Webinar: Managing Security Risks

Mary O’Shaughnessy MOShaughnessy@herjustice.org John Greiner jgreiner@just-tech.com

Risks & Challenges

500 million records were just breached at the Marriott hotel chain. It’s risky having employees on public networks, on company laptops. If you work in legal aid because you have a lot of client data and information you will be a target, and at risk.

As time goes by you will be expected to know more, computer security isn’t just for a dedicated IT people anymore, everyone needs to be involved.

Major Legal Aid Data Risks

- Case Management Systems
- File Servers, SharePoint, Google Drive, DMS
- Accounting & HR Systems
- Donor Management Systems

- Web Presence, Apps and Social Media

Top 10 Operational Risks & Challenges

- Small firms with limited budgets and tech capacity
- Limited training and user participation
- Increasingly mobile work environment
- Use of personally owned devices and private accounts
- Client-owned devices (risks for clients and programs)
- Significant turnover among interns and volunteers
- Data and work collaborations with partners and funders
- Collection of voluminous private and sensitive data
- Demands to improve legal service delivery and innovate
- Managing cloud services for clients and staff

Potential Impacts of Breaches and Interruptions

- Client/staff safety, privacy & expense
- Rapidly evolving state & federal law
    - HIPAA
    - California Consumer Privacy Act of 2018
    - New York General Business Law § 899-aa
    - Supreme Court of Pennsylvania Nov 21, 2018 decision in Dittman v. UPMC
- Ability to Serve Clients
- Time & Cost of Recovery
- Loss of Grants/Funding/Reputation
- Malpractice?

Policies and Practices Either Aggravate or Mitigate Risks

We all have a comprehensive set of technology policies. It is just that, for most of us, those policies are implicit and completely permissive.

Policies & Practices

Some IT Risk Aggravators

Risk Mitigation

- Starvation IT Budgets
    - Out-of-date/unsupported systems
    - Inefficient use of team resources
    - Reduces IT and advocate morale
    - Reactive not strategic
- Isolated or Deprioritized IT
    - Don’t get management’s time & attention
    - Limited budget planning
    - IT training and capacity
    - Compartmentalization not collaboration
- Inadequate Technology Leadership
    - Systems that don’t meet needs
    - Proliferation of software & systems
    - Unapproved or personal technology
    - Reduced staff buy-in

Priority Policies

    - Pervasive Security Culture
    - Collaboration with Leadership, Advocates and Professional Staff
    - Explicit, up-to-date policies
    - Training & Compliance
    - Collaborative Tech Planning
        - Identifies and addresses current & emerging needs
        - Factors in use cases & user experience
        - Adjusts and Responds
    - Adequate Longer-Term Budgeting
        - Reduce risk and costs of old tech
        - Turns policies into practices
        - Provides staffing or consulting resources to reduce the back burner projects
    - **Personnel**

      Make sure you have a system in place / policies in place when a new team member comes on board. Are they having access to private info on their company laptops? If so are the company laptops able to be remotely wiped? Have you discussed using random wi-fi connections? Is there a

system setup for encrypting key files when in transit?

- Onboarding & Offboarding
- Security Awareness Training
- BYOD / BYOA Use
- Internet, Social Media & Email Use
- Authentication Policies
- User Accounts
    - Internal Staff
    - Privileged Staff
    - Vendor/Third Party
    - Service Accounts
- Encryption Use Guidance
- Incident Reporting/Response

Data

Have an idea ow how you will deal with data. How is client and staff privacy protected within your organization, do you have procedures that people actually follow? For example if client information is no longer needed it should be destroyed. Is that going to happen automatically or is your organization hoarding private data?

- Client & Staff Privacy
- Collection
- Retention & Destruction
- Classification
- Sanitization/Redaction
- Leakage Prevention
- Access/Handling
- E-Discovery

Priority Policies & Practices

Physical Security

Are all your screens locked? If somebody steps away from their computer or device for five minutes does it then lock automatically or would

somebody be able to access client data? You need to have a plan in place for storing software licenses, securing access to the server room and ensuring passwords are hidden from view. Also your organization should have some awareness of what visitors are there, and control access to your building / office.

- Hardware Asset Management
- Software License and Media Management
- Screen Locking
- Equipment Theft/Loss
    - Mobile and Office Equipment*
    - Network/Server Closet Access Restrictions
    - Environmental Controls
    - Physical Safety Measures (fire, flood, etc.)
- Visitor Awareness
- Document & Password Visibility

Access & Encryption

- Centralized User Authentication & Control (including cloud services)
- Software Asset Management
- Mobile Device Management
- System and Use Monitoring
- Remote Access
- Account Lockout
- Encryption
    - Data
    - Email
    - Wireless
    - Instant Messenger

Turning Policies into Good Practice

To turn policies in practice you need to have a meeting about the changes, and put somebody in charge of ensuring the policies are carried out. Designate a specific person to deal with security policies and make security an ongoing conversation within your organization.

- Starting off right by tailoring policies to your organization with representative staff input
- Policies do not self-effectuate
    - $$$ to implement, maintain, train, and audit
- Designated person(s)
- Systems or system modifications
- Need to be revisited and revised regularly

Pro Bono Project Partners

- **Kirkland & Ellis (Brian Stempel, Michelle Six & Jacqueline Haberfeld)**
- **Arnold & Porter**
- **IOLA (New York)**
- **Just-Tech**
- **Orrick**
- **Pro Bono Net**
- **Proskauer**
- **Stroock & Stroock & Lavan**

About the Project

- **NYC Bar Legal Aid Committee Need**
- **Started in January 2017**
- **Building on Other NYS Pro Bono Legal Tech**
- **Initially Develop Model Policies, Procedures, & Practices**
- **Issues With Early Approach**
- **Focused On Legal Requirements & Policy Guidance**
- **Follow-up Pro Bono Implementation Assistance**

Become a Cyber Security Ninja Click Here to see LSNTAP's webinar series on how to protect your organization's data and computer systems.

Some Helpful Additional Resources

- **SANS**
- **Krebs on Security**
- **Threat Post**
- **Graham Cluley**

- **Security Ledger**
- **Sophos**
- **Privacy Rights**
- **IT Toolbox**
- **CIS**
- **US-CERT**

Last updated on August 08, 2019.

Print

Table of Contents

NEWS

News & publications

The news about recent activities for needed peoples.

More News

24 Mar 2023

Project Spotlight: UpToCode

Because everyone has a right to a safe home, Northeast Legal Aid (NLA) is…

Continue Reading

28 Feb 2023

Member Spotlight: Josh Lazar

We are heading south to Florida today to meet community member Josh Lazar, the…

Continue Reading

Our Partners

MAP | MICHIGAN ADVOCACY PROGRAM

LSC | America's Partner for Equal Justice

LEGAL SERVICES CORPORATION