Recommendations and Associated Costs

Susan Poling, Executive Director
Alabama Leaders in Educational Technology

February 2021

Accounting Departments Have Unique Responsibilities

Expected to -

- Pay employees on time, based on accurate time/attendance data
- Pay vendors on time
- Protect system funds
- Protect employee personal information

Cybercrime Impacting Accounting Departments

- Routing number scams result in loss of funds
  - Payroll direct deposit
  - Accounts payable
- W-2 scams can result in identity theft
- Ransomware can
  - Interfere with timely payroll and accounts payable
  - Prevent access to check printers
  - Result in identity theft (stolen data containing DOB, SSN, etc.)
  - Ransomware can lead to downgraded credit ratings

System Credit Rating

Credit rating agency Moody's Corp. warns that cyber defenses as well as breach detection, prevention and response will be higher priorities in its analysis of the creditworthiness of companies across all sectors, including healthcare and financial services.

https://www.bankinfosecurity.com/moodys-warns-cyber-risks-could-impact-credit-ratings-a-8702

https://www.cyberinsecuritynews.com/cyber-credit-risk

Cyber Insurance *is Not* Cybersecurity

- Rapidly developing “product”
- Contains lots of clauses that would enable the company not to pay.
- May not be issued if you aren’t already doing a great deal to protect yourself.
- Be sure what is covered. Paying the ransom that may not be the biggest cost involved.
- Be sure the insurance company has access to crypto-currency (Bitcoin).

THE EXTORTION ECONOMY

The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks

Even when public agencies and companies hit by ransomware could recover their files on their own, insurers prefer to pay the ransom. Why? The attacks are good for business.

Insurance Companies are Scaling Back Coverage

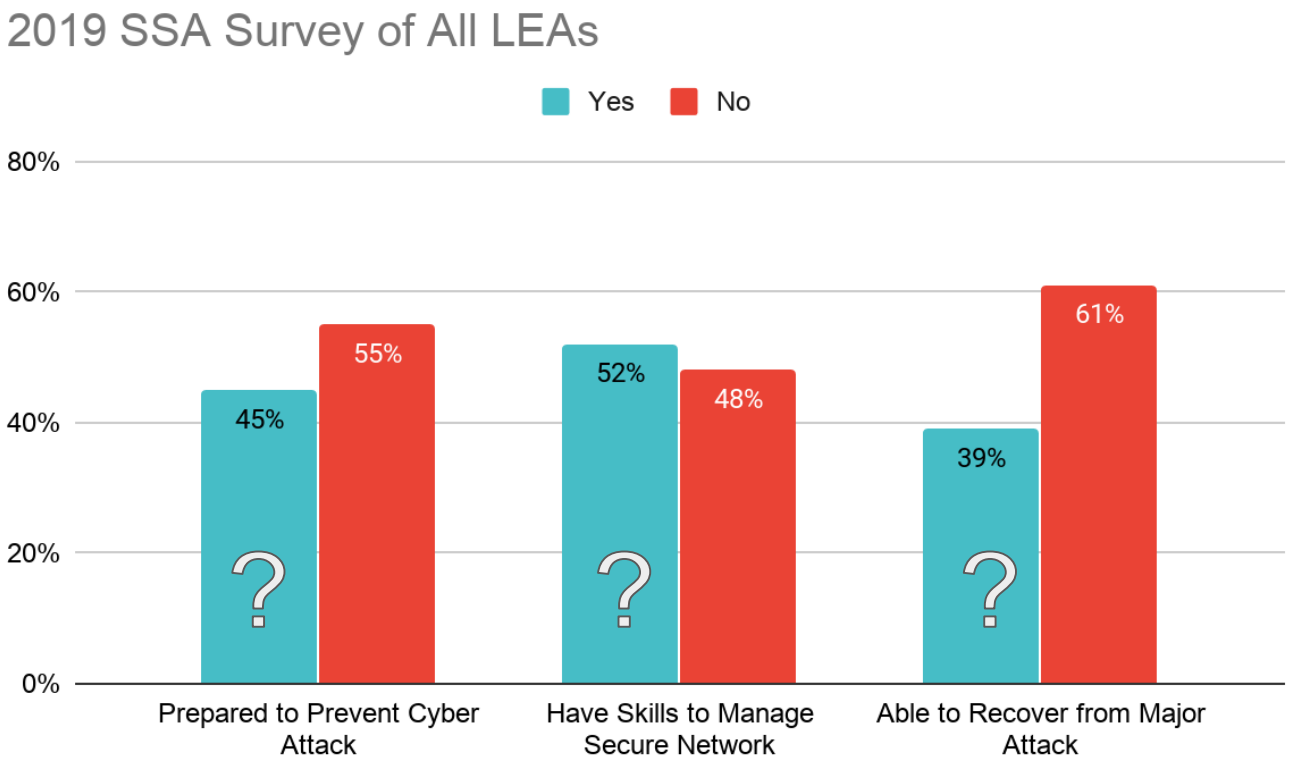
The total costs of ransom payments doubled year-on-year through the first six months of 2020, according to the report from Lloyd's of London . . .

Several industry players have told Reuters that many smaller companies have cut their cyber insurance completely this year . . .

He also said there have been much bigger jumps in rates in certain sectors, including public entities and education.

Dec 16, 2020 Yahoo News article link

Is Your System Prepared to Prevent and Recover?



COVID-Related Demands Increase Vulnerability

- Tech staff have more to implement, manage, maintain, and protect
- Most all employees have been asked to work with new, unfamiliar software or work from home in less guarded environments

Work/Learn from Home & Vulnerability

Massive shift to working/learning from home increases risk.

Home devices do not have same protections as school devices

- Patched operating systems
- Current/good antivirus
- No content filter and/or firewall
- Insecure storage on personal computers

People are more relaxed at home even when they are using a system-issued device. Devices will be used for a mixture of personal and school-related purposes.

Best Practices

Cybersecurity Best Practices

In order to be prepared, you must address all five areas of the NIST Framework.

Your security can never be 100% effective, so the Respond and Recover components are also essential.

National Institute of Standards and Technology
Cybersecurity Framework

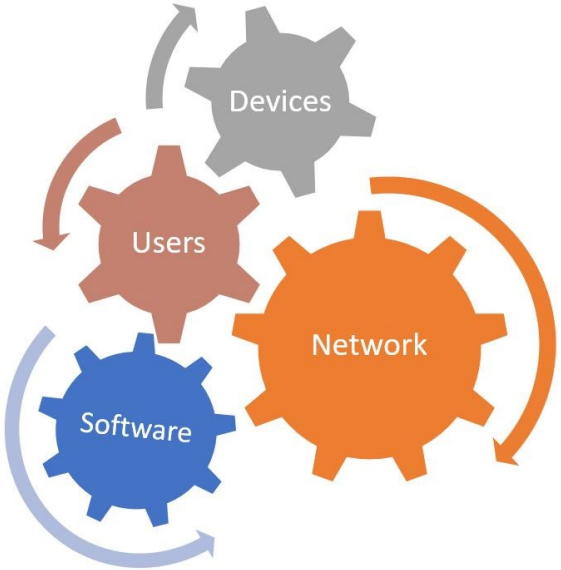
ALET Guide for Cybersecurity

- The **ALET** *Cybersecurity Best Practices Continuum* was develpoed specfically for Alabama school systems.
- **Includes 256 recommendations divided into 3 levels of complexity/expense.** All LEAs should implement Level 1 suggestions.
- Checklist can be used for self-examination.

Standard 2.5: Protect through Software, Hardware, & Contracted Services		Level 1	Level 2	Level 3
2.5.11 End User Device Backup	Establish an alternate backup plan for users who need to protect files stored on their mobile devices (laptops, tablets, phones, etc.)			○
2.5.12 User Accounts	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an emplovee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails. [CIS 16.7]	○		
	Automatically disable dormant accounts after a set period of inactivity. [CIS 16.9]	○		
	Ensure that all accounts have an expiration date that is monitored and enforced. [CIS 16.10]		○	
2.5.13 Unattended Workstations	Automatically lock workstation sessions after a standard period of inactivity. [CIS 16.11]	○		
2.5.14 Mobile Phone Use	Activate email permissions that require users to lock their mobile phones when their system email is installed, if possible.			○
2.5.15 Encryption	In Transit - Hosted applications utilize Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to protect communications as they travel across networks between systems.	○		
	Storage – All student, employee and financial data classified as Sensitive is encrypted in storage. (CSN)	○		
	Passwords to all centralized applications are encrypted in storage and in transit. (CSN)	○		

Essential Security Measures

1. User Training & Testing to Prevent Ransomware/Malware
2. Firewalls & Content Filtering
3. Penetration Testing & Vulnerability Scanning
4. Antivirus/Anti-Malware Software
5. Network Segmentation
6. User Permissions & Multi-Factor Authentication
7. Device Configuration and Security Updates
8. Hardware/Software Vetting and Security Updates
9. Secure/Encrypted Backup
10. Incident Response Plan



What You Buy

- Firewall
- Content Filter
- Employee Training
- Antivirus Software
- Backup hardware and software

If possible, add

- Additional Spam filtering system
- Intrusion detection software
- Cloud backup/ Encrypted backup
- Mobile Device Management (MDM) system

You have these, but what you have may not have advanced capabilities.

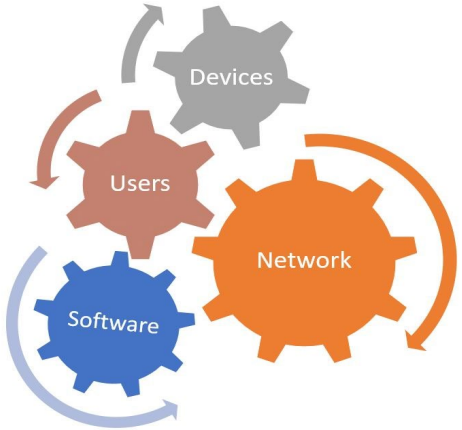
How these are implemented, maintained, and managed are critically important.

What You Do

Cybersecurity Best Practices

Standard 2.5: Protect through Software, Hardware, & Contracted Services		Level 1	Level 2	Level 3
2.5.11 End User Device Backup	Establish an alternate backup plan for users who need to protect files stored on their mobile devices (laptops, tablets, phones, etc.)			○
2.5.12 User Accounts	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails. [CIS 16.7]	○		
	Automatically disable dormant accounts after a set period of inactivity. [CIS 16.9]	○		
	Ensure that all accounts have an expiration date that is monitored and enforced. [CIS 16.10]		○	
2.5.13 Unattended Workstations	Automatically lock workstation sessions after a standard period of inactivity. [CIS 16.11]	○		
2.5.14 Mobile Phone Use	Activate email permissions that require users to lock their mobile phones when their system email is installed, if possible.			○
2.5.15 Encryption	In Transit - Hosted applications utilize Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to protect communications as they travel across networks between systems.	○		
	Storage – All student, employee and financial data classified as Sensitive is encrypted in storage. (CSN)	○		
	Passwords to all centralized applications are encrypted in storage and in transit. (CSN)	○		

80% of the Best Practices are tasks that need to be completed, most on an ongoing basis.



Email is the Number One Threat Vector

90%

of ransomware, malware, and financial cybercrime enters via email.

AASB Cybersecurity Task Force Legislative Request

The Alabama Association of School Boards' Cybersecurity Task Force was formed in 2019. It involves members from: AASB, ALET, ASBO, CLAS, SSA, and the SDE. A series of meetings, held over a period of 6 months, resulted in the following funding proposals to combat cybercrime.

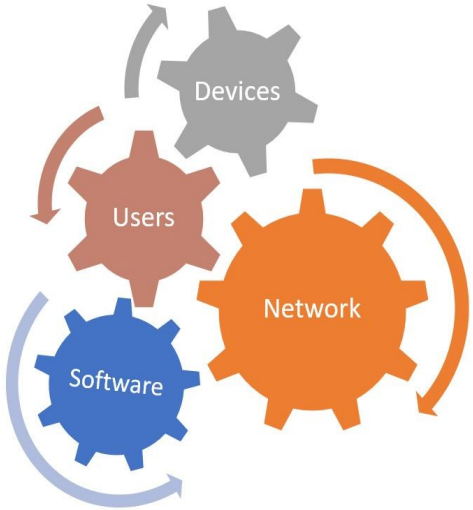
FY20 Supplement	Cybersecurity training for all employees (KnowBe4 or ThreatAdvice)	$1M for 2 years (Approx. $5.50 per employee, per year)
FY22 Priority	Network Administrator/Services	$68K per LEA
	Backup Solutions	$2.50 per Student
	Antivirus/Malware Software	$3.75 per Student

Training & Phishing Paid for by Legislature

- FY20 supplemental budget included $1 million in funding for training
- Administered through Alabama Supercomputer Authority
- Two-year contract for software, beginning in Sept 2020

Security Requires a Continuous Effort

- School technology is constantly changing.
- Hackers are continually trying out new exploits to overcome existing protections.
- Someone needs to continually monitor the changes and make adjustments in order to keep things secure.
- Not all Technology Directors have the skills to manage comprehensive security measures.

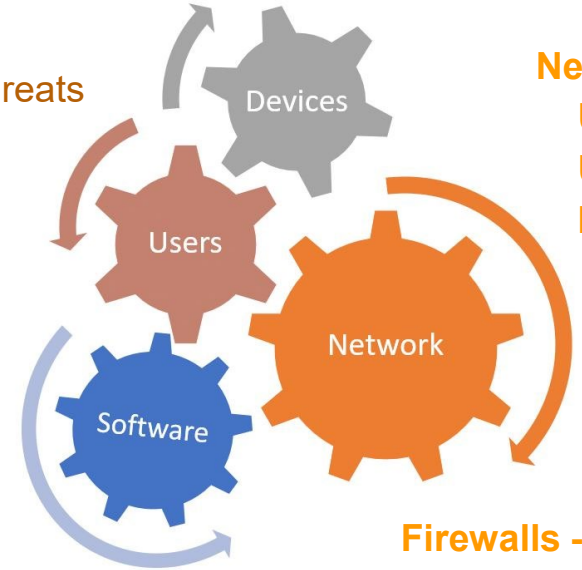


Lack of Management Increases Risk

Users
User permissions too high for need
No one monitoring suspicious logins
Spam filters not adjusted for emerging threats
Poor password security management

Software
Outdated/unpatched software
Compromised accounts
Location of software on the network
Inadequate antivirus/malware software
Unused software left in service
Memorandums of Agreement with SW providers

Device/Server Operating Systems -
Unpatched/outdated operating systems
Poor admin account protections



Network Design -
Un-segmented network (flat)
Unprotected Wi-Fi
Backups on same network

Content Filter -
Inadequate filter allows
Traffic to/from bad websites

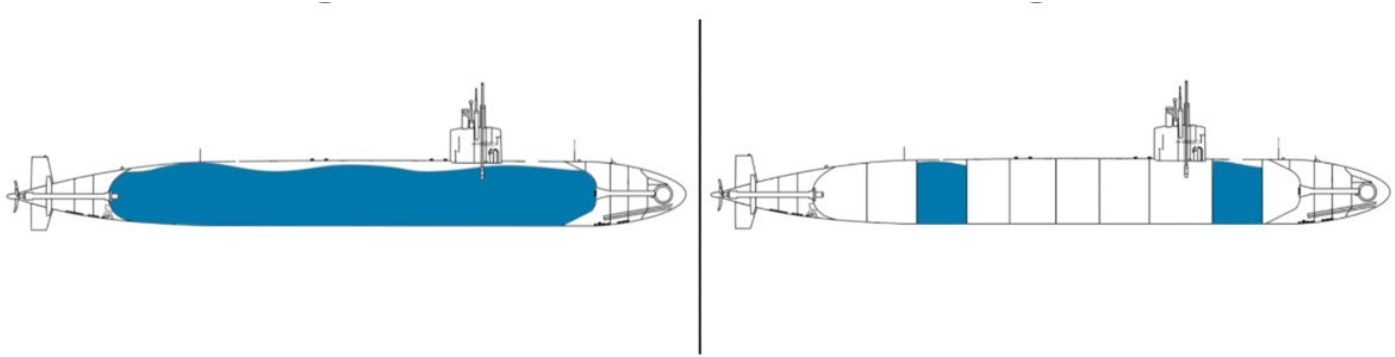
Firewalls -
Outdated, poorly configured, or inadequately managed

Network Design - Segmentation

Networks that are not segmented are like submarines with no compartmentalization. If the right malware gets in, it can flood the entire network faster than anyone can react.

Submarine w/o Compartmentalization

Submarine with Compartmentalization

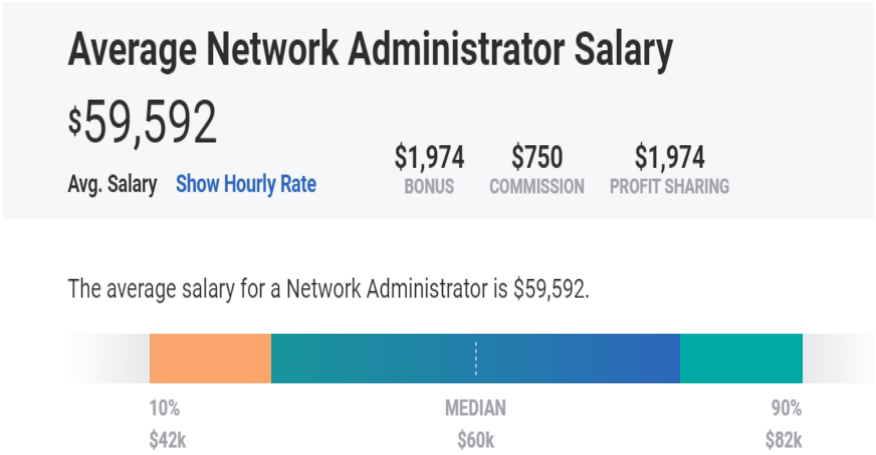


SSA survey shows 34% of LEA networks are not segmented.

https://www.illumio.com/network-segmentation

Network Admin Pay Scale

From: Payscale.com for Alabama



	Approximate
Salary (entry level)	$48,133
Benefits (21%)	$10,267
Insurance	$9,600
Total	$68,000

National average salary is $83,000.
Figures shown above are for Alabama.

Employee vs. Outsourcing

Staff

- Knows the network, users, and software better
- Vets devices and software prior to purchase
- Frequent communications with LEA administrators, employees, and technology providers

Contractor

- Personnel assigned to the account may change frequently
- Won’t know network, users, or technology as well as an employee
- Cost per hour can be high and include travel time

ALJP Bid Pricing for IT Services

IL-TierTwo	Network Techician, Server Support, Proj Mgt	Hr.	$131.58
IL-TierThree	Network Engineering, Adv Systems Support, MCSE	Hr.	$157.89
IL-TierFour	Solutions Architect, Systems Consulting, Storage/Virtualization Design	Hr.	$184.21
IL-TierFive	Certified Classroom Technology Trainer	Hr.	$205.26
IL-CabTech	Lead Cable Technician	Hr.	$68.42
IL-CabAsst	Cabling Assistant	Hr.	$57.89
IL-Travel	Travel	Hr.	$100.00

Hourly rate for Advanced AV engineer/Programmer	$136.50
Hourly rate for travel	$78.75

Network Technician	$	100.00	Hour	10%	$	90.00
Network Engineer	$	125.00	Hour	10%	$	112.50
Senior Network Engineer	$	175.00	Hour	10%	$	157.50
Project Manager	$	175.00	Hour	10%	$	157.50
Training - Per Hour	$	125.00	Hour	10%	$	112.50

Hiring vs. Contracting

240 Day Work Year (12 month employee)	**240 x 8 hrs = 1920 Hours**
Salary + Benefits	**$68,000**
Hourly Cost	**$35.41**

240 Day Work Year (12 month employee)	**240 x 8 hrs = 1920 Hours**
Contractor Network Technician Hourly Rate	**$90.00** (lowest rate – network technician)
Cost for Working Same # Hours	**$172,800**

Hiring vs. Contracting

240 Day Work Year (12 month employee)	**240 x 8 hrs = 1920 Hrs.**
Salary + Benefits	**$68,000**
Hourly Cost	**$35.41**

Contract	**$68,000**
Contractor Network Technician Hourly Rate	**$90.00** (lowest rate – network technician)
Hours/Weeks	**755 Hrs. or 18 Weeks** (40 hr.)

Education Trust Fund Budget Request

(h) Information Technology Services Program (FY21 HB187, page 23)

The above appropriation shall be experienced by local systems towards the position of a district Technology Coordinator that meets the job description and qualifications established by the State Board of Education. ($8,775,573)

In addition to the district Technology Coordinator, this funding shall provide for network administrative services through employment or contacted services; qualifications and duties to include cybersecurity. (≈ $9,384,000)

What Can CSFO's Do?

- Ensure all accounting staff completes training and passes phishing tests
- Add cybersecurity performance to employee evaluations
- Develop a departmental incident response plan
  - Consult with Technology Director
  - Get advice from Harris and/or other SW providers
- Budget for Protection Measures
  - Prioritize investments in line with what posses the greatest risk
  - Understand that many measures will have recurring costs
- Implement Accounting Department specific cybersafety practices

Rules & Guidelines Improve Security

- Prohibit risky email practices
  - Don’t use district email address for personal use
  - Don’t check personal email on district devices
- Expect off-campus use of devices/accounts to be safe
  - Prohibit accessing critical accounts over public Wi-Fi

- Require Multi-Factor-Authentication for high risk accounts
- Prohibit downloading of senstive data to personal devices
- Prohibit employees from saving passwords in browsers at work and at home
- Expect staff to immediately report suspicious events
- Expect supervisors to review logs for unusual activity by accounting staff

Create an Accounting Incident Response Plan

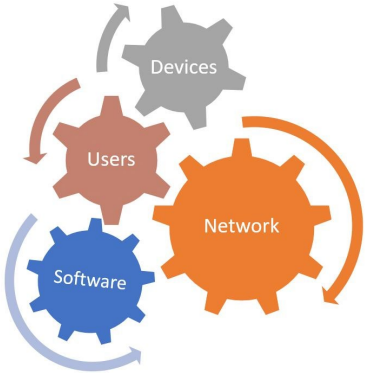
Have a plan for how your staff will work in the event that they are unable to access critical technology systems, such as –

- Accounting workstations and software
- Specialized printers for check writing, etc.
- Phone system
- Know how your data is backed up and how this is kept safe from being encrypted during an attack

Better Informed CSFOs

Threats

- Financial cybercrime
- Ransomware
- Identity theft
- Corrupted data



Protection Measures

What does your system have in place for each of the 5 components?

Who is managing Your IT security?

True or False?

A. Cybersecurity is the sole responsibility of the technology director.

B. Cybersecurity is a shared responsibility among all system employees.

True or False?

A. Cybe[illegible]rity is the sole r[illegible]onsibility of the te[illegible]ology direct[illegible]

B. **Cybersecurity is a shared responsibility among all system employees.**

CSFOs and Staff Can Impact Cybersecurity

1. Budget for critical measures and someone to implement and manage them
2. Establish department/role specific cybersecurity safety practices
3. Ensure new staff receive accounting-specific cybersecurity training
4. Include cybersecurity behavior as part of employee evaluations
5. Develop a cybersecurity Incident Response Plan and train appropriate staff

Thank You

Susan Poling, Executive Director
susan.poling@go-alet.org