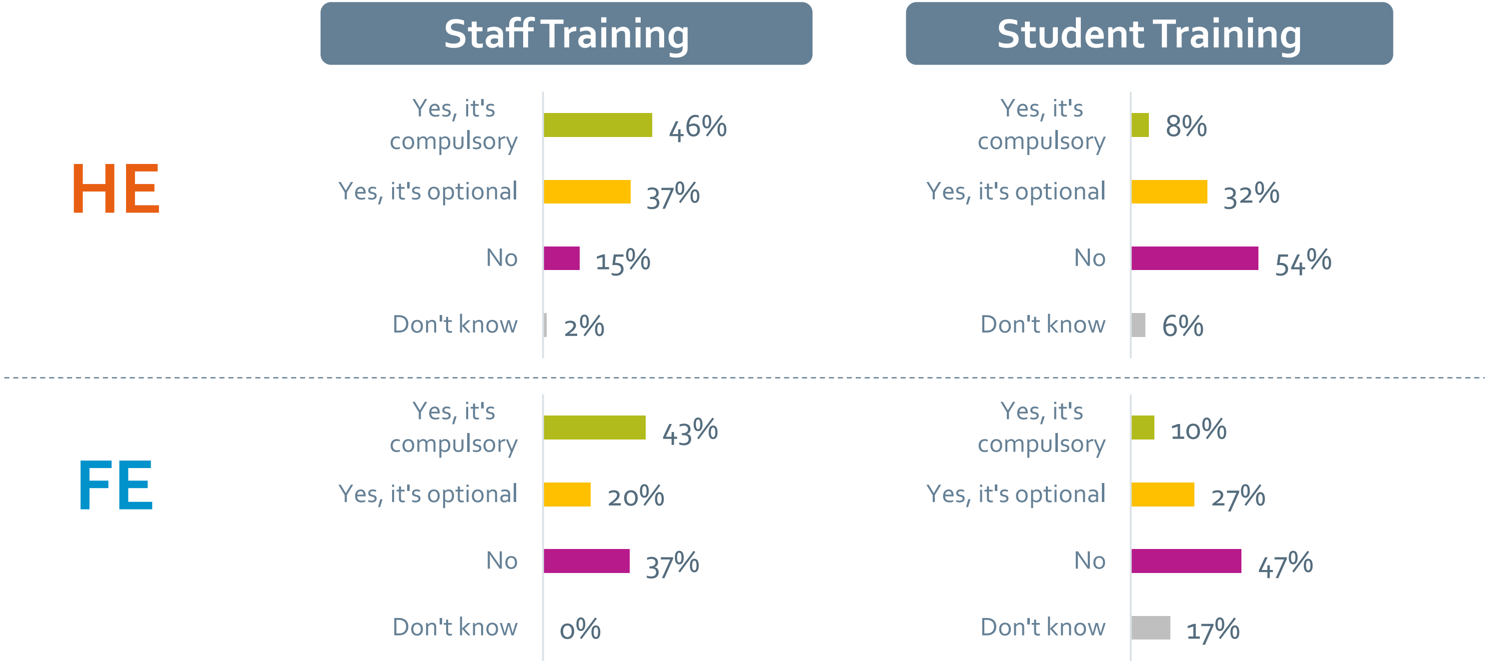

Interest ordered by % “Yes, this year”

For FE, their priorities are slightly different when looking at the proportions who indicated they are interested in these products/services this year, with vulnerability assessment, phishing simulation and Cyber Essentials advice and guidance being the most popular.

Q23. Which of the following products or services would be of interest to you?

Cybersecurity Training

Information Security Awareness Training



Within both HE and FE, staff were more likely to undertake information security awareness training than students. Only 8% of HE respondents and 10% FE respondents indicated student training in this area was compulsory in their organisation, compared to 46% (HE) and 43% (FE) for staff.

Q15. Do your staff undergo any information security awareness training? Q16. Do you students undergo any information security awareness training?

Cybersecurity Training

Types training undertaken

HE

Information Security	n=9
Data protection	n=7
UCISA data security	n=6
IT security/general training	n=5
Computer security	n=2
Data Governance	n=2
Staying safe online	n=1
CBT	n=1
Data safe haven	n=1

FE

General security training	n-4
Information security	n=3
Safe use of IT	n=2
CBT	n=1
Data protection	n=1
Password management	n=1
Phishing	n=1
Mobile device use	n=1
Cyberbullying	n=1

Other Training Interests

HE

(Due to response volume, more than one mention listed only)

Anti-phishing/simulated phishing	n=7
GDPR	n=4
Student focussed training	n=3
Basics: link checking, forged emails	n=2

FE

(Due to response volume, more than one mention listed only)

Training specifically for FE staff	n=3
Scanning links/phishing	n=3
Video training	n=2
Student training	n=2

General training that covers information and data security are the most commonly mentioned types of training undertaken across both HE and FE. Anti-phishing training is consistently requested across HE and FE in terms of training needs going forwards, as well as GDPR within HE and training specifically aimed at staff in FE

Q17. Please describe the type of information security awareness training undertaken by staff and/or students. Q18. Is there any other cybersecurity related training that you think would be useful that you don't currently provide at your institution?

Contact

John Chapman, Cybersecurity Compliance Manager

john.chapman@jisc.ac.uk

01235 822 346

12:57 pm
jisc.ac.uk
Jisc
0203 697 5800
Search Jisc
MENU
We provide digital solutions for UK education and research
Embedding technology
Five steps to the strategic adoption of technologies in colleges
Jisc