1. Security Toolkit: An Overview of Topics in Cyber Security

How To Use This Toolkit

This toolkit serves as a jumping off point for legal aid programs to start being more intentional about their security practices. It includes information from LSNTAP's 2021 Seasons of Security webinar series as well as additional information about security compiled from experts on the subject. It is not intended to be the complete and final answer to your organization’s security practices. It is a resource to get the conversation going and to move towards a more secure environment. But it does include some immediate and concrete suggestions for every organization, no matter where they are in the process of thinking through cybersecurity issues.

Overview

At its most basic, cyber security in legal aid is about making reasonable efforts to protect confidential data, ensure business continuity, and ensure business recovery after a cyber incident all while enabling an organization to serve its clients and mission. Cyber security needs will vary somewhat by organization based on the data they collect, who they work with, how they interact with data and the services they provide clients. But there are some issues and subjects that are pertinent across most legal aid organizations.

This section is a great place to start; it provides an overview of many of the topics we will cover, with links to other parts of the kit for more information. As the content covered by the toolkit expands, the information here will be updated to reference new material on this site.

Staying Up to Date of Cyber Security Technology and Practices

Legal Aid providers need to actively keep up with current and emerging security technologies and practices that may need to be implemented within their programs. A few current security technologies and practices for providers to consider or implement include:

a. Next generations firewalls (NGFW) provide additional services beyond basic inspection and management of web traffic that firewalls have provided for 30 years. NGFWs have functionality such as Intrusion Detection Systems and Intrusion Prevention Systems (IDP/IPS), anti-virus scanning, limiting access by geography (Geo IP Filtering/Blocking), and Virtual Private Network (VPN) functionality. For more on these technologies see Next Generation Firewall, Intrusion Detection System, Virtual Private Network, and Geo-Blocking.
b. Multi-factor authentication [1](MFA) provides controlled access to organizational networks, systems, and data. MFA better protects sensitive or confidential data from simple password compromise schemes and phishing attacks.
c. Endpoint Detection and Response (EDP) software monitors endpoints (laptops/desktops/servers) with automated response to a wider variety of security threats than traditional anti-virus software.
d. Offline server image and file backup solutions make it harder for malicious software and actors to encrypt or destroy backup copies of your data while also enabling faster and more tailored recovery that may be needed after a cyber security incident or system failure.
e. Segmentation of the office network environment into multiple logical networks can make it harder for malicious software or actors to move across your network environment or even across an individual application once they have gained initial access to your network or application.

[1]*Enterprise-wide MFA typically also makes use of single sign on technology to reduce the number of times users have to sign in when accessing multiple systems within an organization or across their cloud services.*

Access Control and Account Management Practices

By improving the management, configuration, and access to existing technology, legal aid providers can significantly increase security and also mitigate the risks associated with a cyber breach. This work may include:

a. Locking down software, hardware, and cloud service configuration to restrict access, eliminate default account access, or eliminate services and functions that are not immediately needed or actively managed and monitored.
b. Active user management by limiting place, time, and duration of access (e.g., disabling summer intern accounts promptly after summer ends); limiting permissions within and across applications; and monitoring for abnormal access and use of systems.
c. Configuring systems to log access and use by staff and volunteers.
d. Maintaining current infrastructure by keeping current, actively supported versions of hardware and software in place along with patching and updating software as recommended by product vendors.

Managing Office and Home Technology

Cyber security typically includes managing office technology and home office technology. Providers work to protect the physical security of technology to reduce loss or theft of hardware and data. They work to keep known, insecure hardware and software out of the work environments. They try to keep unauthorized devices (e.g., unknown laptops, hard drives, phones, USB storage keys) from adding significant cyber security risks out of their environment. Especially in the age of Covid-19, organizations are starting to actively manage personally owned devices (POD) that are used for work purposes by establishing appropriate access restrictions for untrusted devices, minimum software requirements and creating mechanisms for monitoring or interrogating access and use of organizational systems. In managing equipment, organizations should have preventive measures in place to protect against lost or stolen equipment. Such measures may include the use of full-disk encryption that helps ensure data on devices are inaccessible to unauthorized persons, mobile device management that helps keep the devices configured in secure manner and, in some instances, can erase lost or stolen devices.

Building a Security Culture

Perhaps one of the most crucial elements of strong cyber security is building and maintaining a cyber security culture among your staff and volunteers. End users

can be a great asset to maintaining the security of your systems and data, but that does not happen without sustained effort. In fact, most cyber incidents rely on user actions to stop the advance of attacks. Security culture work typically includes:

i. Technology training and security training
ii. Testing or auditing user skills and responses to cyber attacks
iii. Supervision and monitoring of technology use by staff and volunteers
iv. Developing, implementing, updating, and enforcing security-related tech policies

Understanding the Organization's Collection, Use, and Storage of Sensitive or Confidential Data

Legal aid organizations generally have significant and diverse needs to collect, use, and retain data. That data needs to be kept secure. Legal Aid providers need to inventory, document, analyze, and control the sensitive and confidential data it works with organization wide. This work typically includes:

1. Tracking data collected across the organization and across the range of technology systems (e.g., CMS, HR, Fundraising, Self-help tools, email, Website)
2. Documenting who has access to the data and how the data moves or is shared inside and outside the organization
3. Understanding how the data is securely stored, backed-up, and securely destroyed across all its systems
4. Examining why the data is necessary for the work as well as why and when it needs to be shared
5. Ensuring that policies and practices are developed and consistently followed to govern the life cycle of confidential and sensitive data
6. Learning how technology might assist the organization in working more securely with data and helping to ensure compliance.

Managing Security for IT Staff, Contractors and Vendors

Technology professionals pose additional risks for organizations as they typically have access to a broad array of systems and data and typically have permissions to

make potentially disastrous changes to your technology environment. To help address these risks providers may work to:

1. Ensure staff and contractors are properly trained and competent to do the technology work required
2. Limit permissions and privileges to the extent practical
3. Implement logging, audit tools, and develop a reporting mechanism on the work being done
4. Invest in ongoing security training for tech staff
5. Work to eliminate single points of failure due to loss of IT personnel

Comprehensive Documentation of the Technology Environment

Maintaining up to date documentation helps ensure that an organization can properly implement new technology, reduce the risks of technology that may not be properly managed or integrated, and more competently and quickly recover from a cyber security incident.

Addressing Management’s Role on Cyber Security

Management has a critical, ongoing role in maintaining a more secure environment. Management’s technology oversight role is broad but certainly includes assessing and auditing, supervising tech staff, technology planning, developing, and implementing policies, technology budgeting, inventory management of hardware, and software and services.

Third Party Audits and Testing

Security Audits and Penetration Testing of technologies that serve the organization and client communities are growing in importance. Major factors affecting the need for third party audits are increasing complexity (e.g.t echnology environments on-site and in the cloud, rapid changes to technology environments, development of new security attacks, and the need to prioritize security improvements and risk mitigation strategies). Third party audits help identify new and emerging security risks and solutions to better manage the risks. They are done regularly since the

organization’s technology environment and its use are not static. Auditors work with providers to develop action plans to address identified deficiencies

Insurance

Procurement and maintenance of cyber liability insurance is a critical part of cyber security. Insurance helps cover the substantial costs of managing and responding to a cyber security incident. It is a key part of an organization’s risk management strategy. Insurers are increasingly driving critical security improvements within organizations to reduce insurance claims.

Cyber Incident Preparation and Response

Preparing to detect, log and respond to cyber security incidents of varying types and severity helps minimize the disruption and risks associated with such incidents.

1. Technologies and services that actively monitor for and/or interrupt current and emerging cyber security compromises
    i. Security Information and Event Management (SIEM) services that use software, security personnel, and/or artificial intelligence to detect and respond to events on your network, systems, and application that may relate to a cyber attack
    ii. Endpoint detection and response software (EDR) may be part of a SIEM solution or stand on its own to help identify an attack, stop the attack, report the behavior, and / or recover from the attack
    iii. Extensive and durable logging, typically to a cloud-based repository, of access attempts, access granted, application access, as well as the movement of users and data across the technology environment
    iv. Security policies and training that cover identification and reporting of incidents that might indicate or lead to a cyber security incident (e.g., loss of equipment, clicking on unknown or dangerous links)

2. Developing an incident response policy and related protocols that includes incident handling, data capture/reporting, activation of response, communications, alternative solutions/services/resources, and cyber liability insurance.

3. Cyber incident response and recovery work
    a. Following incident response policy
    b. Interrupting the incident and stemming the damage
    c. Communicating internally and externally
    d. Getting help
    e. Forensic analysis
        1. Establishing the path for the compromise
        2. Establishing extent of access/compromise
        3. Establishing the likelihood of data exfiltration
        4. Establishing the path to securing the environment
    f. Managing the cyber incident
        1. Working with board, management, and staff
        2. Working with counsel on understanding the nature of the incident, internal/external communications, interaction with cyber criminals, and disclosure/compliance requirements
        3. Working with ransom negotiators
        4. Working with IT staff/contractors on interim and longer-term recovery
        5. Managing client services and staff needs/morale

Last updated on December 15, 2023.

Print

Table of Contents

NEWS

News & publications

The news about recent activities for needed peoples.

More News

10 Oct 2024

LSNTAP Announces Access to Comprehensive Technology Initiative Grants Database

Ypsilanti, MI – October 10, 2024 – Legal Services National Technology…

[Continue Reading]

18 Jul 2024

LSNTAP Launches a New Resource for the Community: the RFP Library

Over the last two years, LSNTAP staff has pored over the listserv archive to…

[Continue Reading]

Our Partners

MAP | MICHIGAN ADVOCACY PROGRAM

LSC | America's Partner for Equal Justice

LEGAL SERVICES CORPORATION