Cybersecurity

What Board Members Should Know

AASB District Meetings

Susan Poling, Executive Director
Alabama Leaders in Educational Technology

Today’s Goal

- Impact of Cybercrime on Schools
- Best Practices
- Essential Components
- Costs
- Role of Board Member

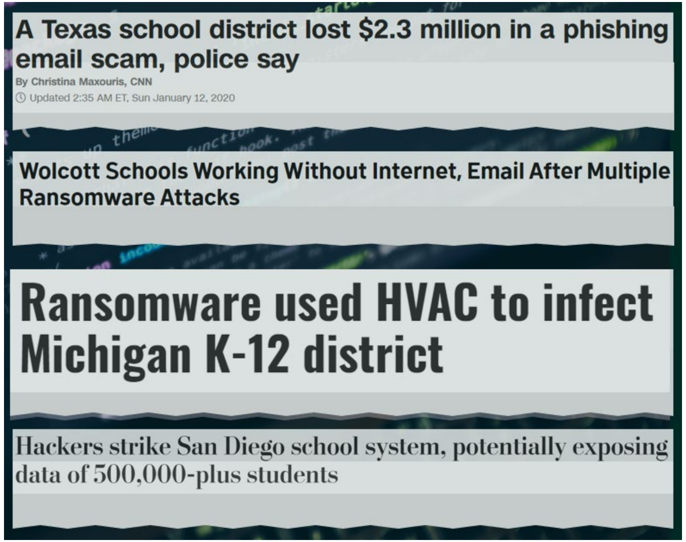
Impact of COVID on Cybersecurity

Massive shift to working/learning from home increases risk because -

- Home devices do not have same protections as school devices (antivirus, firewall, content filter, etc.)
- People are more relaxed at home
- Devices are used for personal and school-related purposes
- Tech Directors are so busy, they may not be focusing on protection measures

Cybercrime – The Other Epidemic

- Hackers attack every 39 seconds, on average 2,244 times a day
- 71% of breaches were financially motivated



A Texas school district lost $2.3 million in a phishing email scam, police say

By Christina Maxouris, CNN

Updated 2:35 AM ET, Sun January 12, 2020

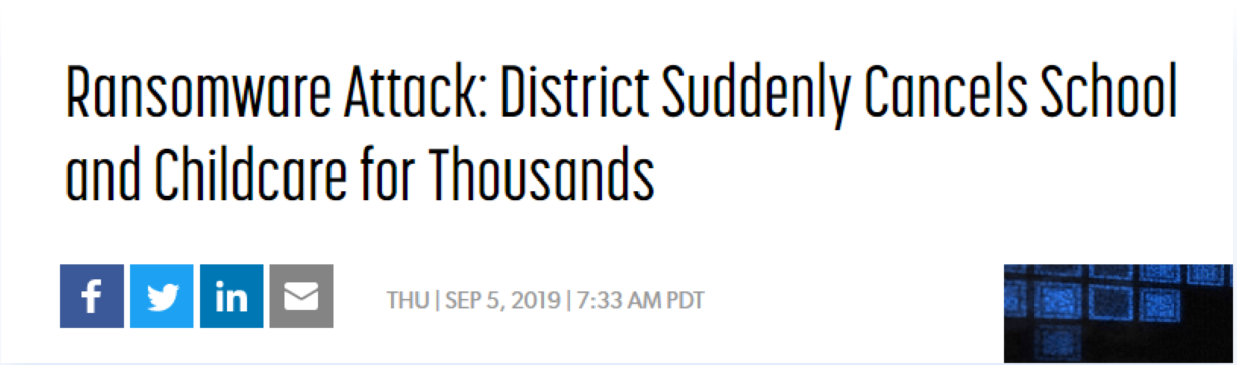
Wolcott Schools Working Without Internet, Email After Multiple Ransomware Attacks

Ransomware used HVAC to infect Michigan K-12 district

Hackers strike San Diego school system, potentially exposing data of 500,000-plus students

What’s at Risk?

Ability to Function

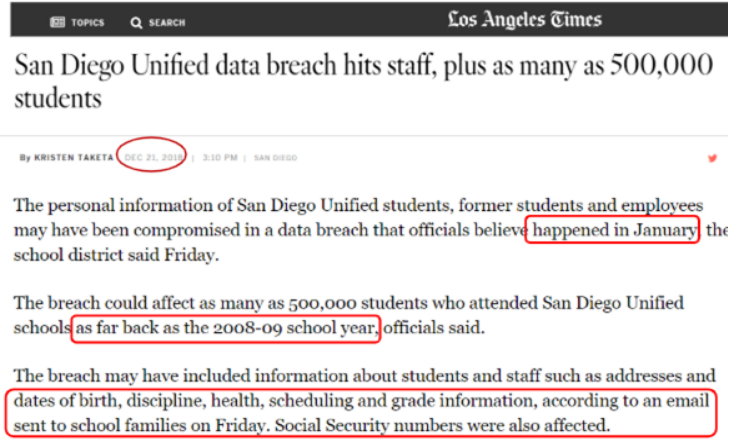


Ransomware Attack: District Suddenly Cancels School and Childcare for Thousands

THU | SEP 5, 2019 | 7:33 AM PDT

Attacks can encrypt computers, servers, phone systems and other digital systems. Can enter the system via email, firewall, USB drive, or even IoT systems, like HVAC.

Data – Identity Theft



TOPICS SEARCH Los Angeles Times

San Diego Unified data breach hits staff, plus as many as 500,000 students

By KRISTEN TAKETA DEC 21, 2018 | 3:10 PM | SAN DIEGO

The personal information of San Diego Unified students, former students and employees may have been compromised in a data breach that officials believe happened in January, the school district said Friday.

The breach could affect as many as 500,000 students who attended San Diego Unified schools as far back as the 2008-09 school year, officials said.

The breach may have included information about students and staff such as addresses and dates of birth, discipline, health, scheduling and grade information, according to an email sent to school families on Friday. Social Security numbers were also affected.

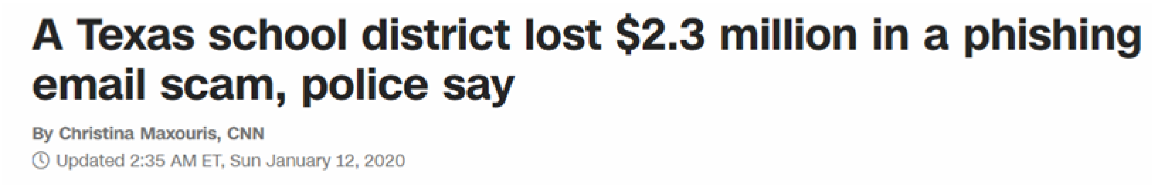
ress and ZIP code
ployer's state ID num
Form W-2 Wage and Tax Statement
Copy B—To Be Filed With Employee's FEDERAL Tax
information is being furnished to the Internal Rev

Even if future Student Information Systems do not require student social security numbers, historical data in INOW and other applications contain this information.

System Funds

Atlanta public schools lost $65,000 to direct deposit scams in 2017.

(SHREVEPORT, LA) Jan 8, 2019 - **Almost $1 million in public funds, designated for a charter school in Shreveport, were diverted from a Caddo Parish school system account to an overseas account**



A Texas school district lost $2.3 million in a phishing email scam, police say

By Christina Maxouris, CNN

Updated 2:35 AM ET, Sun January 12, 2020

Personal Funds

Alabama teachers are being fooled into purchasing hundreds or thousands of dollars worth of gift cards with their personal credit cards and sending codes to individuals impersonating their supervisors.

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

THE SIXTH C OF CREDIT IS CYBER

Schoolchildren learn the 3 Rs. Credit officers learn the 5 Cs. Now there's a new risk to worry about.

By Kurtis Suhs

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

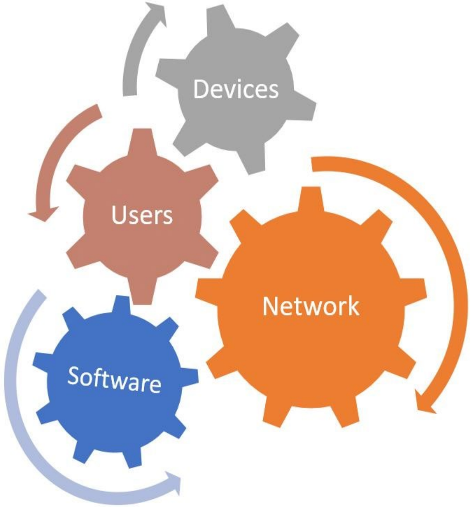
Good cybersecurity measures and an effective Incident Response Plan saved the Flagstaff, Arizona school district from having their credit rating lowered on a multi-million bond when it was hit by ransomware in 2020.

Reputation

Parents, staff and students trust schools to keep their data secure.

School System Technologies

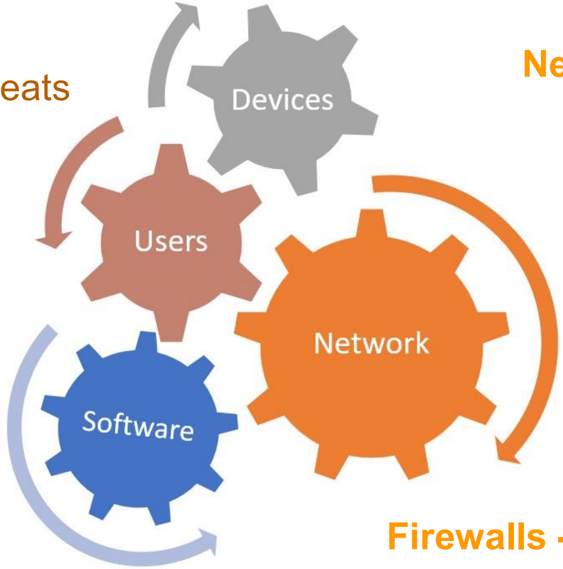
- Interconnected and continually changing
- Criminals continually try new exploits against each of the elements



Every Component has Vulnerabilities

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

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

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

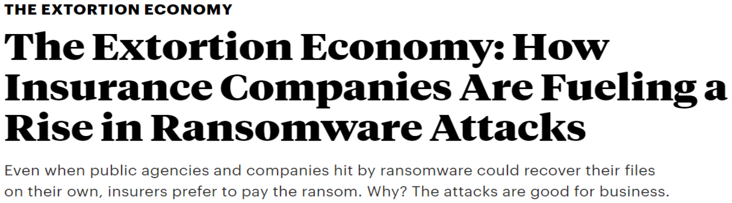
Content Filter -
Inadequate filter allows
Traffic to/from bad
websites

Firewalls -
Outdated, poorly configured, or
inadequately managed

How Do You Stay Protected?

Cyber Insurance is Not Cybersecurity

- Rapidly developing “product”
- Contains lots of clauses that could 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 may not be the biggest cost involved.
- Be sure the insurance company has access to crypto-currency (Bitcoin).



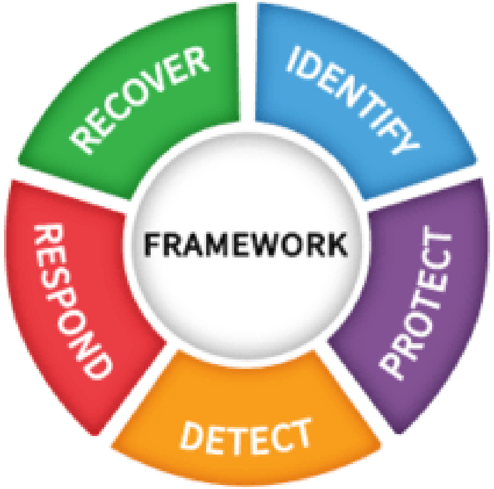
THE EXTORTION ECONOMY

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.

National Standards

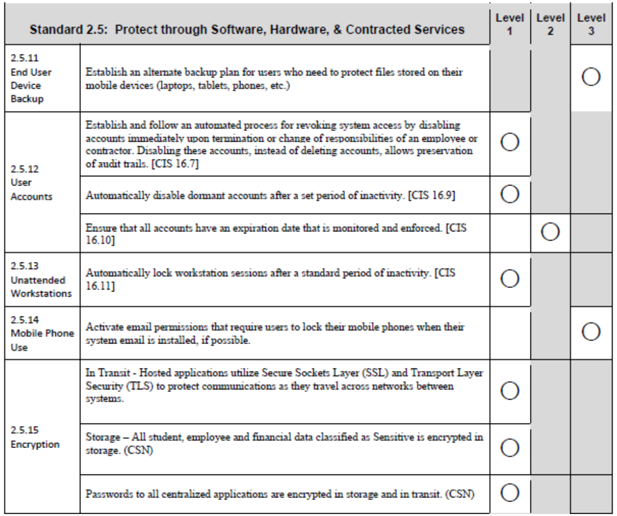
In order to be prepared, you must address **<u>all five areas</u>** of the NIST Cybersecurity Framework.



National Institute of Standards and Technology

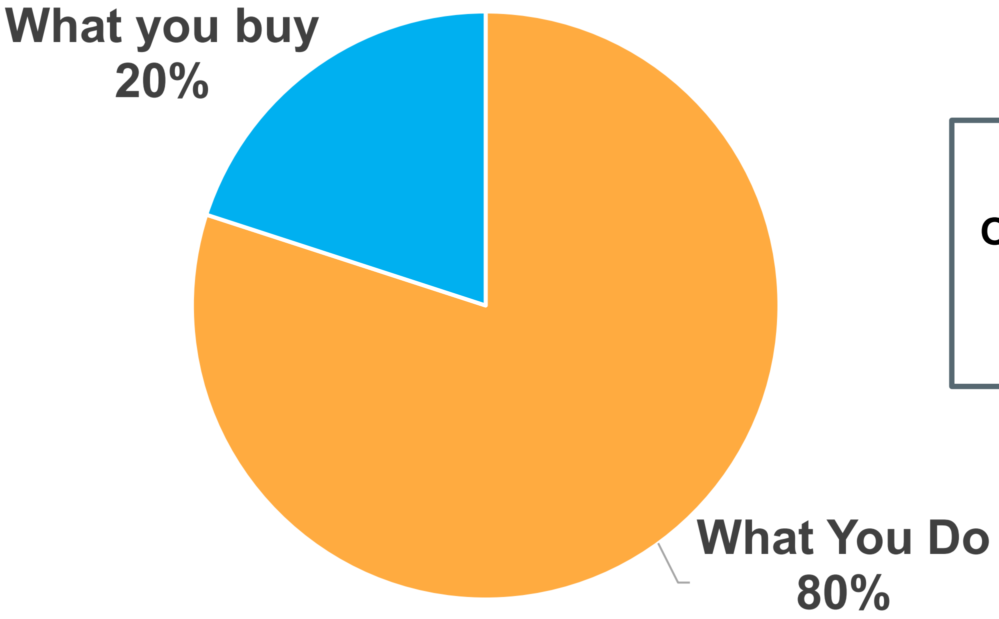
Alabama Leaders in Educational Technology

- *ALET Cybersecurity Best Practices Guide*
- 256 recommendations specifically for K12
- Three levels of complexity and/or expense
- All LEAs should implement Level 1
- Checklist can be used for self-assessment



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)	○		

Cybersecurity Measures

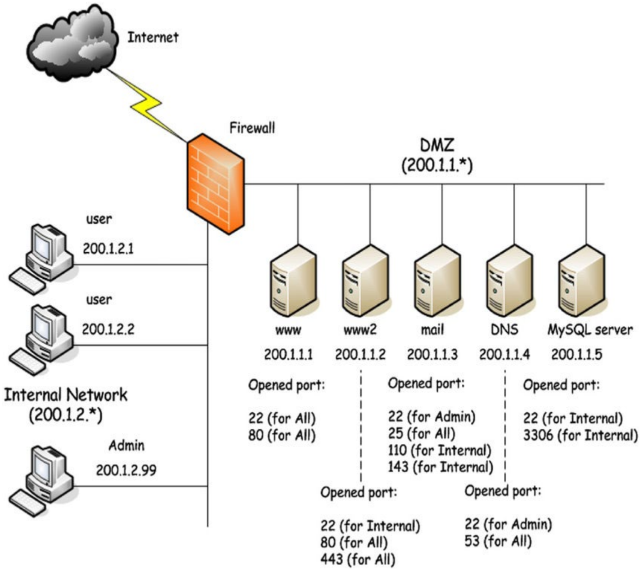


Over 50% of “What You Do” needs continual attention.

Step 1 - Identify

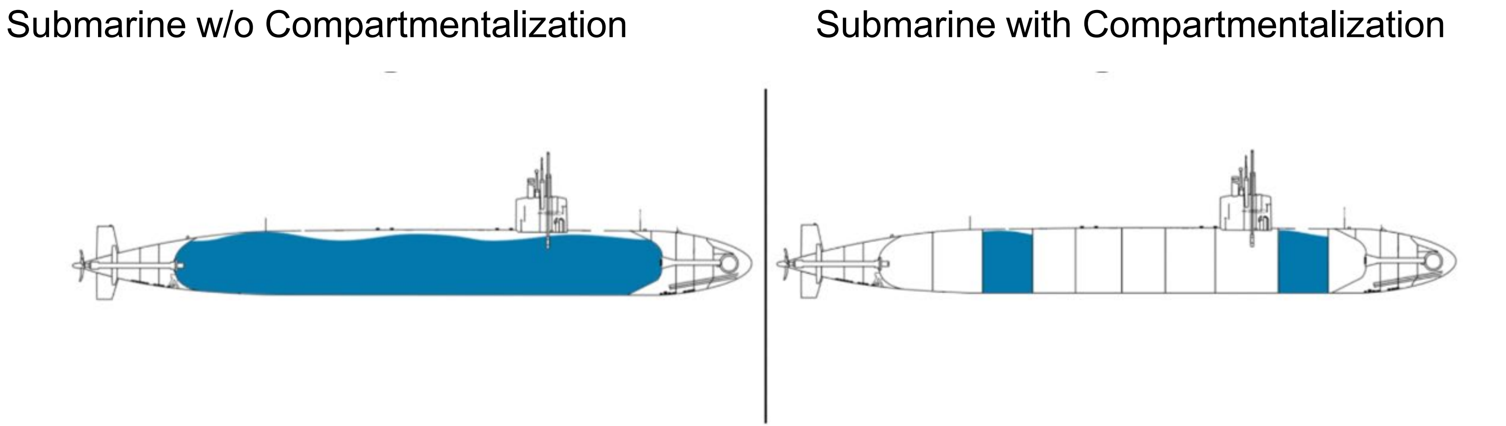
New Tech Directors often walk into situations where key assets have never been mapped and have no clear idea of what the LEA’s security status is.

- Where is confidential and critical data stored?
- How vulnerable is it?
- Who has access to it?
- Is it securely backed up?



Example of a Periodic Task

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

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

Over 1/3 of LEA networks need to improve their network design.

Examples of Ongoing Tasks

Users

Create, delete, manage user accounts

Disable accounts of terminated employees

Grant & update user permissions

Monitor for suspicious logins

Adjust spam filter settings

Enforce password security

Manage user cbyer training

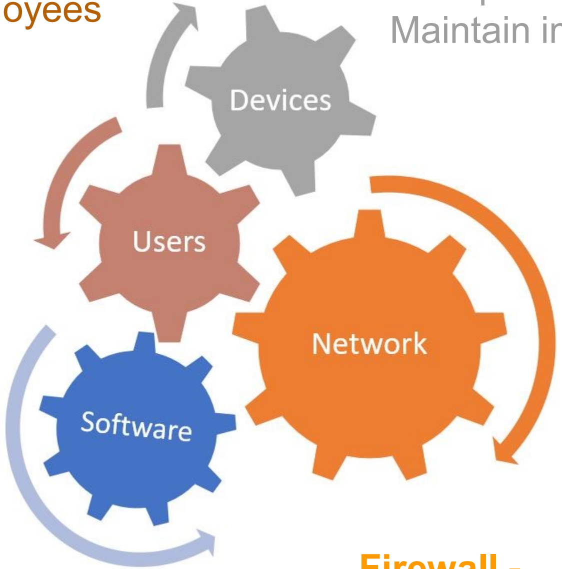
Perodically issue phishing tests

Device/Server Operating Systems –

Patch or replace operating systems

Limit permissions to admin accounts

Maintain images for restore purposes



Network -

Patch/update gear

Monitor for unusual activity

Adjust design for security

Content Filter -

Update settings

Configure devices to use

Software

Patch or remove outdated software

Monitor suspicious logins

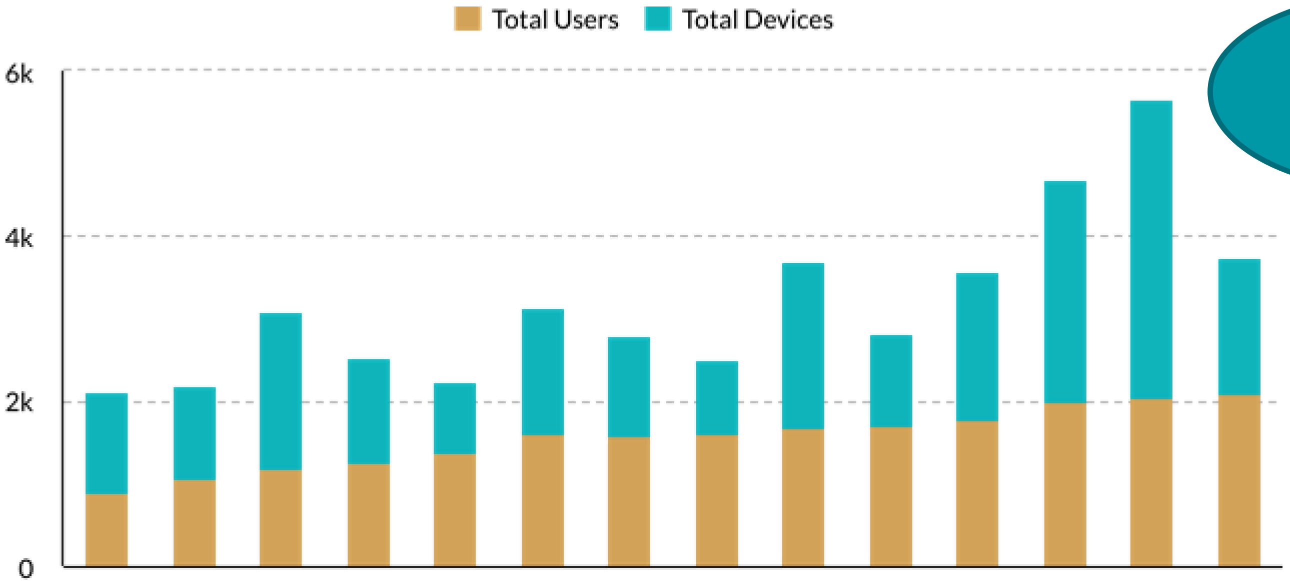
Vet new purchases or use of freeware

Ensure AV is up-to-date & deployed

Firewall -

Adjust in accordance with internal changes and external threats

When it comes to Technology – There are no Small School Systems



Device numbers are pre-COVID.

Even the smallest school systems in Alabama have over 2,000 combined users & devices to manage. Not to mention the network, backups, teacher training, software management, etc.

Essential Cybersecurity Components

- Network Administrator
- Employee Training
- Antivirus
- Secure Backup
- Firewall
- Content Filter

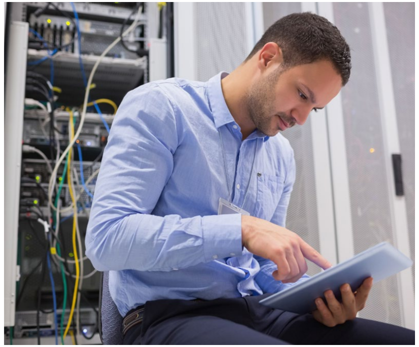
ALABAMA ASSOCIATION OF SCHOOL BOARDS

Cybersecurity Task Force 2020

AASB Cybersecurity Task Force includes AASB, ALET, SSA, CLAS, ASBO, SDE, ASA.
Studied the problem, determined highest priority needs, requested funding from State legislature.

Network Administrator

- Determines an organization’s system needs and installs network hardware and software
- Makes needed upgrades and repairs to networks and ensures that systems are operating correctly
- **Maintains network and computer system security**
- Evaluates and optimizes network or system performance
- Adds users to a network, and **assigns and update security permissions** on the network
- Trains users in the proper use of hardware and software
- **Interprets and solves problems** when a user or an automated monitoring system alerts them that a problem exists

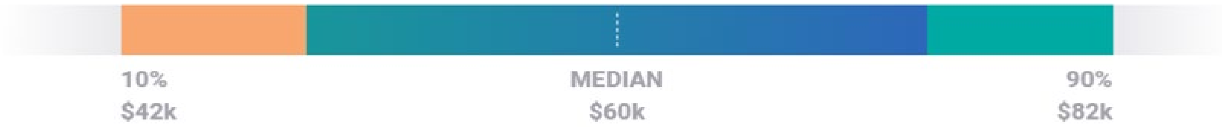


Bureau of Labor Statistics list of duties for Network Admin

Network Administrator Salary

Alabama salary range - $42,000 to $82,000

(Payscale.com)



National average salary is $83,000

Considerations include the qualifications, years experience, local area comparable salaries (including in private sector), and your system’s tolerance for turnover.

Task Force Advocacy

ALABAMA ASSOCIATION OF SCHOOL BOARDS

Cybersecurity Task Force 2020

AASB Cybersecurity Task Force has requested $68,000 annually per LEA for network administration – (staff or contractor).

Staff is Generally Better than Contracting

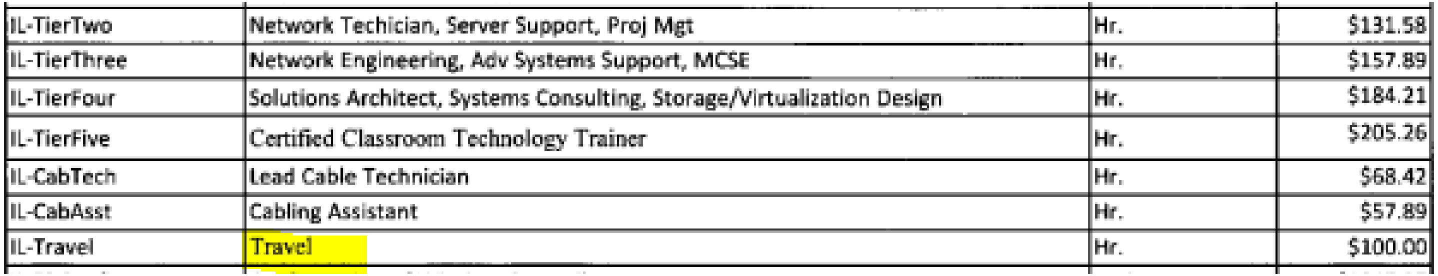
Staff

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

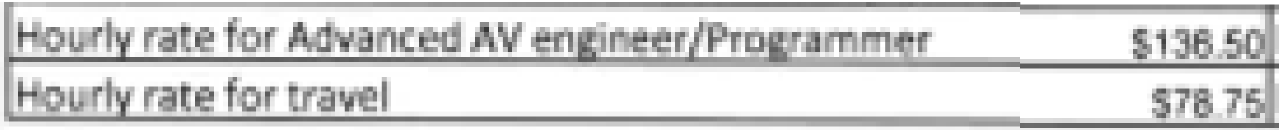
Contractor

- 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
- Pay for travel time

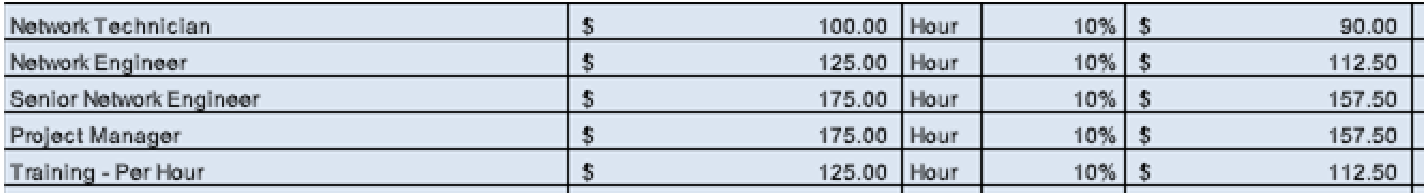
Alabama Joint Purchasing Bid Pricing



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

Cost Comparision for Same Number of Hours

240 Day Work Year (12 month employee)	**240 x 8 hrs = 1920 Hours**
Salary (≈$48,000*) + Benefits	**$68,000**
Hourly Cost	**$35.41**

*Does not represent a suggested salary.

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

Essential Cybersecurity Components

- Network Administrator
- **Employee Training**
- Antivirus
- Secure Backup
- Firewall
- Content Filter

ALABAMA ASSOCIATION OF SCHOOL BOARDS

Cybersecurity Task Force 2020

AASB Cybersecurity Task Force includes AASB, ALET, SSA, CLAS, ASBO, SDE, ASA.
Studied the problem, determined highest priority needs, requested funding from State legislature.

Employee Training

- **90% of cybercrime enters via email**
- **Any employee with an email account can click the wrong link, download the wrong attachment, or follow malicious instructions**
- **Software includes unlimited Phishing tests**

KnowBe4
Human error. Conquered.

LEAs have selected one of these two.

Will get 2 year license for all employees.

ThreatAdvice
Assess. Educate. Insure.

ALABAMA ASSOCIATION OF SCHOOL BOARDS
Cybersecurity Task Force 2020

AASB Cybersecurity Task Force succeeded in getting $1 million in the FY20 supplemental budget for employee cybersecurity training!

Essential Cybersecurity Components

- Network Administrator
- Employee Training
- **Antivirus**
- Secure Backup
- Firewall
- Content Filter

ALABAMA
ASSOCIATION OF
SCHOOL BOARDS

Cybersecurity Task Force 2020

AASB Cybersecurity Task Force includes AASB, ALET, SSA, CLAS, ASBO, SDE, ASA.
Studied the problem, determined highest priority needs, requested funding from State legislature.

Antivirus

Centrally-managed AV is essential.

Some work by identifying known virus files.

More sophisticated AV SW also reacts when it detects a device that is acting suspiciously, i.e. when it detects that the machine is being encrypted by ransomware.

Costs for AV/Anti-malware software vary greatly.

Essential Cybersecurity Components

- Network Administrator
- Employee Training
- Antivirus
- **Secure Backup**
- Firewall
- Content Filter

ALABAMA
ASSOCIATION OF
SCHOOL BOARDS

Cybersecurity Task Force 2020

AASB Cybersecurity Task Force includes AASB, ALET, SSA, CLAS, ASBO, SDE, ASA.
Studied the problem, determined highest priority needs, requested funding from State legislature.

Secure Backup

Good backup strategies are critical.

Ransomware will search across networks, for backup systems. If the hacker can encrypt the backups, then the victim may have no choice but to pay the ransom.

Encrypted backups also ensure that if the hacker gets to the backups, they can’t harvest the data.

Backups must be tested periodically to be sure they can be restored.

Essential Cybersecurity Components

- Network Administrator
- Employee Training
- Antivirus
- Secure Backup

ALABAMA ASSOCIATION OF SCHOOL BOARDS

Cybersecurity Task Force 2020

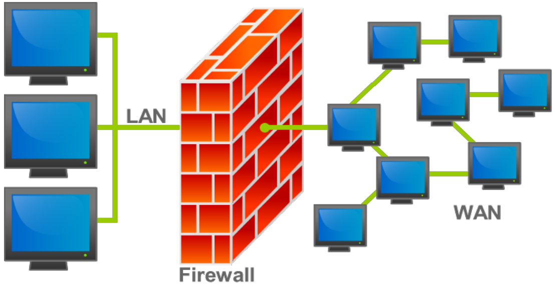
- **Firewall**
- **Content Filter**

Not included in AASB Cybersecurity Task Force funding request, but are essential components.

Alabama Supercomputer Authority provides **basic** firewall and content filtering services to school systems who use them for their Internet access. Some LEAs who use ASA have chosen to purchase their own firewall & filter in order to access more advanced features.

Firewall

Content Filter

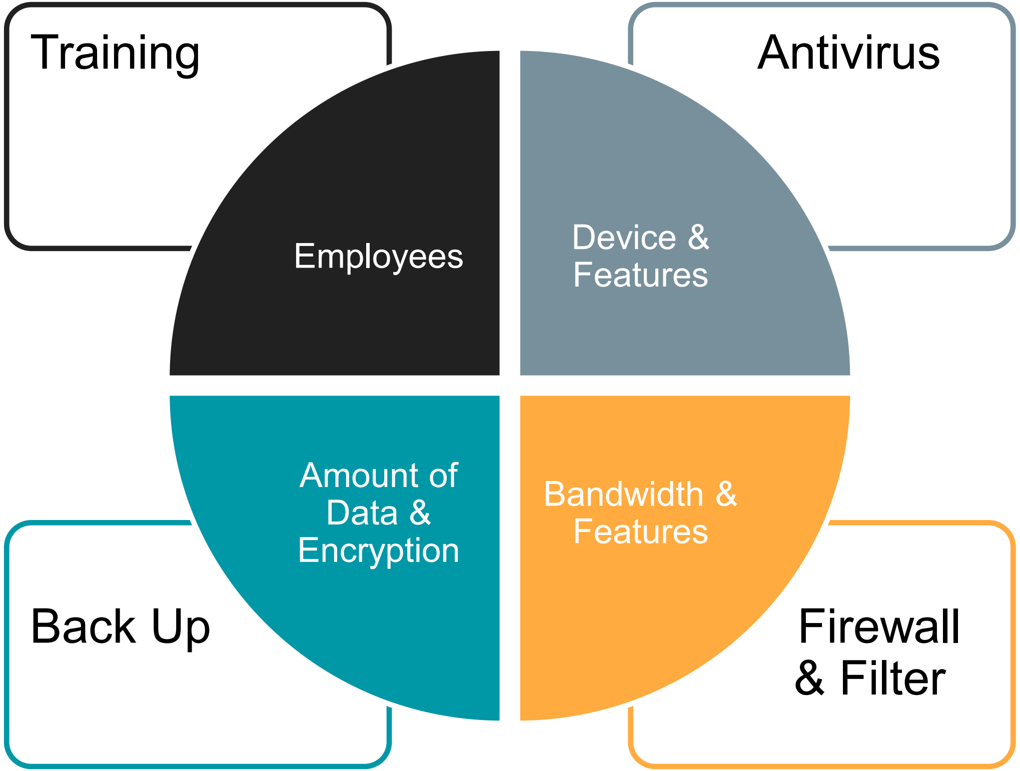


Firewalls can be set to allow or block different types of digital traffic from entering your network. Next Generation Firewalls provide even more protection by inspecting encrypted traffic and allowing more advanced blocking.

Http (web) traffic must be allowed to pass through the Firewall. That is why you also need a Content Filter.

Content filters further restrict web traffic. They can prevent your users from reaching inappropriate or malicious sites when they search the web or click on a malicious link.

Security Cost Metrics



Training

Employees

Antivirus

Device & Features

Back Up

Amount of Data & Encryption

Firewall & Filter

Bandwidth & Features

Sample of *Annual Recurring* Costs from 2019

LEA	Employee Training	Annual Antivirus	Annual Backup Costs	Annual Firewall	Annual Content Filter	Actual Total	Avg Per User + Devices
System 1	$0	$4,333	$4,500	$0	$0	$8,833	$2.49
System 2	$0	$7,567	$0	$0	$4,700	$12,267	$3.74
System 3	$0	$3,823	$0	$0	$11,040	$14,863	$3.17
System 4	$0	$3,750	$3,100	$12,721	$8,776	$28,347	$5.01
System 5	$0	$11,629	$8,000	$10,000	$10,755	$40,385	$2.95
System 6	$0	$34,543	$16,000	$25,200	$62,780	$138,523	$4.46
System 7	$0	$64,000	$50,000	$18,333	$140,000	$272,333	$3.24
System 8	$0	$88,506	$29,667	$25,333	$50,000	$193,506	$2.72
						Average	$3.47

School Boards and Cybersecurity

What Can You Do?

- Educate yourself about cybersecurity
- Request a briefing from your Technology Director
    - AL Data Breach Laws recommends this
    - Do it in an executive session in order not to expose your system’s vulnerabilities
- Implement policies & Set Expectations
- Prioritize & Fund
    - Prioritize investments in line with what poses the greatest risk
    - Understand that many measures will have recurring costs

Policies, Rules, & Guidelines

- Technology Acceptable Use Policies are *not enough*
- Rules /Guidelines for employee’s use of email & district devices
- Human Resources Practices
  - Add digital security responsibility to all job descriptions
  - Add digital security behavior to employee evaluations for staff with high-risk access
  - Ensure that IT is notified promptly of any employees put on administrative leave or terminated
- Require Multi-Factor Authentication (MFA) for staff with high level access
- Insist on an Incident Response Plan being developed and implemented

Incident Response Plan

- Incident response is a well-planned approach to addressing and managing reaction after a cyber attack or network security breach.
- The goal is to minimize damage, reduce disaster recovery time, and mitigate breach-related expenses.

https://phoenixnap.com/blog/cyber-security-incident-response-plan

How well you respond, how fast you respond, and how you effectively you communicate about cyber incidents can make a huge difference in the amount of damage done.

Policies Alone Won’t Work

> **“Culture eats strategy for breakfast.”**
> Peter Drucker

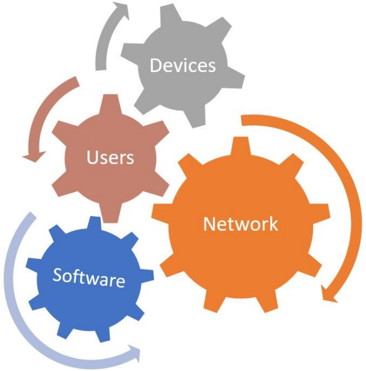
Expect everyone to share in the responsibility.

Reward and celebrate success! Don’t shame and blame.

Better Informed Board Members Can Lead to Better Cybersecurity

Threats

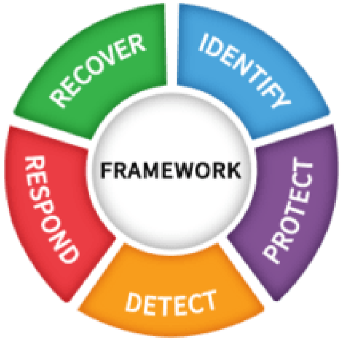
- Financial cybercrime
- Ransomware
- Identity theft
- Corrupted data



Protection Measures

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

Who is managing Your IT security?



Thank You

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