Legal Services National Technology Assistance Project

Helping nonprofit legal aid programs improve client services through innovative use of technology.

www.lsntap.org

Webinar: Improving Security

This webinar will help you look more critically at your data security risks and take steps to reduce them. We'll review common risky habits, what to do if a breach occurs, and how to establish policies that help prevent the loss or theft of your data. We will close the session with a walk-through of the new Legal Aid Technology Toolkit on Information Security plus three other tech toolkits for legal aid organizations.

Eric Leland

Founder, Five Paths
IDEALWARE EXPERT TRAINER

Eliot Sasaki

Legal Services Corporation
COLOR COMMENTATOR

Angela Tripp

Director Michigan Legal Help Program

Legal Aid Toolkit: Information Security Free Download

Idealware helps you stay informed about tech trends, assess your needs, select tools that are a great fit, get the most out of technology you already have, and plan for a future that is tech-powered and data-informed. We do that through publications, articles, and other resources which are free to all on our website. We also offer workshops, webinars, and courses. All of our work is based on rigorous, impartial research. Through a merger in 2018 Idealware become a program of Tech Impact, a nonprofit organization that provides technology support and consulting services which are a great complement to Idealware's resources, and hosts the annual Tech Forward Conference. Tech Impact also operates award winning workforce development programs in the technology field.

It's not a question of IF you will be hacked, but WHEN, according to IT consultant Donny Carder who was a contributing subject matter expert on this curriculum. New technologies = new vulnerabilities and new avenues for attacks. That doesn't mean don't use technology. But understand the risks and be smart about it. Security breaches cost time and money. From 3/29/18 Atlanta's government computer files have been held hostage. For a week now.

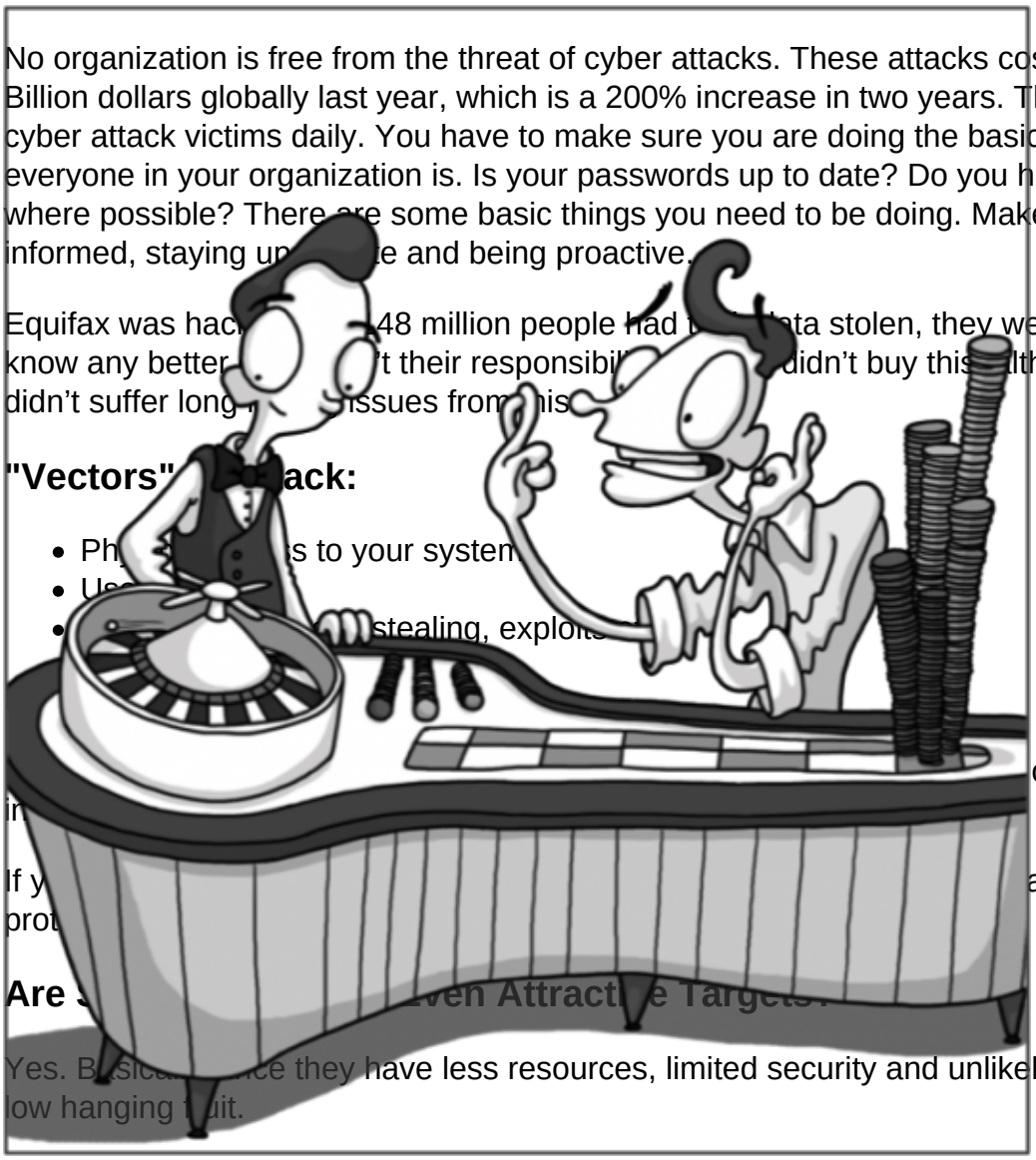
One week ago today, Atlanta's government computer system was hit by a malware attack that encrypted a big chunk of the city's files. To unlock everything, the hackers demanded a $51,000 ransom in bitcoin, which could be due around now. The city's government has been in chaos ever since. It might be one of the biggest cyberattacks against a major US city, ever. Who did this? Unclear. Experts are pointing fingers at an anonymous group of hackers called SamSam that apparently pulls this stuff pretty regularly.

So this has happened before?

Yup, in places like Texas and Colorado. Last year, hackers got into Dallas's tornado warning system. And freaked everyone out in the middle of the night by blasting a fake - and loud -

tornado warning. Earlier this year, Denver's transportation department was also hacked. The dept managed to decrypt its files without paying up. But then got hacked again - and didn't pay up again.

A False Sense of Security



No organization is free from the threat of cyber attacks. These attacks cost organizations 450 Billion dollars globally last year, which is a 200% increase in two years. There is about a million cyber attack victims daily. You have to make sure you are doing the basics right, and that everyone in your organization is. Is your passwords up to date? Do you have captcha set up where possible? There are some basic things you need to be doing. Make sure you are keeping informed, staying up[illegible]e and being proactive.

Equifax was hac[illegible]48 million people had [illegible]ata stolen, they were arguing they didn't know any better[illegible]'t their responsibil[illegible]didn't buy this although the company didn't suffer long [illegible]issues from this

"Vectors" [illegible]ack:

- Ph[illegible]s to your system
- Us[illegible]
- [illegible]stealing, exploit[illegible]

[illegible]can steal valuable in[illegible]

If y[illegible]ata that needs to be prot[illegible]

Are [illegible]Even Attractive Targets?

Yes. B[illegible]ce they have less resources, limited security and unlikely to notice an attack as low hanging fruit.

In terms of cyber attacks, recently in 2017 the global law firm LA Piper was hit with a ransomware attack - one of the most devastating attacks in history, it crippled the firm and put over 3,500 attorneys and support staff out of commision for weeks. It cost the firm millions of dollars in downtime, wasted wages and bad publicity.

Even more recently just in October ransomware took down three different law firms in Florida.

Possessing sensitive data makes non profits targets, but what really does them in is their weak IT infrastructure and inattention to security protocols.

What Are Your Risks? (And what should you do about them

It’s a process. To understand the risks and your comfort with them, you need to carry out a thorough assessment of your data.

You can simply (with stickinotes) make an inventory of your data on a wall. Sort them where data is stored (E.G Case management system.)

Classify your Information

Confidentiality: Data that can’t be exposed.
Integrity: Data you can’t lose.
Availability: Data you can’t lose access to for any period of time.

Consider the Risks

Think through:

What could happen to your data?
How likely is it to happen?
How bad would it be if something happened?

Seven Risky Practices to Avoid

Unmanaged Personal Devices - do your staff use personal devices for work? If so you need to get them so stop doing this right away because there is no way to implement sweeping security precautions if people are using personal phones or laptops for work. A personal device may have additional users. Terminated employees are likely to still have organizational information after leaving. How do you know personal computers and devices have basic protections? In terms of software your nonprofit might purchase the software, but not control the license. Lack of Password Management. If you aren't making people use a password manager or at the minimum a strong password generator then you are putting your organization at risk. The more "simple" a password is the easier it is to "brute force" into the account and steal your data. Sharing passwords between accounts and users is also a risk.

Consumer-Grade Cloud Storage - make sure the cloud system you are using is secure and has automatic backups in case of a server crash. Services like Dropbox can take a lot of the headache out of storing a large amount of data.

Poor Backup Infrastructure - What would you do if your organization faced a disaster?If you have to store it physically, take your backup off site. The Cloud is a great option for backup. Cloud data can't simply be destroyed in a flood or lost in a move. Regularly schedule backups. Create incident response, business continuity, and disaster recovery plans— and test them!

Poor Software Management - Is the software your team is using safe? Hackers keep up to date on security holes and are always looking for opportunities to exploit them. Establish patch management procedures. Manage software installations. Perform regular tune-ups.

Overlooking Physical Security - Is your actual office protected? What if Someone Walks in the Door? Would it be easy to access or steal computers? Take basic office security measures. Lock computers to desks. Institute a check out policy for shared devices and keep them locked away.

Unsafe Wi-Fi - Is your connection secure? You can't just plug in a router and assume everything is fine. Make sure your network is protected by a firewall and a password. Avoid working in insecure environments.

Establishing Policies

Form a Committee A diverse committee can help you see risk from multiple angles and come up with smart ways to deal with those risks.

Ask Tough Questions Anything you overlook has the potential to be a hazard in the future.

What Will Prevent a Breach? Think of all the ways a breach might occur. Write rules that govern activities such as how to create and handle passwords or how files can be stored and shared.

How Will You Respond if a Breach Occurs? Map out a response plan that includes steps and roles for data recovery, business continuity, and communications.

BYOD? Write clear usage guidelines for things such as what security software needs to be installed and whether your organization provides IT support.

From the Toolkit You'll find a worksheet on page 24 to help you develop a Personal Device Policy. There's also a worksheet for an Acceptable Use Policy (page 17).

Policy Making Is Iterative You'll need to review your rules and update them periodically to make sure they're addressing your needs.

Policy Examples Go to http://bit.ly/SecurityPolicy Examples to find examples and templates that you can use as your starting point.

Perfect Security Isn't Possible There will always be risks out there. But by breaking bad habits and establishing good ones, you can protect your nonprofit.

Additional Resources

- Legal Aid Technology Toolkit: Information Security (MAP and Idealware)
- What Nonprofits Need to Know About Security: A Practical Guide to Managing Risk (Idealware)
- Security Guide & Checklist (Tech Impact)
- 2 Minute Training to Protect Against Phishing Attacks (RoundTable)
- Cyber Security One-Year Roadmap Template (RoundTable)
- Nonprofit Guidelines for Cybersecurity and Privacy (Tech Impact / Microsoft)
- SANS Institute Policy Resources

Printed:December 18, 2018
http://www.lsntap.org/node/178/webinar-improving-security