Cyber security posture survey results 2022
A snapshot of the cyber security landscape in Higher education
November 2022
• Cyber security remains high priority at a senior level, evidenced by inclusion on risk registers for most and reporting of security risks/resilience to executive boards.

• The numbers of organisations with dedicated cyber security staff continues to rise with 90% reporting dedicated staff this year. 24/7 cover is still most likely to be provided on a best-efforts basis by staff who are contactable in an emergency.

• Perceptions of cyber security protection have remained broadly consistent with the overall mean score (on a scale of 1-10) at 6.4. Comments suggest that, while solid processes and controls are being implemented and certifications help with assessment, organisations feel that the changing threat landscape means that more can always be done.

• We have seen a slight a dip in the numbers of organisations achieving Cyber Essentials for the second year in a row. While the majority of organisations with the certificate intend to recertify, a number express concerns about meeting the requirements and some question whether something more appropriate for HE may be needed.
Headlines (2)

• Ransomware/malware is seen as the top threat for HE for a second year. With accidental data breaches also ranking high on the list of threats, the implementation of training for staff remains a priority, with a high proportion required to undertake this every year. Student training is less common.

• Multi-factor authentication (MFA) has increased this year, with a rise in the proportion of organisations deploying to both staff and students. There is a marked increase in student deployment in HE, with 80% reporting deployment to some or all students. Responses in 2020 and 2021 suggested that the increase in remote working due to the pandemic had expediated MFA implementation, and the roll-out appears to be continuing.
Background and sample
Method and sample

In June 2022 we surveyed Jisc members and customers about their cyber security posture and governance. We had 123 completes overall, a decrease of 30% compared to 2021.

This report gives an institutional view and covers HE responses (n=62). Where the same organisation submitted multiple times, the most senior/relevant staff member's response was included. 7 responses were removed from the HE dataset.

The HE sample represents 38% of the Jisc HE membership. 5% of the HE sample responded for the first time in 2022. Variations in sample size mean that trend data should be interpreted in this context.

Results cannot be generalized to the wider sector, however the findings invite conversations about potential watchpoints and solutions around cyber security.

Where information was available, organisations were classified by size based on number of total students. However, sample sizes are small and so any differences in response are indicative only.

<table>
<thead>
<tr>
<th>HE 2022 (n=62)</th>
<th>n=</th>
</tr>
</thead>
<tbody>
<tr>
<td>(38%, 62/164)</td>
<td></td>
</tr>
<tr>
<td>Large (&gt; 20,000 students)</td>
<td>20</td>
</tr>
<tr>
<td>Small (&lt; 20,000 students)</td>
<td>40</td>
</tr>
<tr>
<td>No information available</td>
<td>2</td>
</tr>
</tbody>
</table>

*Data Sources: Jisc CRM, HE student numbers= HESA | FE Student numbers= Education and skills funding agency (England), Department for the Economy (Northern Ireland), Scottish Funding Council (Scotland), Stats Wales (Wales).
Cyber security governance, structure and operations
Priority given to cyber security

Almost all (97%) indicate that cyber security appears on their risk register, a rise of 2 percentage points compared to 2021. Further evidence of strategic importance is also evidenced by the high numbers of organisations that regularly report on cyber security risks and resilience to their executive board (87%).

Q3: Does cyber security appear on your organisation’s risk register?

HE 97%

Q4: Do you or a colleague regularly report on cyber security risks and resilience to your executive board?

HE 87%
Dedicated cyber security roles

56 (90%) have dedicated cyber security roles and the proportion continues to rise, with an increase of 21 percentage points in HE since 2017. Larger organisations are more likely to report dedicated cyber roles. Large organisations with dedicated staff report an average of 6.1 posts (range=1-12), while smaller institutions report an average of 3.9 (range=1-11).

Q5. 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

Security Analyst, IT Security Manager, and Information Security Manager are most common overall, which matches the results in 2021.

- As in 2021, large organisations are more likely to have senior roles with 45% of those with cyber staff reporting a Chief Information Officer (63% in 2021) compared to 28% of smaller organisations. 50% of large organisations have a Chief Information Security Officer (50% in 2021) compared to 25% of smaller organisations.
- For those who report having a CISO, this role mostly reports to the CIO or lead IT role in the organisation.
- Comments suggest that some staff work across roles, and some are part-time roles.

Q5. Do you have any dedicated cyber security roles in your organisation?
Q6. How many dedicated cyber security posts do you have at each role?
Availability of staff to respond 24/7

24/7 cover is mostly provided by staff that are contactable in an emergency on a ‘best efforts’ call out and only 5% have formal staff contracts for 24/7 cover. Resource is a core issue, with 29% unable to cover 24/7 currently.

Q10. Do you have staff available 24/7 to respond to security incidents?

- Yes, staff work on call as a formal part of their contract: 5%
- Yes, staff are contactable in an emergency: 53%
- Yes, outsource to a third party: 13%
- No, not a requirement: 11%
- No, no resource to cover 24/7: 29%
Posture
Cyber security protection perceptions

Continuing the trend of the last six years, HE organisations are cautious about their posture score, with only 16% (10 institutions) scoring 8+.

Comments suggest that organisations in the 5-7 bracket feel that they have controls and processes already in place (e.g. MFA and SIEM) but that there is more that can be done to keep up with threats in the sector. Organisational culture and staff resource are also referenced as ways to monitor and manage cyber posture. For those who scored 8-10, the importance of robust systems and processes were key themes, along with audits, frameworks and certification.

<table>
<thead>
<tr>
<th>HE</th>
<th>Not at all well protected</th>
<th>Mean score = 6.4</th>
<th>Very well protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-4</td>
<td>11%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-7</td>
<td>73%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8-10</td>
<td>16%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q11. Thinking about cyber security, how well do you feel your organisation is protected?
Q12. Please tell us why you gave your organization a score of x?
Perceptions of cyber security protection have remained broadly consistent over the last three years, with little change to the mean score from 2020 to 2022.

Q11. Thinking about cyber security, how well do you feel your organisation is protected?
## Protection perception rationale HE

<table>
<thead>
<tr>
<th>Rationale scores 1-4 (n=8)</th>
<th>Rationale scores 5-7 (n=47)</th>
<th>Rationale scores 8-10 (n=11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Need to implement additional processes or products (5)</td>
<td>• Some controls/processes in place, but... (26)</td>
<td>• Good/solid controls in place (4)</td>
</tr>
<tr>
<td>• Culture priorities in the organisation (3)</td>
<td>• Need to implement additional processes or products (14)</td>
<td>• Certifications and frameworks (have or working towards) (4)</td>
</tr>
<tr>
<td>• Some controls/processes in place, but... (2)</td>
<td>• Culture priorities in the organisation (8)</td>
<td>• Need to implement additional processes or products (3)</td>
</tr>
<tr>
<td>• Limited or siloed staff expertise (1)</td>
<td>• Always more to do (generic) (7)</td>
<td>• Always more to do (generic) (2)</td>
</tr>
<tr>
<td>• Always more to do (generic) (1)</td>
<td>• Resource, e.g. staffing or finance (7)</td>
<td>• Culture priorities in the organisation (2)</td>
</tr>
<tr>
<td>• Certifications and frameworks (needs improvement) (1)</td>
<td>• Certifications and frameworks (have or working towards) (5)</td>
<td>• Dedicated staff expertise (1)</td>
</tr>
</tbody>
</table>

### Q12. Please tell us why you gave your organisation a score of x?
68% indicate they have completed a self assessment in the last 12 months. The majority of organisations intend to use use Cyber Essentials for their next assessment, with the NCSC Cyber Assessment Framework as the next most popular option.

Q14. Which tools, models or frameworks are you most likely to use for your next assessment?

- Cyber Essentials: 81%
- NCSC Cyber Assessment Framework: 27%
- Own internal risk assessment: 21%
- NCSC 10 Steps: 21%
- CIS Controls: 19%
- ISO27001: 16%
- PCI-DSS: 18%
- NIST Cyber Security Framework: 13%
- Public Sector Action Plan: 6%
- PSN-ITHC: 2%

Other options:
- NHS Digital DSPT
- Jisc 16 cyber questions
- Consultant's own
- Gartner maturity score

Q13. The Janet Security Policy requires all organisations connected to the Janet network to undertake an annual self-assessment security posture review to ensure awareness of strengths and weaknesses regarding security controls and culture. Have you completed a self-assessment in the past 12 months?
Record of technology assets

Only 16% maintain a complete or near complete asset register and organisations are more likely to have a register that doesn’t contain all assets (73%). Five organisations (8%) do not maintain a register.

Q15. Do you maintain a record of technology assets?

- Yes, we maintain a complete, or near complete, asset register: 16%
- Yes, we maintain an asset register but it doesn’t contain all assets: 73%
- No: 8%
- Don’t know: 3%
Offsite secondary DNS capability

66% report an offsite secondary DNS capability.

Q37: Do you have an offsite secondary DNS capability?
Certification
The proportion of HE organisations with Cyber Essentials has fallen slightly again in 2022, but we have seen a rise in organisations with Cyber Essentials Plus and ISO 27001, bringing this closer to the percentages reported in 2020.

- Across the responding organisations, 21(34%) have none of the certifications and two have all three. 18 (29%) have Cyber Essentials only and 14 (23%) have both Cyber Essentials and Cyber Essentials Plus.

- Comments from the sector over the last two years suggest that home working, bring your own device (BYOD), and changes to the Cyber Essentials requirements are all contributing to the fall in participation, with some questioning the suitability of the scheme for education environments.

Q16. Does your organisation have any of the following security certifications?
Certifications - Cyber Essentials (CE)

Most organisations have achieved or are working towards CE and the majority (84%) intend to recertify. Reasons given for not recertifying include the changes to requirements (BYOD), questions around the suitability for HE environments, and a lack of direction from senior management.

Only three organisations with CE have ‘whole organisation’ as the scope, while the scope is more likely to refer to specific departments (9 mentions), managed services/devices (9 mentions) or the core/corporate networks (9 mentions).

Q16. Does your organisation have any of the following security certifications?
Q17. If you have Cyber Essentials, will you be recertifying?
Q22. Why do you have no plans to complete Cyber Essentials?

- 84% of HE organisations with CE intend to recertify: 47% with the same scope, 31% with an increased scope, and 6% with a reduced scope.
- 7 of the 9 HE organisations with no plans to complete CE are not able to meet current requirements.
Certifications - Cyber Essentials Plus (CE+)

Over half of responding institutions have achieved or are working towards CE+. As with CE, most (68%) intend to recertify but comments indicate concerns about whether the scheme is fit for purpose and BYOD requirements make it difficult to meet the criteria.

Again, in HE, the scope is more likely to refer to specific departments (5 mentions), managed services/devices (4 mentions) and the core/corporate networks (5 mentions).

Q16. Does your organisation have any of the following security certifications?
Q18. If you have Cyber Essentials, will you be recertifying?
Q23. Why do you have no plans to complete Cyber Essentials?

21 Cyber security posture survey results 2022
For ISO27001 the scope mostly covers individual business units, departments or research groups.

- **Achieved**: 11%
- **Working towards**: 7%
- **Considering**: 27%
- **No plans to complete**: 53%
- **No plans to complete but have in past**: 2%

- All 7 HE organisations with ISO27001 intend to recertify: 6 with the same scope, and 1 with an increased scope.
- 20 (59%) of HE organisations with no plans to complete ISO27001 are focussing on a different certification and 18 (53%) cite a lack of resource.

**Q16.** Does your organisation have any of the following security certifications?
**Q19.** If you have Cyber Essentials, will you be recertifying?
**Q24.** Why do you have no plans to complete Cyber Essentials?
Information security training
Compulsory training is more common for staff than students, with 84% implementing this. As in previous years, compulsory student training is less common in HE (5%).

Q25. Do your staff undergo information security awareness training?
Q26. Do your students undergo information security awareness training?
Cyber security training over time

The proportion of organisations who indicate they have some form of compulsory staff training has risen slightly in HE compared to 2021, but compulsory student training remains low, with little change since 2019.

Q25. Do any of your staff undergo information security awareness training?
Q26. Do any of your students undergo information security awareness training?
Information security training frequency

For staff, annual training is most common with induction and HR or IT processes the main ways of monitoring this. Mandatory training is common, and many report enforcement via line management or senior management. Few mention loss of access or rights, although some comments suggest this is under review. For those with training for students, they are likely to require this only once through onboarding or induction.

<table>
<thead>
<tr>
<th>Frequency of information security awareness training for staff</th>
<th>Frequency of information security awareness training for students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Once</td>
<td>14%</td>
</tr>
<tr>
<td>Every year</td>
<td>39%</td>
</tr>
<tr>
<td>Every 18 months</td>
<td>4%</td>
</tr>
<tr>
<td>Every two years</td>
<td>26%</td>
</tr>
<tr>
<td>Less frequently</td>
<td>16%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>2%</td>
</tr>
</tbody>
</table>

Q27. How often are staff expected to complete information security awareness training?
Q28. How often are students expected to complete information security awareness training?
Q29. How is compulsory information security training enforced?
Multi-factor authentication
Multi-factor authentication (MFA) in HE

Organisations are more likely to deploy MFA to staff than students, with all deploying to at least some staff.

- 100% of HE deploy MFA to some or all staff, a rise of 13 percentage points compared to 2021 (87% in 2021)
- HE organisations reporting MFA for some or all students has risen by 31 percentage points, at 80% (49% in 2021)
- One HE organisation is considering deployment, giving their reasons for non-deployment to date as lack of time.
- For those who have deployed to some staff IT, domain admins and security staff are the top three categories. Students in specific schools/departments have MFA deployed.
- For those who have not deployed MFA, lack of resource is the main reason, followed by platform integration issues and lack of time.

% HE deploying MFA to staff

<table>
<thead>
<tr>
<th>Deployed MFA</th>
<th>HE deploying MFA to staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, to all staff</td>
<td>87%</td>
</tr>
<tr>
<td>Yes, to some staff</td>
<td>13%</td>
</tr>
<tr>
<td>No, but working towards</td>
<td>0%</td>
</tr>
<tr>
<td>No, but considering</td>
<td>0%</td>
</tr>
<tr>
<td>No plans to deploy</td>
<td>0%</td>
</tr>
</tbody>
</table>

% HE deploying MFA to students

<table>
<thead>
<tr>
<th>Deployed MFA</th>
<th>HE deploying MFA to students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, to all students</td>
<td>61%</td>
</tr>
<tr>
<td>Yes, to some students</td>
<td>19%</td>
</tr>
<tr>
<td>No, but working towards</td>
<td>10%</td>
</tr>
<tr>
<td>No, but considering</td>
<td>8%</td>
</tr>
<tr>
<td>No plans to deploy</td>
<td>2%</td>
</tr>
</tbody>
</table>

Q30. Have you deployed MFA for staff within your organisation?
Q31. Have you deployed MFA for students within your organization?
Multi-factor authentication over time

Trend data suggest that MFA rollout has become more of a priority over the three years we have asked this question. The numbers of HE organisations deploying MFA to some or all students has risen by 58 percentage points since 2020, which could be a lasting impact of the COVID-19 pandemic and increase in flexible working/learning.

% with MFA for all or some staff

- 2020: 72%
- 2021: 87%
- 2022: 100%

% with MFA for all or some students

- 2020: 22%
- 2021: 49%
- 2022: 80%
Multi-factor authentication for systems and services

44% implement MFA on all relevant systems and services. For those that answered no, the majority implement on most critical systems and services.

Of the 55% who do not implement for all:

- 3% implement for all critical systems and services
- 53% implement for most critical systems and services
- 38% implement for some critical systems and services
- 6% do not implement for all critical services

Q34. Have you implemented MFA authentication for all relevant systems and services?
Q35. Have you implemented MFA on all your critical systems and services?
Threats and insurance
Cyber security concerns

Ransomware/malware is the top concern, with 34 (55%) ranking this as their no. 1 threat. Phishing/social engineering is ranked 2\textsuperscript{nd} with unpatched security vulnerabilities and accidental data breaches in 3\textsuperscript{rd} and 4\textsuperscript{th} place. This is a similar picture to 2021.

Top cyber security concerns (frequencies and rank based on a weighted score)

<table>
<thead>
<tr>
<th>Rank HE</th>
<th>Threat</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>Weighted score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ransomware/malware</td>
<td>34</td>
<td>14</td>
<td>4</td>
<td>134</td>
</tr>
<tr>
<td>2</td>
<td>Phishing/social engineering</td>
<td>17</td>
<td>19</td>
<td>9</td>
<td>98</td>
</tr>
<tr>
<td>3</td>
<td>Unpatched security vulnerabilities</td>
<td>8</td>
<td>15</td>
<td>23</td>
<td>77</td>
</tr>
<tr>
<td>4</td>
<td>Accidental data breaches</td>
<td>3</td>
<td>6</td>
<td>15</td>
<td>36</td>
</tr>
<tr>
<td>5</td>
<td>Users bringing own devices BYOD</td>
<td>0</td>
<td>4</td>
<td>6</td>
<td>14</td>
</tr>
<tr>
<td>6</td>
<td>Intellectual property theft</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>IoT based attacks</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Internal attacks</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Denial of Service attacks</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Q38. What do you feel are the three most significant cyber security threats to your organisation?
Cyber security insurance

There is a rise in the number of organisations reporting some form of cyber insurance this year.

As in 2020 and 2021, insurance claims for cyber security breaches are not common. 24 (71%) institutions indicate they have not made any insurance claims.

- 55% of HE of HE organisations have some form of cyber security cover (47%, 2021). This has risen each year since 2020.
- As in 2020 and 2021, a high proportion report no insurance against cyber security breaches at 31%. Of the 19 HE organisations who reported no cover, 13 said that they had struggled to find specific policies that provide cover for cyber security breaches.

% HE with cyber security insurance vs. 2021

- Specific cyber policy: 34% (30%)
- Part of broader policy: 21% (17%)
- Not insured, cyber: 31% (27%)
- Don't know: 3% (13%)
- Prefer not to say: 5% (11%)
- Other: 2% (7%)

71% (24 out of 34)  
Have not made a claim in the last two years

18% (6 out of 34)  
Have made a claim in the last two years

Q43. Insurance: which of the following best describes your situation?
Q44. Have you made any insurance claims for cyber security breaches under this insurance?
Q45: Have you struggled to find specific policies that provide cover for cyber security breaches?
Reporting of cyber security incidents

Organisations were most likely to report incidents to Jisc CSIRT, the ICO and Action Fraud. 43% reported no incidents within the last 12 months. Those that had not reported incidents were most likely to indicate that they did not consider the incidents reportable.

Q41. In the last 12 months have you reported cyber security incidents to any of the following external organisations?

Q42. Why have you not reported any incidents?
Microsoft Defender for Endpoint (MDE) and Sophos Intercept were the most popular systems indicated. Only 11 did not report an EDR or XDR in place, however feedback from the community suggests that we may need to conduct further research to understand the true picture of threat protection in the sector.

<table>
<thead>
<tr>
<th>EDR or XDR Solutions</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Defender for Endpoint (MDE)</td>
<td>46%</td>
</tr>
<tr>
<td>Sophos Intercept</td>
<td>23%</td>
</tr>
<tr>
<td>Cortex XDR</td>
<td>7%</td>
</tr>
<tr>
<td>Trend Micro XDR</td>
<td>5%</td>
</tr>
<tr>
<td>FortiEDR</td>
<td>3%</td>
</tr>
<tr>
<td>Falcon (Crowdstrike)</td>
<td>3%</td>
</tr>
<tr>
<td>Don't have but considering</td>
<td>15%</td>
</tr>
<tr>
<td>Don't have and no plans to introduce</td>
<td>3%</td>
</tr>
</tbody>
</table>

Q40. Which EDR or XDR solutions do you use?
Feedback on Jisc services
Feedback on Jisc’s existing services

We received positive comments about the Jisc offer and our staff, with particular mentions for CSIRT, penetration testing, CSP and DDoS mitigation. However, comments highlight issues with the implementation of Managed SIEM.

Very happy with the service, alerts and information. The team and people around are brilliant and I would say I/we feel looked well after!

Happy with the services we have with JISC (JNRS and DDoS protection...)

Overall experience with JISC CSIRT is very positive, keep up the great work.

CSIRT do a great job and we value their work.

Overall quality is good, though SIEM service seems to be struggling with capacity - I appreciate there has been considerable re-organisation.

Suggestions for development:
• Improvement of Managed SIEM, including customer service
• Introduction of Managed SOC

Q46. Do you have any feedback on Jisc’s existing cyber security services?
Products/services interested in Jisc providing

A range of responses were received, with cyber security training emerging as the biggest request, as in 2021. Responses are summarised below.

<table>
<thead>
<tr>
<th>HE</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Training, e.g. infosec (4)</td>
</tr>
<tr>
<td>• Managed SOC (3)</td>
</tr>
<tr>
<td>• Managed SIEM, including improving the current offer (3)</td>
</tr>
<tr>
<td>• Web content filtering (1)</td>
</tr>
<tr>
<td>• Certification assistance (1)</td>
</tr>
<tr>
<td>• Vendor due diligence (1)</td>
</tr>
</tbody>
</table>

Q47. Are there any additional cyber security related products or services you are interested in Jisc providing?
Review process

The results of this research were shared through our CISO forum, our HE IT Leaders Focus 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 will present the findings at the Jisc cyber security conference in November 2022.
Contact

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

John Chapman
Director information security policy & governance
john.chapman@jisc.ac.uk

4 Portwall Lane
Bristol
BS1 6NB