10

Legal Services National
Technology Assistance Project

Top 10 For Executive Directors

1 What are the technology systems, services, devices, & data that are being used by staff & volunteers in the organization? For what purpose? How are they being kept up-to-date & secure?

Leadership must have an up-to-date inventory and understanding of their technology environment. This leads to better questions, management, and risk reduction.

2 How do we control, monitor, and manage employee and volunteer access to each system, service, or device used by the firm?

Leaders should understand how the firm limits access to systems and data as well as what data users have access to and where the data may be stored intentionally or unintentionally.

3 What are we doing to protect the firm from password/identity compromises?

User and administrative accounts are typically protected by passwords that may be compromised through phishing and other attacks. Many firms now use multi-factor authentication, unified identity management, single sign-on and similar technologies.

4 Are there any accounts, services, or data that relate to the firm's employees, clients, or work product that are not controlled by our firm?

Understanding the tech being used will allow program leaders to decide whether and how the firm needs to gain control of technology or data as well as how it might continue the use of such technology where it better serves staff or clients.

5 Are there any technology gaps that advocates and other professionals in the firm need addressed?

Supporting your dedicated advocates and professional staff with the technology tools they need to do their job has two benefits. One, it empowers staff to work more effectively. Two, it reduces the likelihood that staff work outside of or around the firm's technology.

6 What, if any, devices not owned by the firm are used in connection with the firm's business or client services?

Firms need to understand and manage the use of equipment that the firm doesn't own. Firms may decide to provide more equipment to their users, install software on the equipment that makes the data more secure, or limit the use of personally owned devices to certain groups or to certain services.

7 How are we prepared to identify, mitigate, and manage a cybersecurity incident?

Do we have adequate cyber liability insurance in place? How are we monitoring access and movement of data? How would the firm identify/be alerted to a security incident? Who gets alerted? When? What about attempts? Have there been any security incidents?

8 What is our business continuity plan, when was it last revised, when did we last test it?

https://www.ready.gov/business-continuity-plan

9 How are we training staff to proficiently and securely access/use firm systems and data inside and outside of the office?

Being trained to use technology properly helps improve productivity while reducing the risk of misuse that can lead to unsafe practices or even the use of unauthorized technology.

10 Do we have adequate security policies or guidelines in place, disseminated and enforced to manage and mitigate major cybersecurity risks?