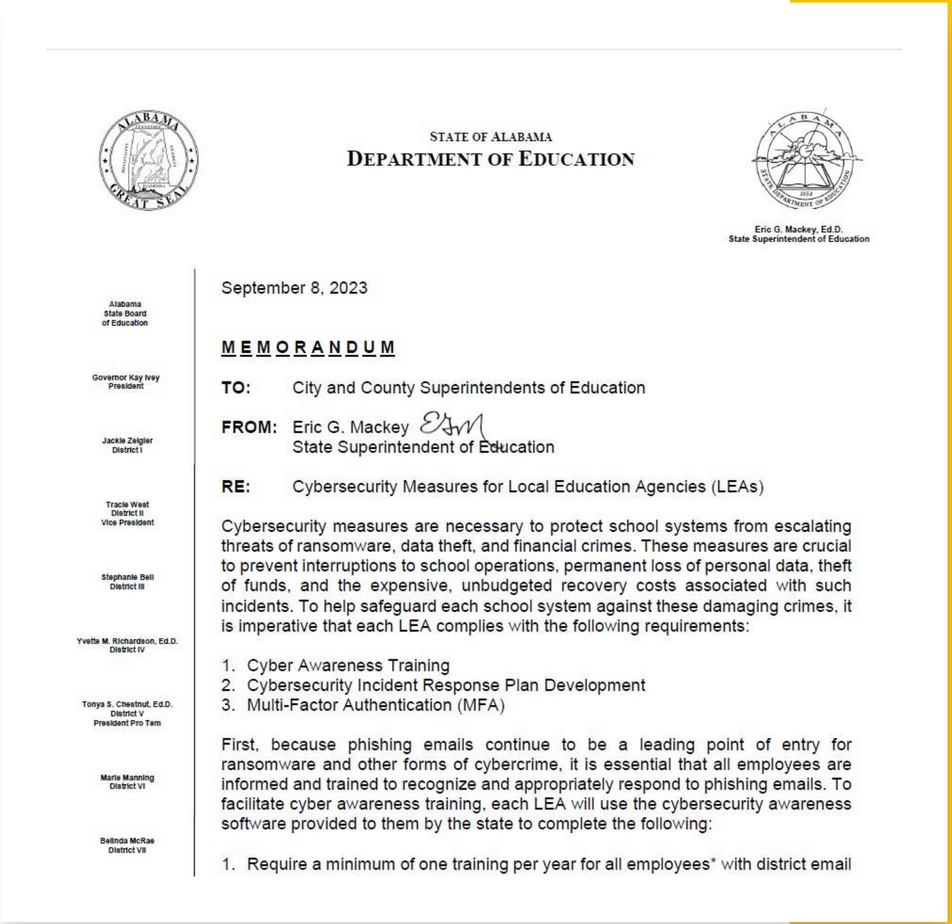
ALET
ALABAMA LEADERS in EDUCATIONAL TECHNOLOGY

Cybersecurity

Susan Poling, Executive Director

State Department Cybersecurity Memo

- Employee training/phishing
- Multi-Factor Authentication
- Incident Response Plan



STATE OF ALABAMA
DEPARTMENT OF EDUCATION

Eric G. Mackey, Ed.D.
State Superintendent of Education

Alabama
State Board
of Education

Governor Kay Ivey
President

Jackie Zeigler
District I

Tracie West
District II
Vice President

Stephanie Bell
District III

Yvette M. Richardson, Ed.D.
District IV

Tonya S. Chestnut, Ed.D.
District V
President Pro Tem

Marie Manning
District VI

Belinda McRae
District VII

September 8, 2023

MEMORANDUM

TO: City and County Superintendents of Education

FROM: Eric G. Mackey
State Superintendent of Education

RE: Cybersecurity Measures for Local Education Agencies (LEAs)

Cybersecurity measures are necessary to protect school systems from escalating threats of ransomware, data theft, and financial crimes. These measures are crucial to prevent interruptions to school operations, permanent loss of personal data, theft of funds, and the expensive, unbudgeted recovery costs associated with such incidents. To help safeguard each school system against these damaging crimes, it is imperative that each LEA complies with the following requirements:

1. Cyber Awareness Training
2. Cybersecurity Incident Response Plan Development
3. Multi-Factor Authentication (MFA)

First, because phishing emails continue to be a leading point of entry for ransomware and other forms of cybercrime, it is essential that all employees are informed and trained to recognize and appropriately respond to phishing emails. To facilitate cyber awareness training, each LEA will use the cybersecurity awareness software provided to them by the state to complete the following:

1. Require a minimum of one training per year for all employees* with district email

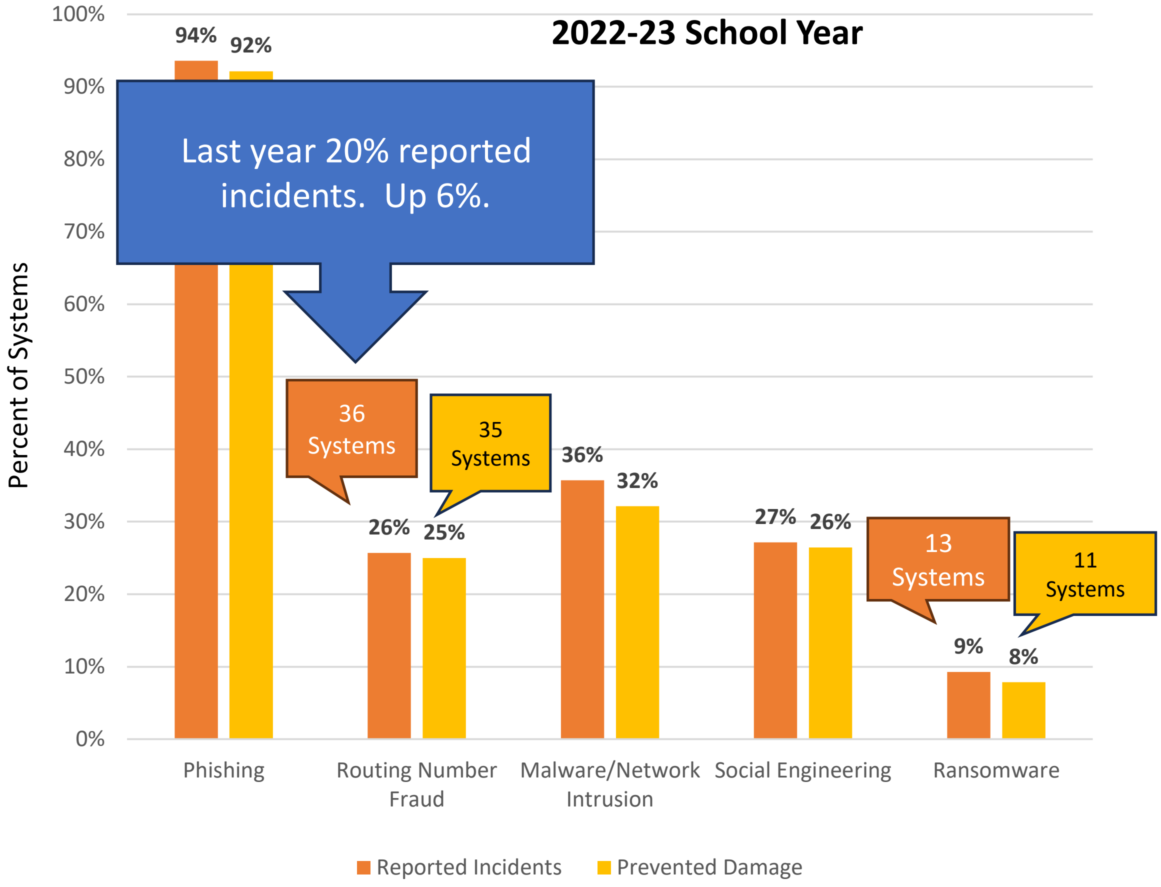
The High Cost of Cyber Attacks

2022-23 Academic Year

- At least 8 districts nationwide significantly impacted. Resulting in -
- Stolen financial information
- Compromised security system information
- Monetary losses ranging from $50,000 to $1 million

Alabama Incidents

140 of 152 Systems Submitted Data

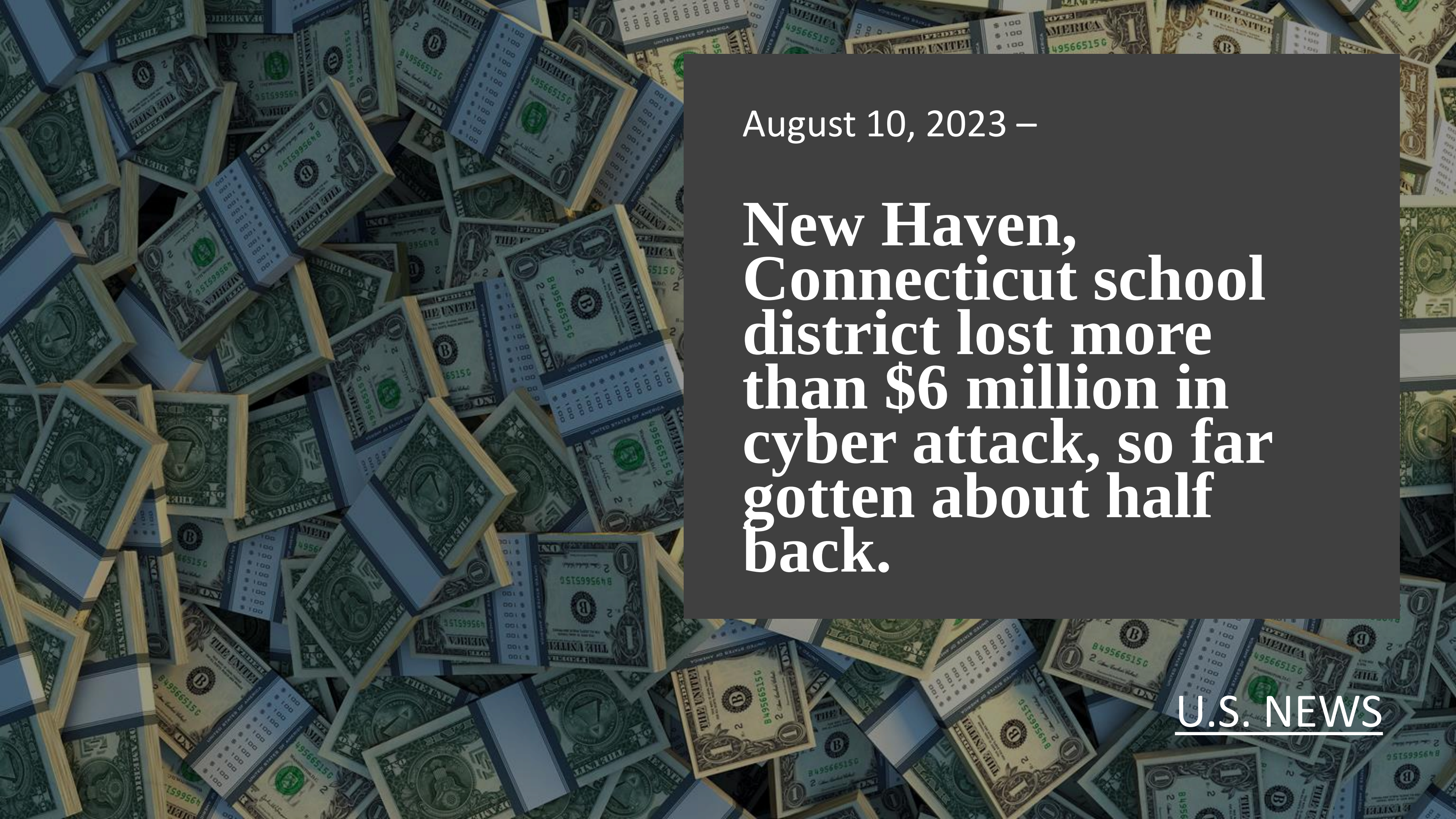


Last year 20% reported incidents. Up 6%.

Why Accounting Should Care?

You have access to–

- Money
- Routing numbers
- Employee data
- Social security numbers



August 10, 2023 –

New Haven, Connecticut school district lost more than $6 million in cyber attack, so far gotten about half back.

U.S. NEWS

Theft came to light only after a school bus company asked why it hadn't yet been paid.

. . . thieves gained access to the COO's public school email address in May, monitored online conversations with vendors and eventually inserted themselves into the conversations by impersonating the COO and the vendors.

The thieves then made requests for electronic transfers to fraudulent accounts.

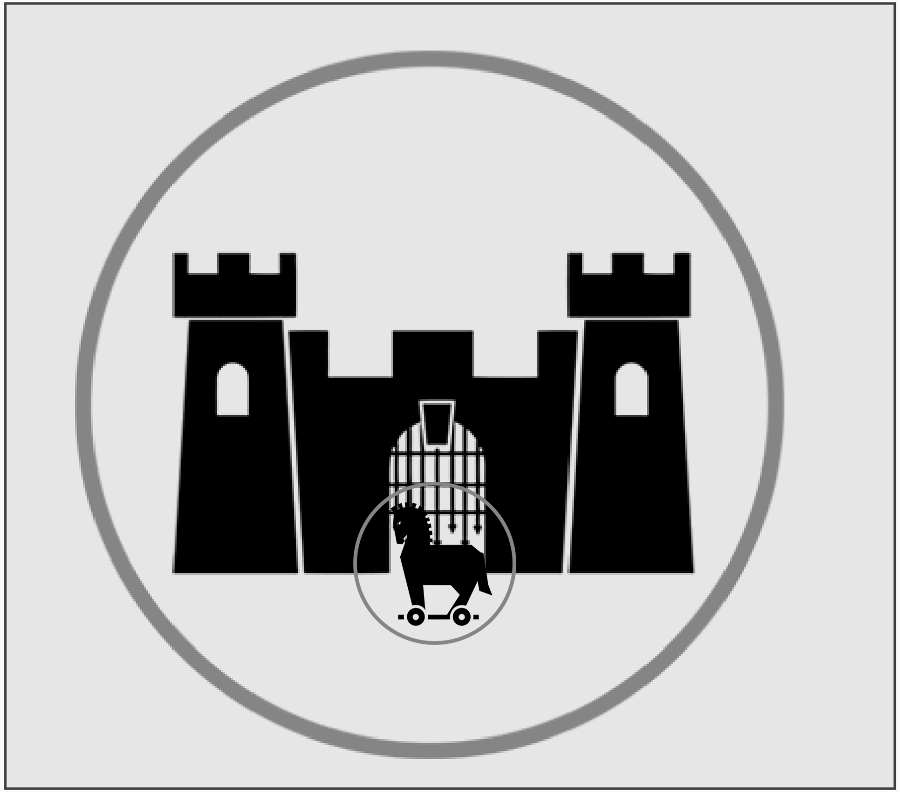
Internal Controls

Why Internal Controls are Needed

Perimeter defenses cannot stop all threats.

Sometimes the threat comes from the 'inside'.

Often it is a Combination of the Two



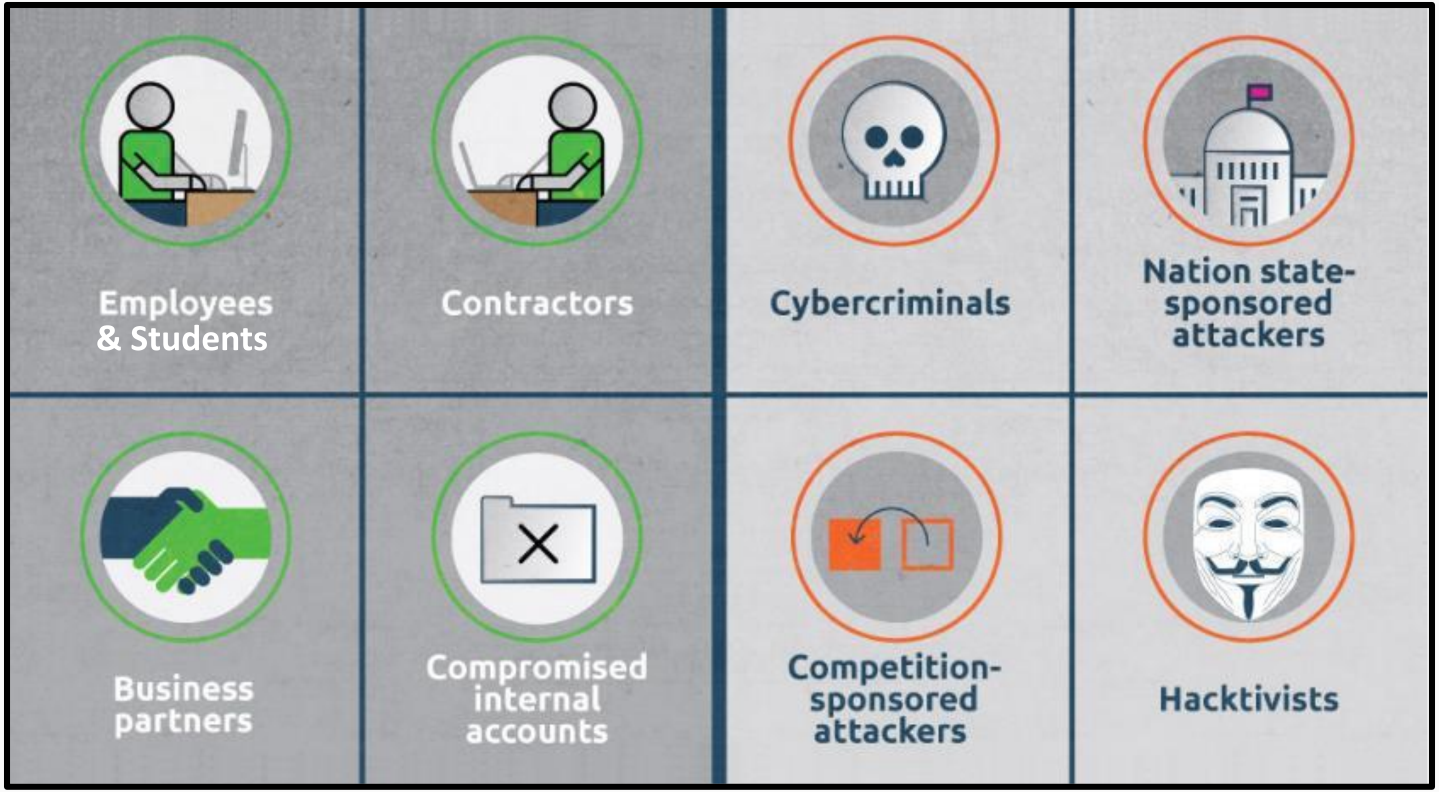
1. Phishing email enters the system by-passing the firewall, content filter, and spam filter

2. A link prompts the employee to change their password

3. Now the ‘hacker’ has access to that account and all actions are recorded as if it was the employee’s actions

Insider Threats

Outsider Threats


Employees & Students
Contractors
Cybercriminals
Nation state-sponsored attackers
Business partners
Compromised internal accounts
Competition-sponsored attackers
Hacktivists

Insider Risk
vs.
Insider Threats

Insider **Risk**

Insider Risk occurs when any ***data exposure***, regardless of perceived data value or user intent, ***jeopardizes*** the well-being of an organization and its employees, customers or partners.

https://www.code42.com/glossary/what-is-insider-risk/

Examples

- Publishing email addresses of accounting staff on websites
- Online check registers can reveal what software, services, and vendors you use

https://www.code42.com/glossary/what-is-insider-risk/

Website Contact Information

Jane Doe
Director of Payroll

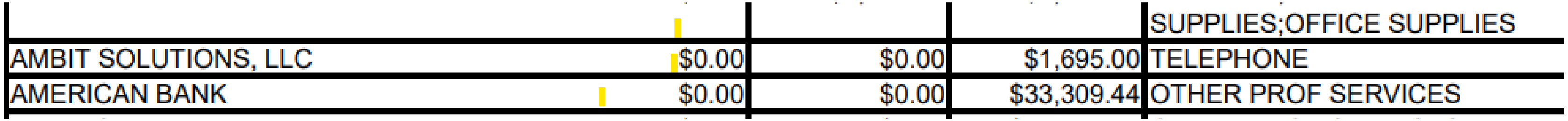
Email Jane Doe

John Smith
Chief School Financial Officer

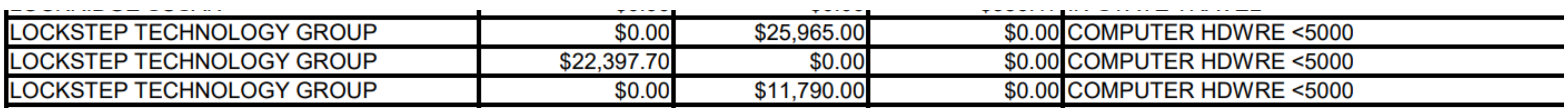
Email John Smith

If clicking these links opens up an email with the To: address filled in, you are not disguising anything. You are giving bad actors an invite.

Check Register Examples

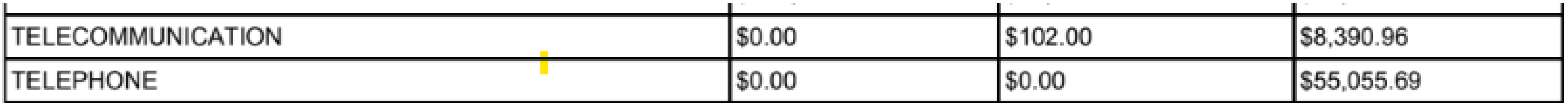


				SUPPLIES;OFFICE SUPPLIES
AMBIT SOLUTIONS, LLC	$0.00	$0.00	$1,695.00	TELEPHONE
AMERICAN BANK	$0.00	$0.00	$33,309.44	OTHER PROF SERVICES

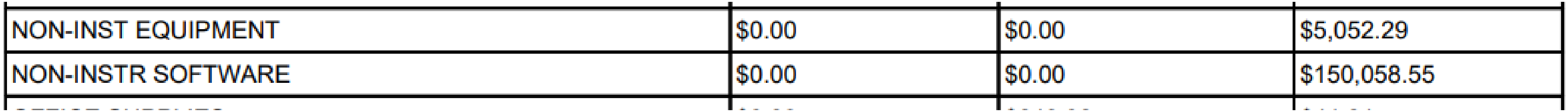


LOCKSTEP TECHNOLOGY GROUP	$0.00	$25,965.00	$0.00	COMPUTER HDWRE <5000
LOCKSTEP TECHNOLOGY GROUP	$22,397.70	$0.00	$0.00	COMPUTER HDWRE <5000
LOCKSTEP TECHNOLOGY GROUP	$0.00	$11,790.00	$0.00	COMPUTER HDWRE <5000

Vs.



TELECOMMUNICATION	$0.00	$102.00	$8,390.96
TELEPHONE	$0.00	$0.00	$55,055.69



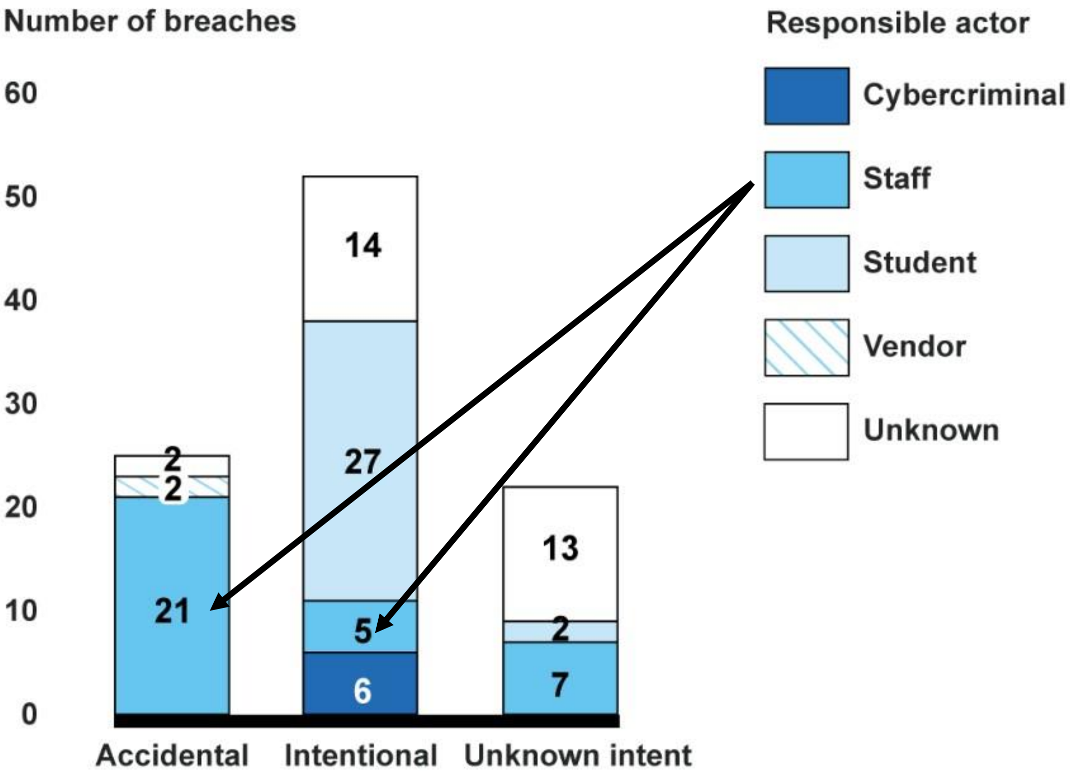
NON-INST EQUIPMENT	$0.00	$0.00	$5,052.29
NON-INSTR SOFTWARE	$0.00	$0.00	$150,058.55

Insider **Threat**

The potential for an individual who has or had authorized access to an organization’s assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

99 Student Data Breaches Nationwide

2016-2020



Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

https://www.gao.gov/products/gao-20-644

Insider **Threat**

- Can arise from anyone with authorized access to a company’s underlying network and applications, such as employees, partners, vendors, interns, suppliers or contractors.

- Not all insider threats are necessarily malicious. Some occur due to –
  - Human error
  - Trying to work more efficiently
  - Unfamiliarity with applications or technology
  - Ignoring or being unfamiliar with rules and procedures

Types of Insiders

- Accidental insiders
- Negligent insiders
- Compromised insiders
- Malicious insiders
- Recruited insiders

Factors that can Increase Insider Threat

- Disengaged employees
- Employee burnout
- ‘Quiet quitting’
- Lack of training
- Security not emphasized as a responsibility of the job

Departing Employee

- May take data with them as examples of their work
- May take or expose data if disgruntled
- Likely to send or take data in the 90 days prior to giving notice

https://www.code42.com/blog/what-is-an-insider-threat/

Terminations & Administrative Leave

Technology Director should be notified of terminations and administrative leave decisions and dates.

The digital accounts and access for these individuals should be locked immediately upon these actions taking effect.

Internal Controls

Preventative Controls

Measures to deter errors or fraud from happening in the first place and include thorough documentation and authorization practices.

Detective Controls

Procedures that are designed to catch items or events that have been missed by the first line of defense.

Preventative Controls

- Require employee training in cybersecurity
- Perform phishing tests monthly
- Ensure proper training on software applications
- Ensure employees know where they can and cannot download or store data

It is not unusual for accounting and payroll staff to get dozens of social engineering or phishing emails per month.

Password Changes & Access to NextGen

- Set and require password standards and refresh requirements for both email and NextGen

- Require the use of non-privileged accounts when not performing higher level tasks

Multi-Factor Authentication

- Prevents a bad actor from logging into your system using your user id and password
- Should be implemented for anyone whose account has rights to:
  - Enter or change routing numbers
  - View social security numbers
  - Prepare W-2 forms
  - Create other NextGen users or change the permissions of other NextGen users

Multi-Factor Authentication

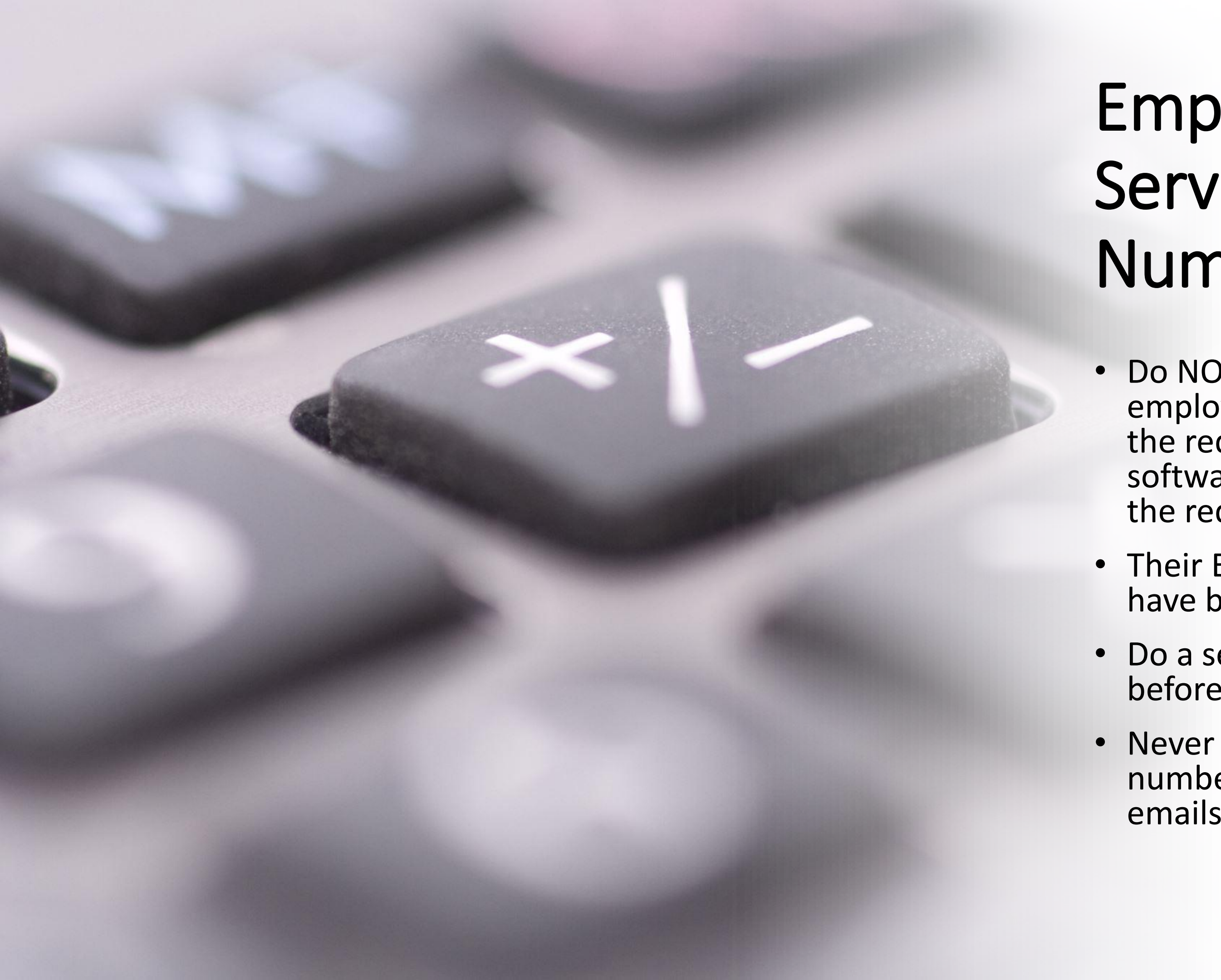
- Does not necessarily require the person to use their personal cell phone to get the code
- Cloud-hosted NextGen – has MFA option
- Locally-hosted NextGen – various options such as Cisco Duo can be implemented

Routing Number Change Controls

- NEVER change routing numbers without using a method for getting a second confirmation from a **KNOWN*** requestor.**
- If **UNKNOWN**, then get secondary verification that the request is legitimate from a KNOWN person.
- Have a second member of the accounting dept. review the request before making the change.

*Someone telling you who they are doesn't mean that's who they are.

**Keep in mind that the vendor may also have their own Insider Threats.



Employee Self-Service & Routing Numbers

- Do NOT assume that because the employee had to log in to submit the request (either to the ESS software or their email account) the request is really from them.
- Their ESS id and password could have been compromised.
- Do a secondary check yourself before approving any change.
- Never change employee routing numbers based on phone calls or emails alone.

Preventative Internal Controls

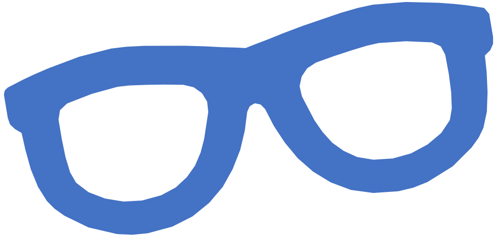
- Discuss security at departmental meetings.
- Establish step-by-step procedures for highly sensitive.

Detective Controls

Use reports of who was logged into NextGen and when to identify any unusual activity.

If unusual activity is spotted it could mean an Insider Threat or it could mean an employee’s NextGen account has been compromised.

Keeping an Eye on Things



Review monthly reports on which staff are failing phishing tests. These are people can pose an Insider Threat. Discuss this with them and/or assign additional training.

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.

Ransomware

Accounting Servers are Likely Targets

Encrypting the system will motivate you to pay the ransom

Contains data cybercriminals want

You Will Need Back Ups

- Ransomware will often seek out backups first to prevent you from recovering.
- Locally-hosted – Should have more than 1 backup and should be air-gapped from the network.
- Cloud-hosted – NextGen provides backups. Be sure you know exactly what they have and will do in the event you need to recover.

You Will Need a Plan

- The system Incident Response Plan should include actions you and your staff will take and a list of potential resources you may need in the event of an incident.
- Depending on what time of month the ransomware hits, you may need alternate equipment to run payroll or complete other time-sensitive tasks.

Routing Number Fraud Reporting

- FBI investigates cybercrimes but does not help you to recover from it.
- **Secret Service deals with financial crimes. They investigate and may be able to help recover stolen funds.**
  - *Our goal is to protect the nation's financial infrastructure and maintain a safe environment for the American people to conduct financial transactions. Our mission is to investigate complex cyber-enabled financial crimes.*
  - https://www.secretservice.gov/investigation/cyber
  - Report routing number fraud to Secret Service ASAP
  - Birmingham field office – 205-731-1144

Incident Response Plan Workshops

- SDE and ALET will be conducting IRP beginning in November.
- Workshops will be hosted at Regional Inservice Centers and other locations throughout the state.
- SDE will issue a memo about the dates and locations.

What Can You Do to Prevent Cybercrime?

1

Train your staff and implement Internal Controls.

2

Have secure backups and accounting procedures in the System Incident Response Plan procedures.

3

Don’t think it can’t happen to you. It can. Act like it.

One of the best controls you and your staff can have is self-control.

Thank You

ALET

ALABAMA
LEADERS in
EDUCATIONAL
TECHNOLOGY