ALABAMA LEADERS in EDUCATIONAL TECHNOLOGY

CyberSecurity Internal Controls

Susan Poling

Accounting in the 21st Century

Welcome to a whole new world of threats.

Not All Threats Come from Hackers

Cybercrime - Crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

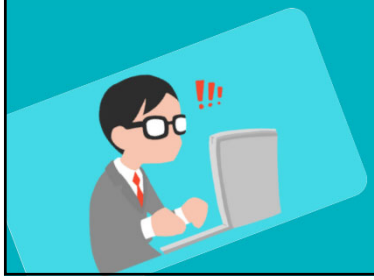
Cybercrime conducted by outsiders is a serious threat that can take many forms, but it isn't the only way things can go wrong.

Employees and Students can also pose threats.

Theft of Funds

Theft of Personal Data

Money from Ransomware



In 2016, **60% of the K–12 schools** that were hit with ransomware decided to pay attackers in order to get back control of their data. -- U.S. Department of Education.

School Systems Make Great Targets

Personal Data

50.7 Million Students
3.2 Million Teachers

Money

$654 Billion in Expenditures

Source: https://nces.ed.gov/fastfacts/display.asp?id=372

Easy Victims

- School systems make great victims because they –
  - Cannot afford the best software protections
  - IT departments are often understaffed
  - Time for training is limited
- Sept 2018 – U.S. News & World Report advises parents not to give their children's social security numbers to school systems

Recent Examples

- April 2018 – Massachusetts school system paid $10K ransom after attack – did not have off-site backups which could have helped them avoid paying
- Sept 2018 – Florida Keys school system lost access to their network for over a week due to ransomware attack – first spotted by payroll employee

The New Alabama Data Breach Notification Law

Covered entities … must implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security…

- Designate an employee to coordinate security
- Identify internal and external risks of a breach of security
- Adopt safeguards to address identified . . . and assess the effectiveness of such safeguards
- Evaluate and adjust of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information
- Keep management of the covered entity, including its board of directors, informed

Alabama Data Breach Notification Law

Sensitive Personally Identifying Information includes a username or e-mail address in combination with a password or security question and answer that would permit access to an online account likely to contain sensitive personally identifying information

Text: https://privacyhunterwilliamsblog.com/wp-content/uploads/sites/18/2018/04/Alabama-Data-Breach-Notification-Act-of-2018.pdf

Alabama Data Breach Notification Law

The Law also addresses the use of -

Third-party agents who are contracted to maintain, store, process, or is otherwise permitted to access sensitive personally identifying information in connection with providing services to a covered entity.

Lincoln Financial Group

ADP

Text: https://privacyhunterwilliamsblog.com/wp-content/uploads/sites/18/2018/04/Alabama-Data-Breach-Notification-Act-of-2018.pdf

Develop a Data Security Plan for Your Department

Start by acknowledging that your staff has a higher duty of care when it comes to data security because of their access to –

- Personal data of employees (Social Security #s)
- Bank accounts
- Critical servers

Find out what security measures are already in place and what they will and won't protect you from

- Technology Director
- Software vendors you use

Cybersecurity Requires Investment

Consider spending more on data protection measures -

- Technical staff or contracts for technical services
- Antivirus/malware software
- Up-to-date servers and workstations
- Updated firewall
- Security penetration and testing services

However, technical solutions alone won't be 100% effective.

Neither Will Relying On

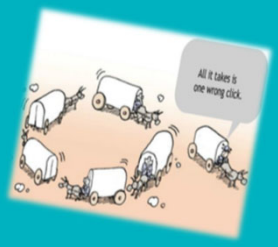
- **'Once and Done' trainings**
  - Threats change
  - New staff come on board
  - Current staff get lax
- **Scary examples**
- **Shaming and blaming**

Cultivate a Sense of Shared Responsibility

Everyone with access to your accounting and banking software is a high value target. They need to know this.

Cultivate a Sense of Shared Responsibility

Training is required, but a sense of shared responsibility will help *ensure that the training is applied*.



Email Safety is Critical

It is easiest way for outsiders to –

- Deliver ransomware
- Deliver links or malware to obtain passwords
- Conduct phishing attacks

Good Email Practices

- Don't publish your full email address online
- Never use your NextGen or banking password for any other school or personal accounts
- Don't save passwords in browsers
- Beware of downloading apps to your Smart Phone that require access to your email account or contacts

It's Not Just Links Any More

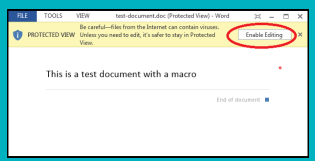
Click-less Malware –

Hackers have reacted to better training by hiding malware in Word, Excel, and PowerPoint files as macros and OLE objects. Antivirus software may not find the threat because it won't activate until you open the file and enable the macro.

*OLE – Object Linking and Embedding

Beware of Attachments from Strangers

- By clicking "Enable Editing" you can unleash malware onto your computer.
- Don't open suspicious documents even if they are from someone you know.



E-Filing Tax Return Scam

1. Steal a legitimate taxpayer's identity, including Social Security number
2. Make up phony wages or other income
3. E-file a tax return early
4. Receive refund by check or electronic transfer

The IRS doesn't match employer submitted data to e-filed returns until several months after the refunds are issued.

IRS Moves to Curb W-2 Fraud

- In 2017 the IRS began a pilot program to better authenticate W-2 forms for online filers.
- The IRS partnered with certain payroll service providers (PSPs) to include a 16-character verification code on many W-2 forms provided to employees.
- A W-2 with a verification code will display it in box 9, labeled "Verification Code."
- A W-2 without a verification code may include a blank box 9 or no box 9 at all.
- The instructions to taxpayers and tax preparers:

  "Box 9. If you are e-filing and if there is a code in this box, enter it when prompted by your software. This code assists the IRS in validating the W-2 data submitted with your return. The code is not entered on paper-filed returns."

Source: https://www.irs.gov/individuals/w-2-verification-code

Overcoming IRS Security Measures

If thieves can't use plain old identity theft to file false tax returns, they be even more motivated to steal legitimate W-2 forms.

Establish *Accounting* CyberSecurity Protocols

All accounting staff should know that email will NEVER be used to request or send sensitive information -

- Passwords to accounting software
- Passwords to bank accounts
- W-2 Forms
- Social Security numbers

Accounting staff should report any requests to the CSFC and the Technology Director by phone immediately.

Establish *Accounting* CyberSecurity Protocols

Top accounting staff should use Two-Factor Authentication (2FA) so hackers cannot log into their accounts and send bogus emails carrying ransomware, malware, or requests for personal data.

With 2FA in place, any time someone tries to log into your email account from an unrecognized device, they will be forced to enter a code texted to your cell phone. Since intruders won't have access to your cell phone, they will not be able to log in even if they have stolen your password.

Your Technology Director can require 2FA for certain types of users.

Establish *Accounting* CyberSecurity Protocols

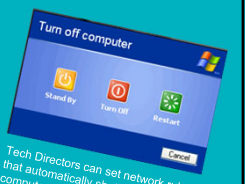
USB key fobs add an extra layer of protection for:

- Logging into various programs
- Printing payroll checks
- Logging onto bank accounts

Turn Off Computers at the End of the Day

Leaving your computer connected to the Internet when it's not in use gives scammers 24/7 access to install malware and commit cyber crimes.

Also allows employees to use private programs to access their work computer from anywhere.



Tech Directors can set network rules that automatically shut down computers at a certain time of day.

Keeping an Eye on Things

- CSFO should receive a daily report of who was logged into NextGen and when in order to identify any unusual activity.
- May want to review print logs to ensure that reports containing social security numbers are not being printed unnecessarily or by unauthorized persons.
  - These can later be scanned and uploaded to be sold online
  - May be left out in view or thrown in trash without shredding
  - Hard drives on printers retain all data. You must destroy these hard drives prior to returning leased copiers back to vendor, or make arrangements for them to do so.

12 Things Tech Directors Can Do

1. Work with CSFO to develop a security plan.
2. Require higher level administrators, including the CSFO, to use 2FA. Set up applications to require USB key fobs.
3. Set email attachment restrictions, including policies that disable macros in MS Office documents.
4. Restrict access to NextGen from public networks or have tech director set up a Virtual Private Network (VPN) for key staff who may need outside access.
5. Setup or provide login reports to CSFO.
6. Make sure check printers are not using default password.

10 Things Tech Directors Can Do

7. Ensure accounting computers meet NextGen security standards.
8. Ensure operating systems, software applications, and antivirus software updates are applied and active.
9. Protect servers with PowerShell updates.
10. Destroy hard drives of moved or dispositioned accounting computers.
11. Ensure good backup and restore practices, including offsite backups, securing backups, and formal destruction procedures for backups no longer needed.
12. Conduct periodic ransomware simulations to identify training needs.

Get Started Now

1. Establish your Accounting Cybersecurity Protocols.
2. Plan new employee training, annual training, and periodic testing of users through ransomware simulations.
3. Communicate with Human Resources Dept. Head and Superintendent.
4. Review third-party contracts to see if they are obligated to report data breaches to you. You may want to know if their servers are in the United States or not.
5. Know what protections you have in place and discuss new ones, including future budgeting, with your technology director.

ALET ALABAMA LEADERS in EDUCATIONAL TECHNOLOGY

Thank You

Susan Poling

Images and Sources

WiFi Hacker: http://www.freewifipasswordhacker.com/

Student Data: https://campustechnology.com/articles/2017/05/17/congress-seeks-to-establish-new-student-data-system-with-college-transparency-act.aspx

Handshake: https://png-library.com/png/cartoon-handshake-illustration-business-cartoons.html

Laptop Guy: https://www.triella.com/do-not-let-hackers-hold-your-data-hostage/

Circle the Wagons: https://premierrapport.com/circle-wagons-7-steps/

Single wagon: http://robertarail.com/circle-the-wagons/

Macros: https://network1consulting.com/tuesday-tip-hackers-love-macros/

Word: http://www.securitynewspaper.com/2018/02/16/hackers-find-new-way-attack-computers-without-using-macros-word/

Massachuessets Attack: https://www.cyberscoop.com/leominster-ransomware-massachusetts-bitcoin/

Florida Keys: https://www.csoonline.com/article/3305950/security/new-gandcrab-ransomware-variant-hammers-florida-school-district.html

Payroll staff: https://www.epaysystems.com/payroll-data-security-keep-payroll-data-safe/

Accounting Updates: https://www.cpapracticeadvisor.com/news/12087207/the-accountant-and-cyber-security-5-actions-your-firm-must-take

Data Breach Notification Law: https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf

Techie Stuff

Periodic updates in operating systems are commonplace and have reduced the incidence of security holes, but software applications are often overlooked except by hackers. It is crucial to update software application regularly and reboot systems to ensure that updates take effect. This includes workstations, servers, laptops and routers. In short, all the hardware and software that is used in your day to day operations.

Active Directory Policies for disabling macros in MS Office documents obtained from the Internet: https://cloudblogs.microsoft.com/microsoftsecure/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

Security Key Fobs: https://www.businessinsider.com/none-of-googles-employees-get-phished-because-of-yubikey-security-key-2018-7

Print Logs: https://www.manageengine.com/products/eventlog/print-server-management.html

Macro-less Word Exploits: http://www.securitynewspaper.com/2018/02/16/hackers-find-new-way-attack-computers-without-using-macros-word/

Windows PowerShell: Machines typically become infected through two methods: (1) when a user clicks on a link in an email, document or website; or (2) when a user's mouse hovers over a link (but does not click the link) in a macro enabled program like PowerPoint or Word. In these instances, a file is not downloaded to the hard drive nor is a program executed. The malware generally operates by using Windows PowerShell to load Base64 code directly from system memory (which cannot be scanned using heuristics). PowerShell is a command-line shell and scripting language built on top of the Windows .NET framework, so it has a trusted signature along with access to the registry, the operating system, and other Windows APIs. In layman's terms, this means that PowerShell is a powerful weapon in a hacker's war chest. Source: https://www.lexology.com/library/detail.aspx?g=f9b967e5-75d3-44a7-9122-810866fc5da3

Clickless Malware

Macro: a single instruction that expands automatically into a set of instructions to perform a particular task.

It's very difficult for network anti-virus programs to scan for these malicious links because they are hidden within a file that is within a file. Do not enable Macros on any attachments you receive via email. If you do think it's real, do yourself a favor and pick up the telephone and call the person who sent it to you to confirm.

Hackers send a DOCX document via e-mail, a document that seems harmless but, when it is executed, loads an embedded OLE object that downloads and opens an RTF document which is used to exploit the vulnerability, which executes a series of commands that finally download a VisualBasic script that, when executed, infects our system with a malware that steals our passwords and sends them to a remote server controlled by hackers.

Source: https://www.lexology.com/library/detail.aspx?g=f9b967e5-75d3-44a7-9122-810866fc5da3