10

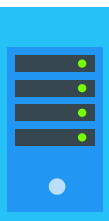
Legal Services National Technology Assistance Project

Top 10 For IT Leaders

Do you have knowledge and control of who has access to any firm system data?

- Working with HR on staff and users
- Working with Managers on access need
- Locking down devices, systems and services to the extent feasible
- Controlling the use of BYOD and unmanaged device access
- Turning up logging and monitoring/retaining logs

1



Is every piece of hardware and software supported by the manufacturer and up-to-date with the latest security patches/updates/firmware and protected with security software?

Do you have managed antivirus, endpoint detection and response software deployed?

2

Are your backup systems comprehensive, compliant, current and available for various recovery scenarios?

For certain cyber incidents and failures you may need file-level recovery while in other instances you may need system image recovery.

3

For technology continuity purposes, have you identified with management all critical systems and services needed for client services and business operation, can you recover those services within the required timelines, have you tested the recovery within the last 12 months?

4

Is your documentation comprehensive, up-to-date, and shared/reviewed by another person/consultant?

Documentation is critical to planning and managing security as well as responding to a cyber security incident.

5

Do you periodically conduct third party security assessments and penetration testing?

6

Have you benchmarked your organization's cybersecurity against CIS Controls v8 or other appropriate security framework?

https://www.cisecurity.org/controls/v8/

7

Do you meet regularly with leadership & staff to learn about client services, current technology pain points/needs, as well as report out on the work you are doing?

Ensuring adequate security planning and reducing the use of unmanaged technology. Understanding the user experiences and minimizing the negative impacts of security technology and practices can improve compliance and morale.

8

Do you have a regular cybersecurity training and testing program for staff and volunteers? Trainings on how to securely share documents and use of firm data encryption?

End users continue to be the starting point for most cyber security breaches. Investing in regular training and testing helps to reduce the risks of user compromise.

9

Have you implemented MFA authentication across systems with confidential or proprietary information?

MFA can significantly reduce the risk of successful user account compromise. Deploying MFA across all systems is important to protecting client and user data. Deploying a unified MFA system across multiple systems is preferred for ease of use, management, and overall security.

10