Education & Skills Funding Agency

Academy trust guide to cyber crime and cyber security

Cyber crime may involve malicious attacks on computer software, including:

Email hacking

Email hackers try to gain access to email accounts by tricking people:

- to open and respond to spam emails
- to open emails with a virus
- to open phishing emails

Phishing

Phishing messages look authentic with corporate logos and a similar format to official emails. Unlike official communications, phishing email ask for verification of personal information such as account numbers, passwords or date of birth. Unsuspecting victims who respond may suffer stolen accounts, financial loss and identity theft.

Malvertising

Malvertising can compromise computers by downloading malicious code when people hover on or click on what looks like an advert. Some will even download malicious code to your computer, while the website is still loading in the background. Cybercriminals use advertisements as a way to hack into computers.

Cyber crime: what can trusts do?

To comply with the requirements of the Academies Financial Handbook (paragraph 4.8.1) and address the risk of fraud, theft and/or irregularity, trusts should as a minimum:

- use firewalls, antivirus software and strong passwords
- routinely back up data and restrict devices that are used to access data
- train staff to ensure that they:
  - check the sender of an email is genuine before, for example, sending payment, data or passwords
  - make direct contact with the sender (without using the reply function) where the email requests a payment
  - understand the risks of using public wifi
  - understand the risks of not following payment checks and measures

This is not an exhaustive list.

Published: March 2018

Cyber security – checklist for academy trusts

Cyber security is the protection of computer systems, including hardware, software and data, from unintended or unauthorised access, change or destruction.

Five strategic questions for audit committees

Academy trusts audit committees should use the following high-level questions, based on government guidelines and industry standards, as a starting point to consider cyber risk in the trust. As part of its assessment, the audit committee should consider the quality of the evidence underpinning assurances provided by management.

1. Information held

Does the trust have a clear and common understanding of the range of information assets it holds and those that are critical to the business?

2. Threats

Does the trust have a clear understanding of cyber threats and vulnerabilities?

3. Risk management

Is the trust proactively managing cyber risks as an integrated facet of broader risk management including scrutiny of security policies, technical activity, user education and testing and monitoring regimes against an agreed risk appetite?

4. Aspects of risk

Does the trust have a balanced approach to managing cyber risk that considers people (culture, behaviours and skills), process, technology and governance to ensure a flexible and resilient cyber security response?

5. Governance oversight

Does the trust have sound governance processes in place to ensure that actions to mitigate threats and maximise opportunities in the cyber environment are effective?

Ten cyber security tests for the wider business

Audit committees should ask detailed questions to assess and gain assurance that cyber security good practice is in place. The following questions are based on the National Cyber Security Centre's 10 steps to cyber security. Again, as part of its assessment, the audit committee should consider the quality of the evidence underpinning the assurances provided by management, including whether there is good evidence that the policies and procedures are well designed, consistently implemented and operating effectively in all relevant areas of the trust.

1. Home and mobile working

- is there a clear policy on mobile working, with all associated training?
- is a secure baseline build applied to all devices?

- is data protected outside formal work environments, including in transit?

2. User education and awareness

- does the trust have security policies covering acceptable and secure use of systems?
- is there a staff training programme covering secure use of systems, including awareness of cyber risks – for example strengthening passwords, risk from public wifi hotspots, risks from use of removable media such as USB sticks, avoiding use of personal accounts for business purposes, and maintaining backups?
- do staff know how to report issues and incidents?

3. Incident management

- does the trust have an incident response and disaster recovery capability, with suitably trained staff?
- are there incident management plans and are these tested?
- are criminal incidents reported to law enforcement bodies?

4. Information risk management regime

- is there a governance structure for managing information risk?
- do information professionals liaise with central government, stakeholders and suppliers to understand the threat?
- does senior management understand and engage with risk mitigation processes?

5. Managing user privileges

- are there effective account management processes, with limits on privileged accounts?
- are use privileges controlled and monitored?
- is access to activity and audit logs controlled? Are these logs reviewed for unusual behaviour?

6. Removable media controls

- is there a policy on the use of removable media (eg CDs, flash/pen drives, mobile phones, wireless printers)?
- are media scanned for malicious software (malware) before being linked to the system?

7. Monitoring

- is there a monitoring strategy in place for all ICT systems and networks?
- do logs and other monitoring activities enable the identification of unusual activity that could indicate an attack?

8. Secure configuration

- does a system inventory exist?
- are security patches applied regularly?
- is there a minimum defined baseline for all devices?

9. Malware protection

- are there effective anti-malware defences in place across all business areas?
- is there regular scanning for malware?
- what changes have been made as a result of monitoring results?

10. Network security

- is the network perimeter managed?
- do information professionals understand where the highest risk information assets are and how they are protected?
- are security controls monitored and tested?

Other resources

The National Audit Office report The UK cyber security strategy: landscape review describes government's evolving approach to cyber security.