16 questions you need to ask to assess your cyber security posture

1. Do we have a data classification scheme to help identify sensitive information and ensure appropriate protections are in place?

2. Do we have effective mechanisms for controlling access to resources, such as how we handle new starters, movers or when staff leave our organisation?

3. Do we review user accounts and systems for unnecessary privileges on a regular basis?

4. Do we enforce multifactor authentication for all systems and users?

5. Do we have a tried and tested process for backing-up critical data in a manner resistant to disasters or cyber attacks?

6. How long will it take us to recover critical business functions, assuming a loss of all infrastructure? What's the business impact of a loss of all digital infrastructure? How will we lead and co-ordinate business recovery in this scenario?

7. Can the business tolerate a recovery period that could take several weeks or months? How is this effected by different critical time periods for our business?

8. Do we have regularly rehearsed plans to deal with the most likely cyber events or disasters?

9. Are all of our hardware and software products free from vulnerabilities, supported by the vendor and regularly patched?

10. Are our networks separated so that if an attacker gets access to one device, they will not have access to our entire estate?

11. How would our organisation identify an attacker's presence on the network?

12. Do we regularly review our cyber risk management approach to ensure that the ways we have decided to manage risks remain effective and appropriate?

13. Are all staff aware of and participate in effective cyber risk management processes?

14. Are we doing everything necessary to support our staff, students and stakeholders to understand and be aware of cyber risk, via training advice and guidance?

15. Do we maintain an accurate record of our technology assets, including hardware, software, firmware, peripheral devices and removable media?

16. Do we adequately understand our business-critical services and functions and their associated data, technology and supply chain dependencies?

Jisc can help you strengthen your position – get in touch to find out how we can support your institution
securityservices@jisc.ac.uk