2. Security Toolkit: Introduction

Purpose

The Problem

According to a study at the University of Maryland, cyberattacks are incredibly common and nearly constant: every 39 seconds, a computer connected to the internet is attacked. Legal aid programs are unfortunately no exception. Legal aid programs collect and store all sorts of client data through the process of representing people. These programs are just as susceptible to attacks on their security and their data as any other entities. In fact, some of our friends in the legal aid community have already experienced cyberattacks.

A breach can have a very high cost. The average cost of a data breach is $4.25 million (Cost of a Data Breach Report 2021). The average total cost of a data breach increased by nearly 10% from 2020 to 2021, and there's reason to believe this upward trend will continue. Because larger firms have largely started to address cybersecurity, attackers may now be targeting smaller organizations more often.

With attacks happening constantly, and with the high cost of a breach, the legal aid community must make conscious efforts to enhance security. We must all be prepared to take proactive steps to make sure our and our clients' data is safe.

Why This Toolkit

We need to enhance security in the legal aid community. We have a duty to our clients not only to serve them, but also to protect their data. We need to take security seriously at every level, from offices just starting to protect themselves all the way to offices looking for the next innovation to add to their arsenals. We need a toolkit to help us all meet this obligation.

Who is this Toolkit for?

This toolkit has something for everyone in a legal aid office:

- Executive Directors and management can use this toolkit to better understand why security is important for their organization and the steps needed to provide a more secure environment.
- IT staff can learn specific steps they can take to build a more secure environment and can find resources to share with others at their organization to help train staff and increase buy-in for enhanced security protection measures.
- Attorneys and advocates can learn more about security and why it is important, including some things they can do to enhance security as an individual.

Background

Why Should Legal Aid Care About Cyber Security?

Cyberattacks are nearly constant and do not discriminate, any computer connected to the internet is vulnerable. But beyond the background threat, legal aid offices have even more reason to be concerned about cybersecurity. Legal aid providers need to keep client, employee, donor, volunteer, and other sensitive data confidential. Our clients, staff and volunteers deserve to have their identities and data protected by the legal aid providers they entrust.

Not only do attacks risk confidential data, cyber security incidents also typically disrupt law firm operations for days, or even months. In a 2020 breach, one Legal Aid experienced disruptions to computer services which prevented staff from directly accessing any files on the office servers for nearly three months. IT staff had to manually share files with people working remotely while they dealt with recovery from the breach. This kind of disruption cannot only impact staff productivity and morale, but it can also have a negative impact on services to clients, and even impact case outcomes.

Additionally, outside stakeholders are increasingly sensitive to cyber security of the organizations they interreact with, or even fund. State laws, regulations, and industry standards (including annual fiscal audits) are increasingly mandating that organization's take action on cyber security.

The threat environment has gotten worse for small and mid-sized firms, and non-profits are not at all spared. Cyber security risks and mitigation strategies are regularly changing, so legal aid providers need to keep focus on security just to keep up with expectations.

What are Some of the Risks?

Many bad actors in the U.S. and abroad are working globally to look for ways to compromise your technology or your users. They do this for many different reasons. The most obvious reason is for financial gain (e.g., asking a ransom from offices to restore services, selling the data they access to other bad actors, using your data for further compromise, using your systems to attack other systems/organizations). Other attackers aim to harm or embarrass your organization for specific reasons (e.g., political, social, individual vendetta).

Impact on Client Services and our Client's Lives

Cyber incidents can result in client data being stolen, which can have a severe negative impact on client's lives as a result. Data theft could lead, for instance, to identity theft or destruction of credit. But attacks don't only expose confidential data, they also may interrupt any services that rely on computers or internet connection to work. This can include disrupting intake (even things like phone systems, case management systems, or web-based intake forms). It can also impact your organization's website and resources clients use for online learning and self-help.

Attacks can also interfere with ongoing client representation. Advocates might lose access to the data and systems they need to do their job representing people. They could also lose the ability to communicate with clients and with each other.

Finally, attacks can cause funders and stakeholders to distrust an office's security practices, which can lead to a loss of funding. And funding decreases also directly impact the communities we serve by decreasing the services we can offer.

Philosophy, Approach, and Culture

The best way to start when thinking about cybersecurity is to remind ourselves that security is an ongoing process and a culture shift. It is impossible to be in a state of "cyber security" (or being "cyber secure"). Rather, we must prioritize ongoing learning and adjusting practices accordingly. This includes learning about current and emerging threats, learning about best practices and technologies to manage the risks, and learning about best practices and technologies to mitigate the harm and interruption of cyber incidents.

This also means that cyber security is a collective responsibility, shared by our whole community and across an entire organization. It can not simply be assigned to a staff member or contractor. Management at all levels are responsible for cybersecurity, both in practice and in creating a culture that takes the issue seriously.

Also, as with anything that is important for legal aid services and clients, an ongoing commitment to cyber security has a cost. Cyber security frequently requires organizations to make compromises between usability or functionality of their technology and the risk that the technology or data might be compromised. Safer practices might feel like more work or might feel like you are not using the technology to its full potential, but this trade-off might be required to secure the technologies that support access to and delivery of legal services. The tradeoff could also be financial: offices might have to pay for additional staff, contractors, software, or services to enhance their security.

In the end, balancing service needs against security requires that organizations stay informed and educated about their technology, the risks inherent in how they use it, and the tools and services that help reduce the associated risks.

Legal aid has been managing complex risks for years (financial mismanagement, compliance, malpractice, and even case decisions), and cyber security is another major risk for legal aid to manage that will likely be with our community for years to come.

Benefits of Proper Security Planning and Management for Advocacy and Advocates (Lemonade)

Benefits for IT Staff

The most obvious benefit to IT staff taking cyber security seriously is a decreased risk of successful security breaches. This reduces business interruptions. Any cyber incidents that do compromise the organization will likely be both identified and shut down more quickly. This early detection and preparedness can also reduce interruption time when incidents do occur.

A strong cybersecurity preparedness plan can also help with recovery. Organizations with the right technology and processes in place will increase the likelihood that IT staff can identify the cause or source of the compromise. This also increases the chances that the organizations will know the extent of access and the extent of any data that has been stolen. Finally, being prepared before an attack can also help staff debrief from any breaches to identify simpler solutions for securing routes of attack against future breaches.

Benefits for Management and Operations

Enhanced cybersecurity also directly benefits management and operations staff. First, better cybersecurity preparedness can improve relationships with funders and stakeholders. Audits and reports for funders and boards often include questions about security. Being prepared can make these reports easier to prepare. It can also increase your organization’s reputation as a responsible non-profit, both to stakeholders and to the larger legal aid community. Plus, better handling of incidents as they arise will mean less likelihood that an office needs to report or disclose a breach.

Being mindful of cybersecurity is also more economical. Preparing ahead of time typically costs a lot less and can be spread out over a longer period than emergency responses. Planned security work can be done in concert with other projects or timed for better pricing. When your organization considers cybersecurity (which you should), this can be more attainable and more

affordable if you are already taking these issues seriously.

Benefits for Staff, Attorneys, and Advocates

Staff, Attorneys, and Advocates will also feel the positive effects of better cybersecurity. They can feel safe that their own data, and the data of their clients, will not be accessed by bad actors and used for nefarious purposes. When things do go wrong in an organization that has taken steps to prepare for a breach, staff will not feel as disrupted. They will be able to get back to work faster after an incident.
