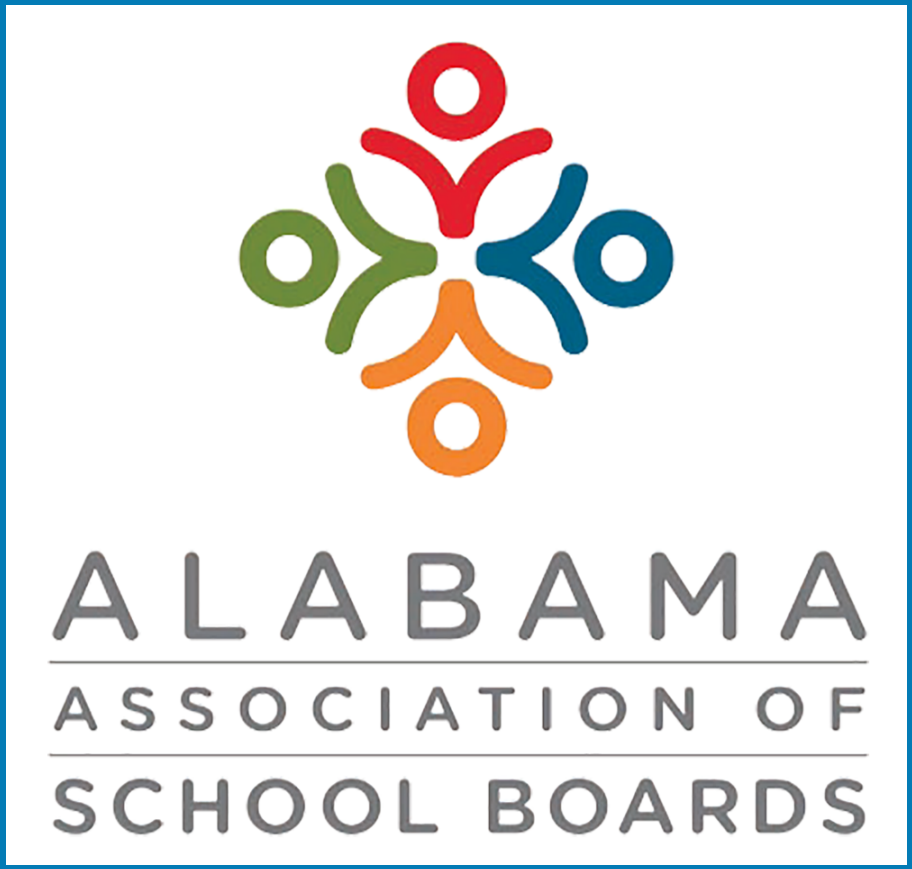


2019 Leadership for Financial Accountability

Data Breach and Cyber Security Threats

Dr. W. Greg Price – Troy University
Pike County Board of Education

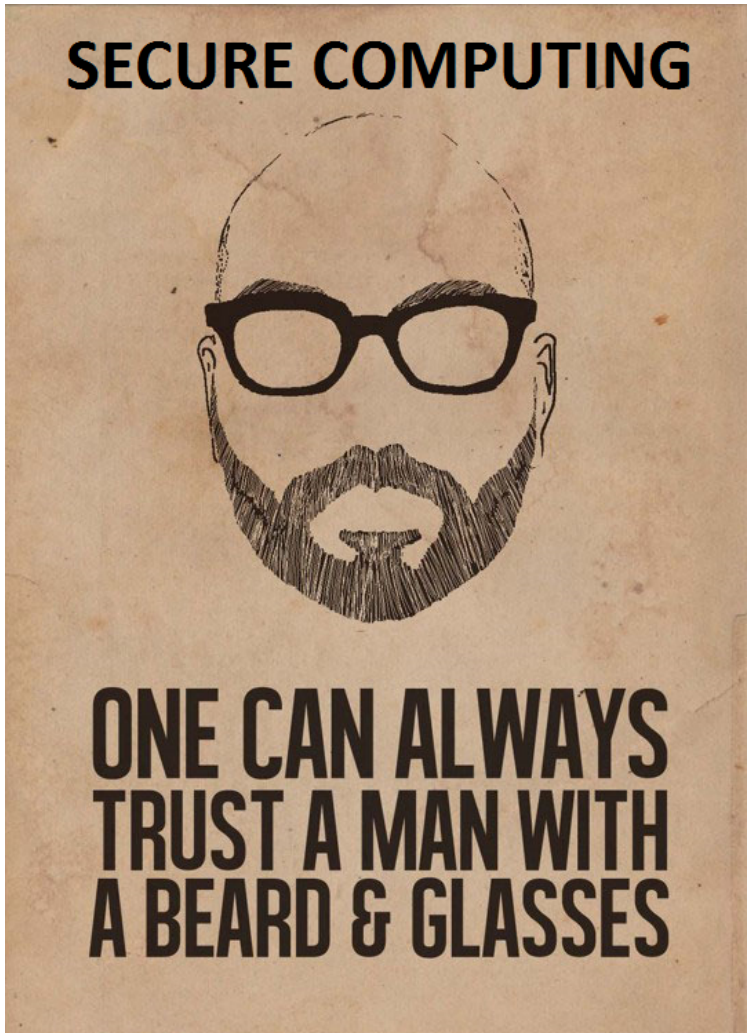
Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

Agenda

- A brief history of Cybersecurity
  - How prevalent is the issue?
  - What trends have emerged?
- Cyber Risk – prompting action and review
  - What is Cyber Risk, how is it quantified?
  - What are common examples?
- Principles of Effective Cybersecurity - overview
- Q&A

Principles of Effective Cybersecurity



Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

A brief history of Cybersecurity

- 1989 – Robert Morris developed first worm and DoS attack resulted, spawning the groundwork for modern day cybersecurity
- Viruses – 1990s, Melissa and ILOVEYOU wreak havoc on email systems globally
- Credit Card theft – 2000s, directed attacks for financial gain, TJX theft, $256 million loss
- Modern day – highly individualized, through indirect means, specifically designed to elude observation and preventive measures - Target

Principles of Effective Cybersecurity

During the last one minute…

45 new viruses emerged

200 new malicious websites launched

180 identities stolen

5,000 variants of malware released

$2,000,000 lost

New social media influencer emerged

Principles of Effective Cybersecurity

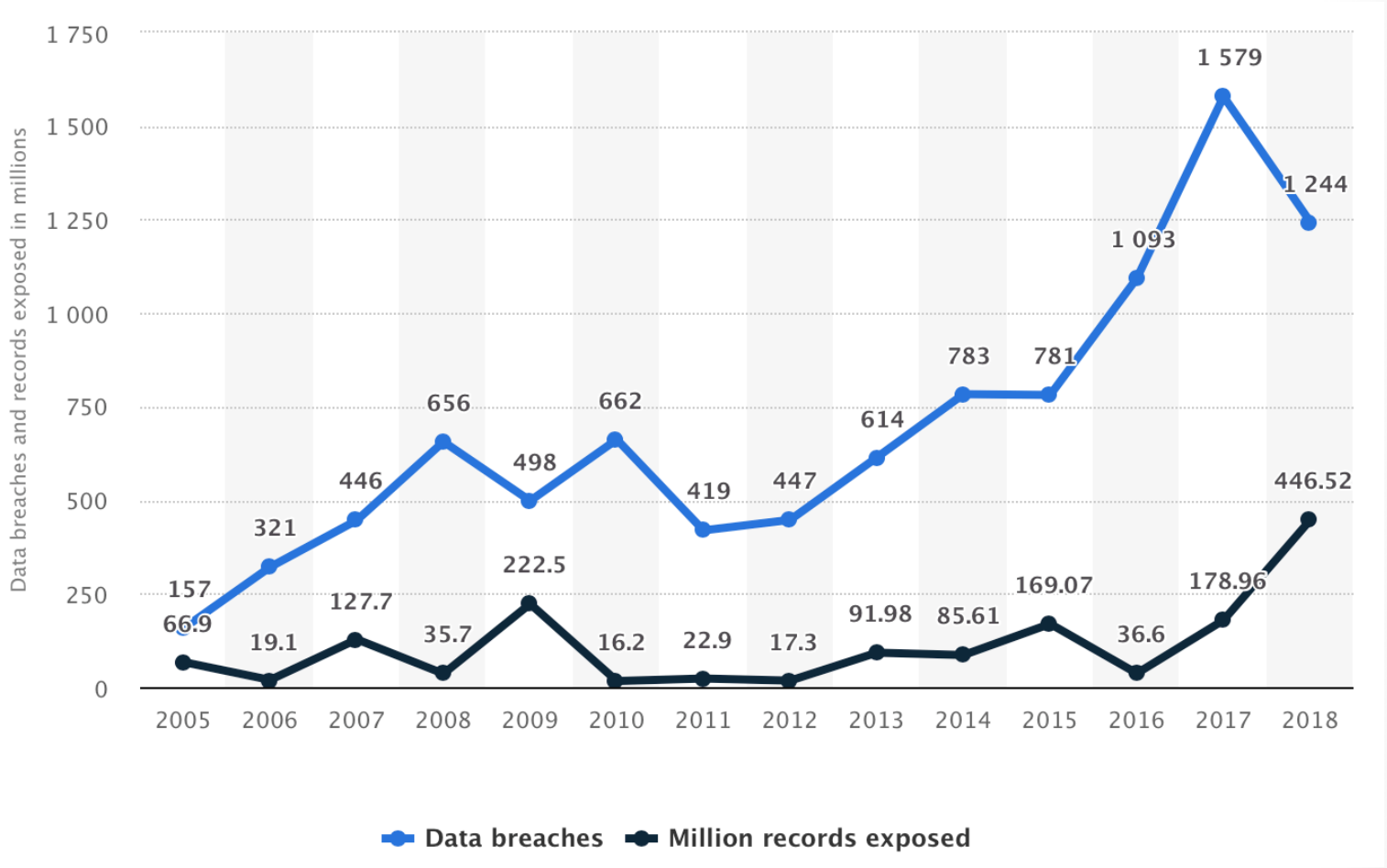
ALABAMA ASSOCIATION OF SCHOOL BOARDS

Prevalence of Cyber Security Issues

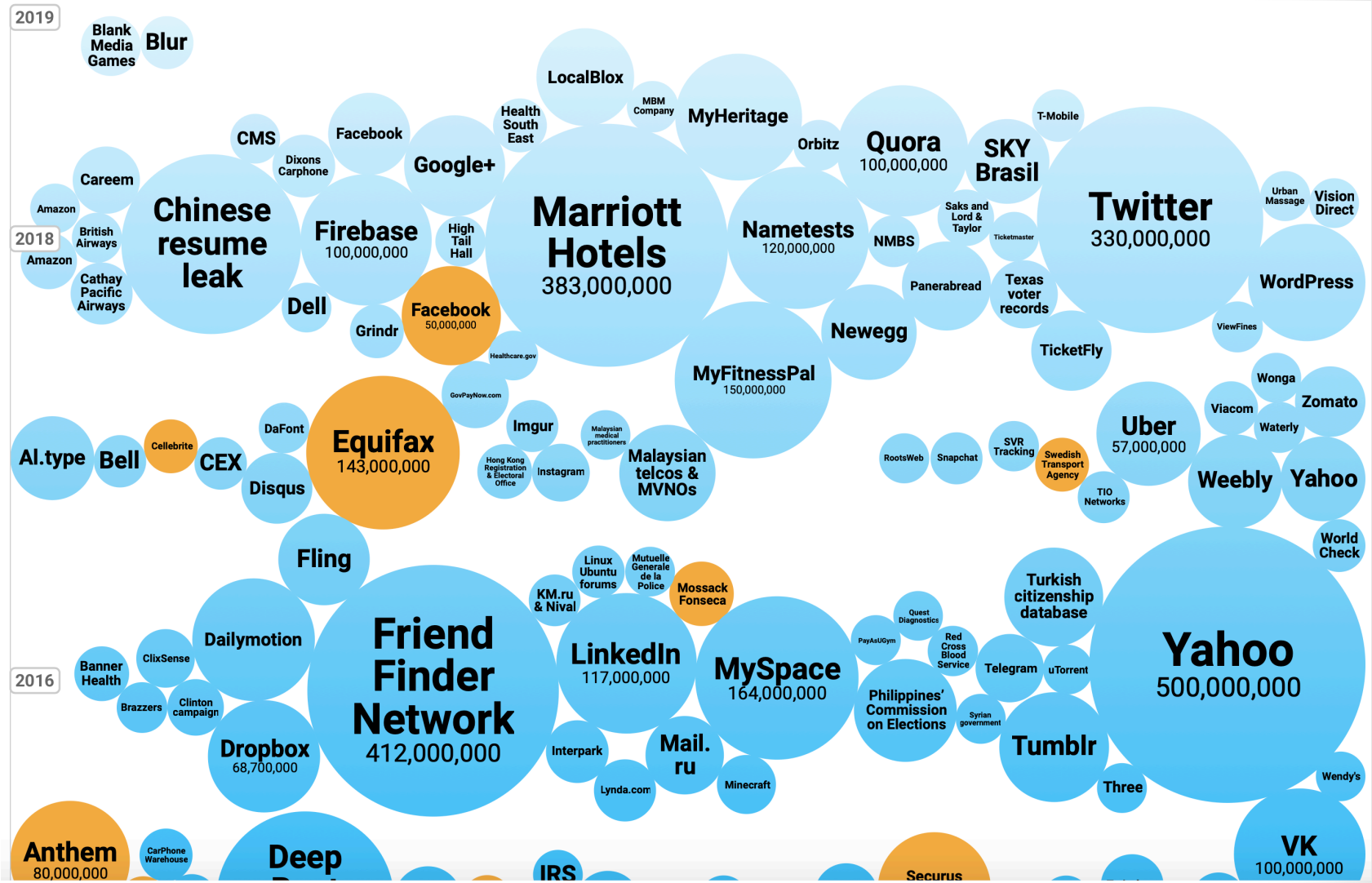
- 2018 – Almost 54,000 documented incidents and 2,200+ confirmed data breaches
- Ten vulnerabilities accounted for 97% of all documented exploits
- The remaining 3% consist of over 7,000,000 different vulnerabilities, some dating to 1999
- Average cost per stolen record: $213.00
- Since 2005, 10,500+ data breaches have been announced
- Average breach time is less than two minutes
- 23% response to Phishing attempts

Principles of Effective Cybersecurity

Annual number of data breaches and exposed records in the US



Principles of Effective Cybersecurity

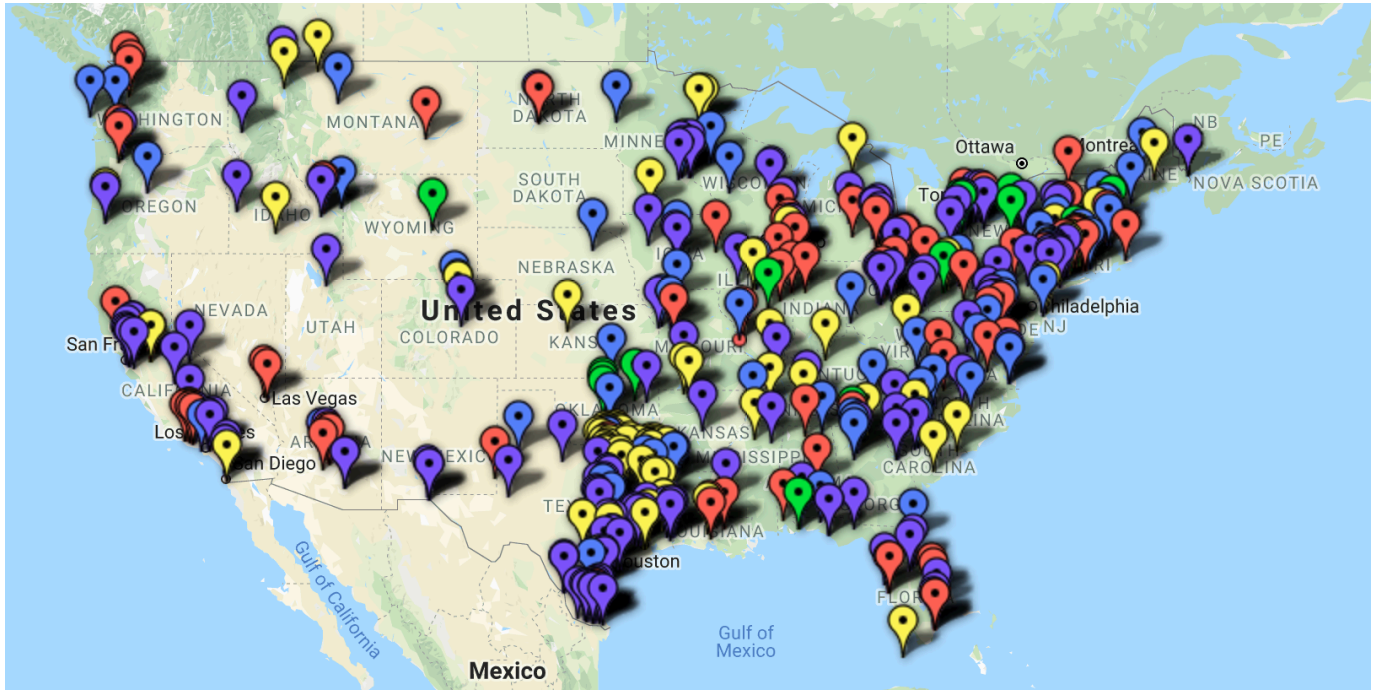


Principles of Effective Cybersecurity

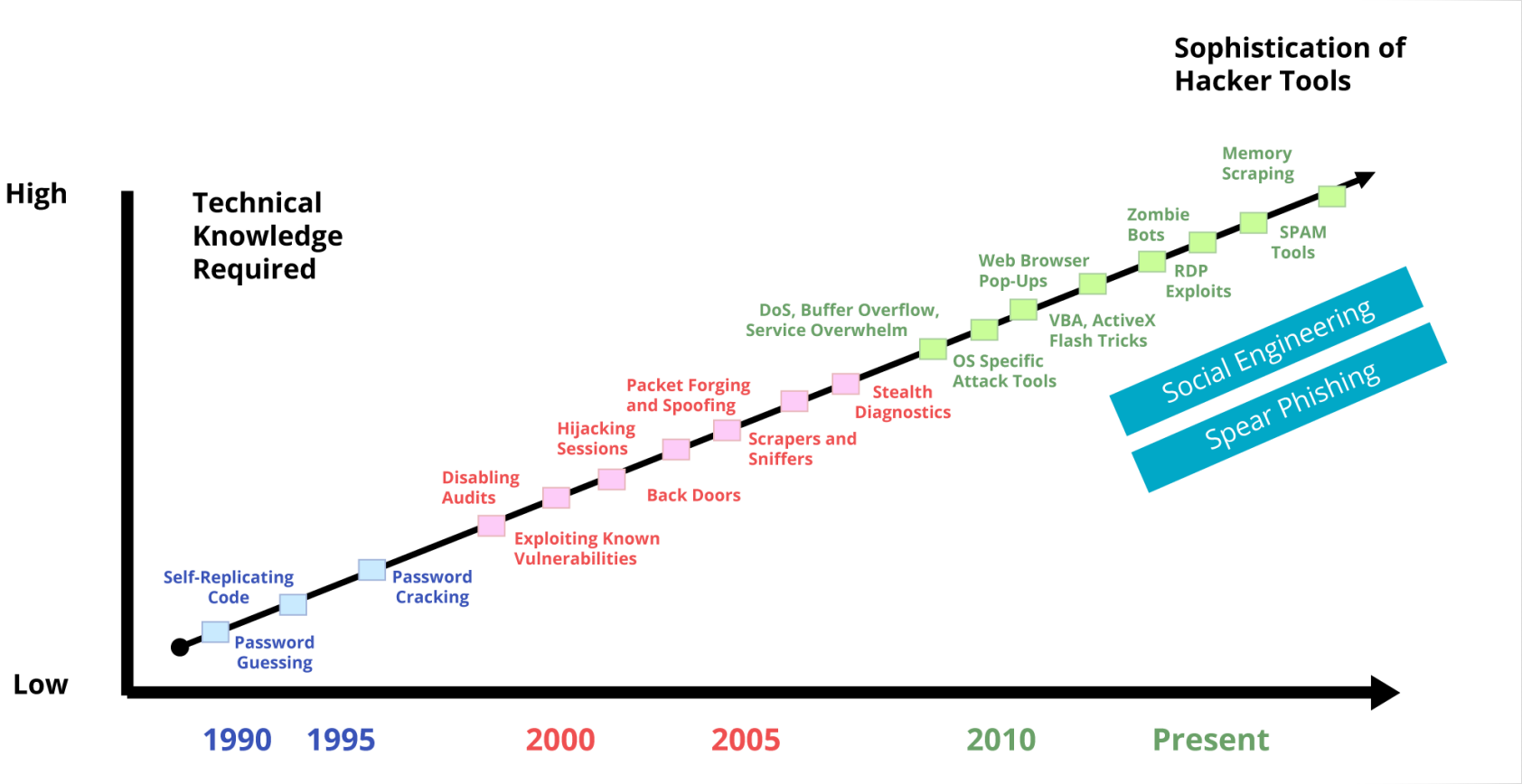
ALABAMA ASSOCIATION OF SCHOOL BOARDS

The K-12 Cyber Incident Map

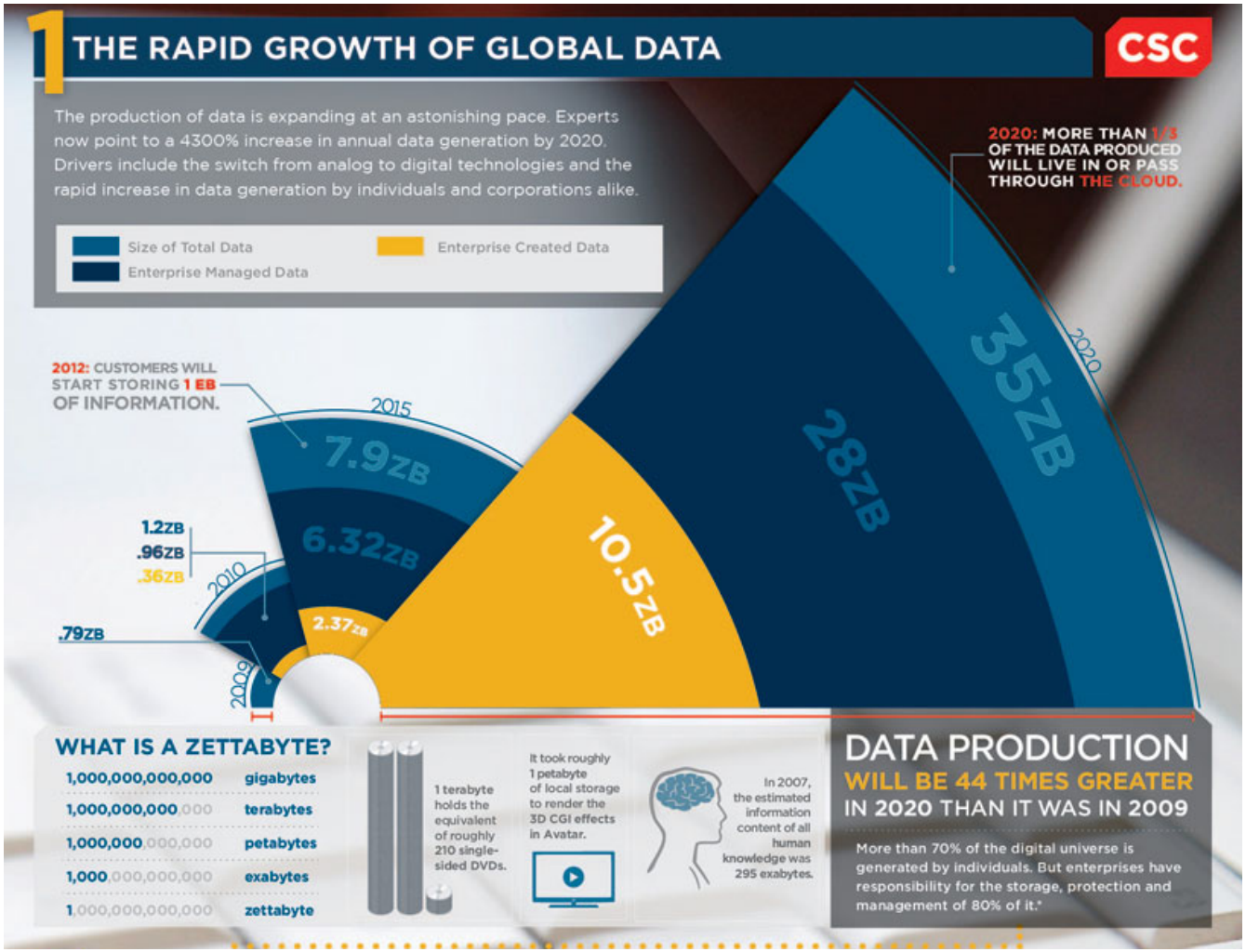
425 Incidents Since January 2016



Principles of Effective Cybersecurity



Principles of Effective Cybersecurity



Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

Cybersecurity Trends

- Specificity of targets have increased since 2005
  - Casting a wider net, with a directed approach
- Users continue to be a major source of problems
  - 73% of successful attacks are attributed to user problems
    - 42% of successful attacks result from misconfigured systems
    - 31% of successful attacks result from end-user error
- Poor security awareness and IT product management
  - 99.9% of the exploited vulnerabilities in 2018 had associated patches that were over 1 year old
  - Awareness campaigns are often poorly designed and lack “teeth”
- 96% of mobile malware targets Android devices

Principles of Effective Cybersecurity

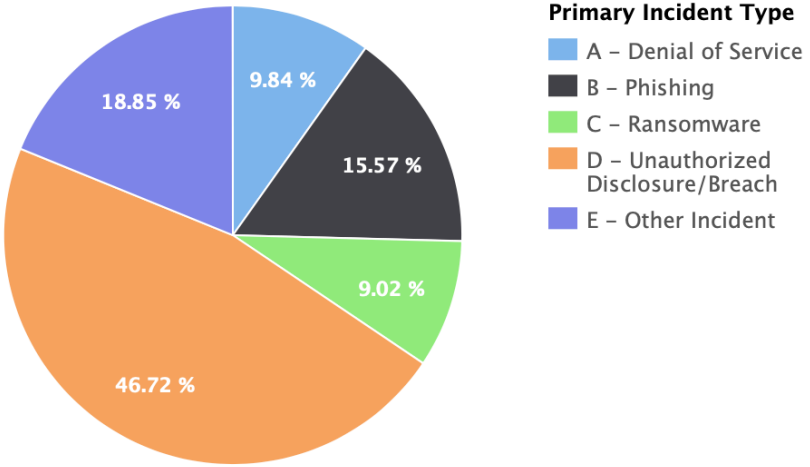
ALABAMA ASSOCIATION OF SCHOOL BOARDS

The most frequently experienced type of K-12 cyber incident reported during 2018 were data breaches, primarily meeting one of the following four profiles:

- Unauthorized disclosures of data by current and former K-12 staff, primarily—but not exclusively—due to human error;
- Unauthorized disclosures of K-12 data held by vendors/partners with a relationship to a school district;
- Unauthorized access to data by K-12 students, often out of curiosity or a desire to modify school records (including grades, attendance records, or financial account balances); or,
- Unauthorized access to data by unknown external actors, often for malicious purposes.

K-12 Cyber Incidents: 2018

Note: Publicly-disclosed incident reports represent a subset of actual incidents experienced by schools and districts. Public reports may also be inaccurate or ambiguous.



Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

Cybersecurity Trends – Small businesses – Education?

Small businesses experience most of the data breach incidents because they:

- Are less aware of their exposures
- Have fewer resources to provide appropriate data protection and/or security awareness training for employees
- Are less likely to have strong cyber risk management controls in place
- Typically do not have a dedicated risk management professional
- Serve as a training ground for cyber thieves who are honing their skills to prepare for bigger attacks
- Are less likely to discover data breach

Forms of data breach your business can potentially be exposed to:

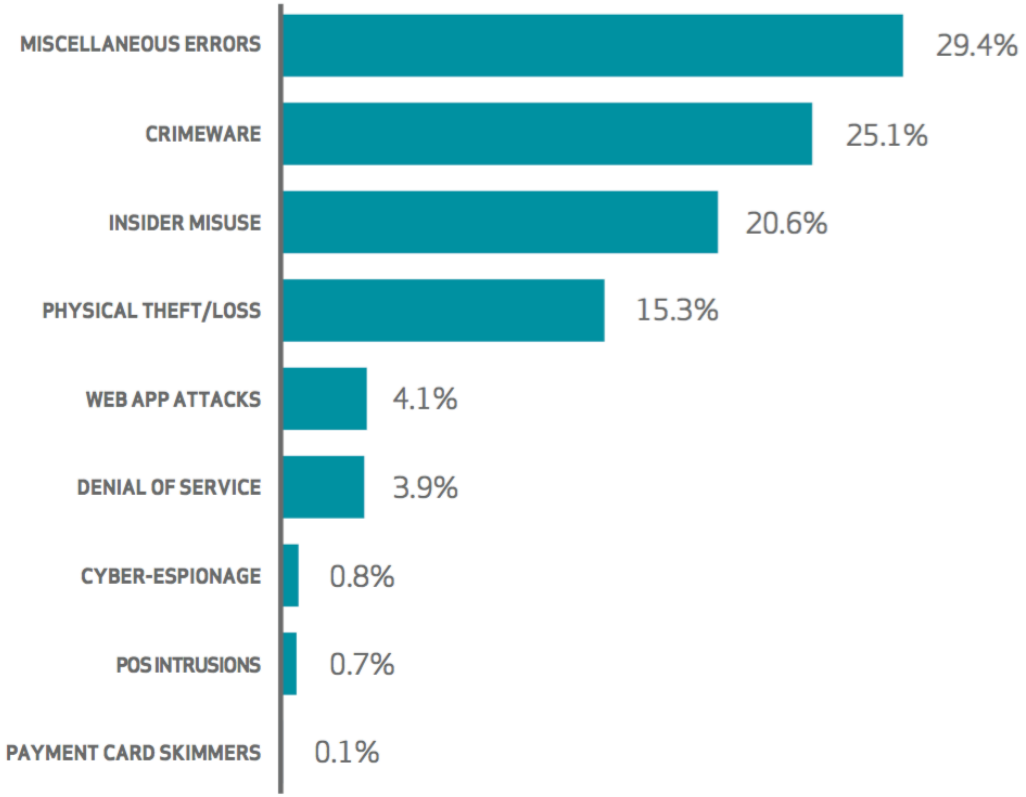
- Hacking
- Theft or release of funds due to unauthorized access (such as by former employees or vendors)
- Stolen or lost paper and electronic files
- Stolen or lost laptop, smartphone, tablet or computer disks
- Stolen credit card information
- Employee error or oversight

Small businesses and educational entities are similar

Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

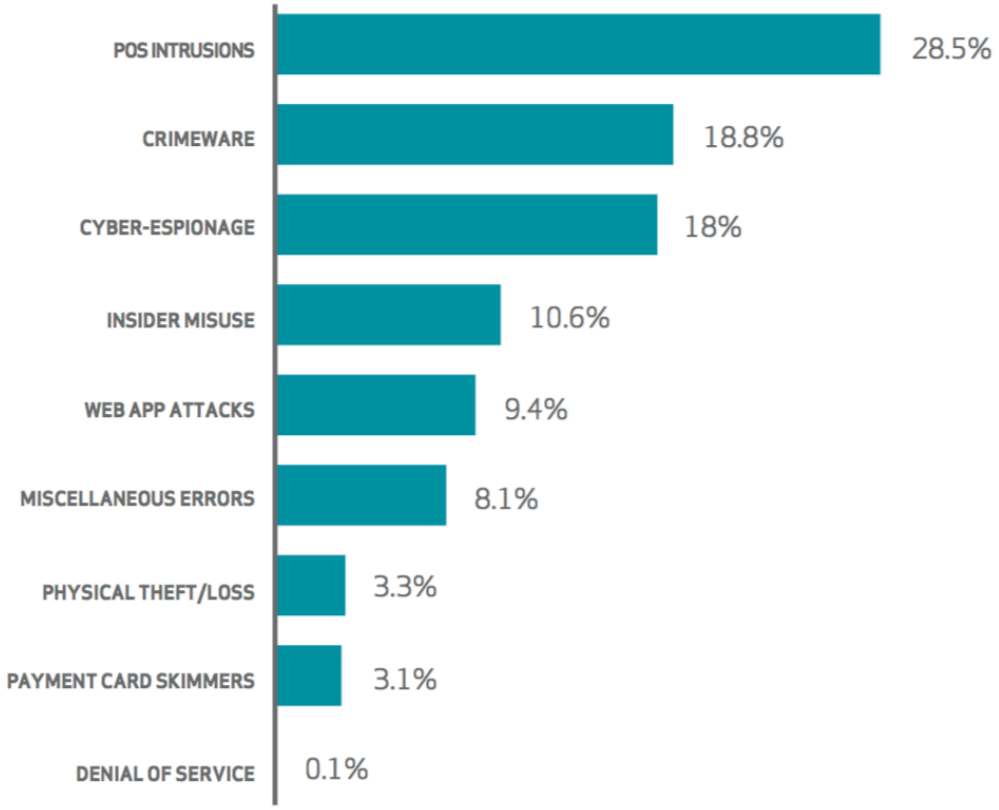
"We are the problem", repeat, "We are the problem"



Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

"We are the problem", repeat, "We are the problem"



Principles of Effective Cybersecurity

Cyber Risk

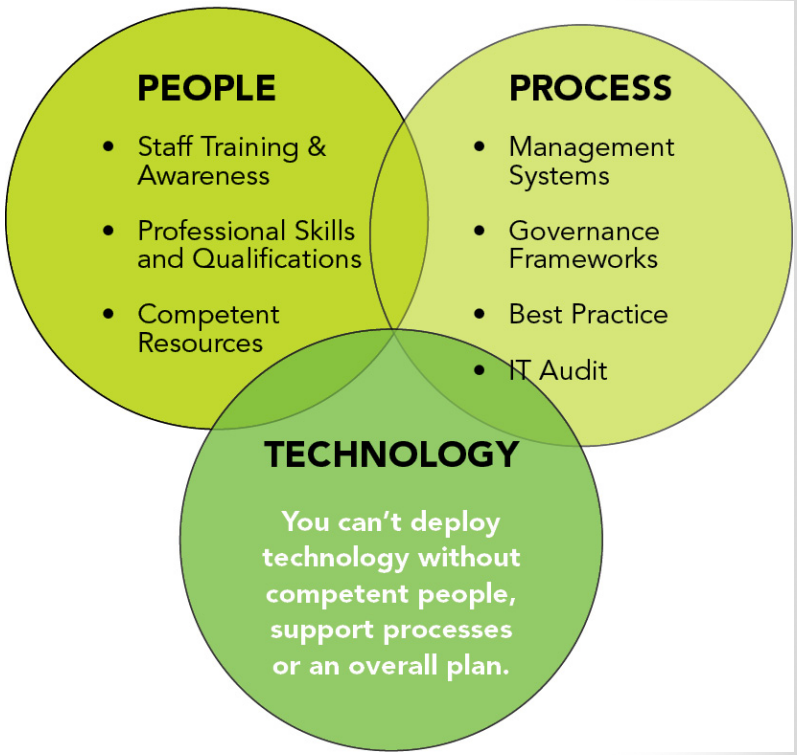
- Any risk of financial loss, disruption or damage to the reputation of an organization from some manner of failure in its information technology systems

Principles of Effective Cybersecurity

Cyber Risk

- Quantifying Exposure – How?

For cyber resilience assurance to be effective, a concerted effort among ecosystem participants is required to develop and validate a shared, standardized cyber threat quantification framework.
In other words,
Security is Everyone's Job.



Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

Cyber Risk

- Quantifying Exposure – How?
  - Understand the key cyber risk drivers (or components) required for modeling cyber risks
  - Understand the dependences between these components that can be embedded in a quantification model
  - Understand ways to incorporate cyber risk quantification into enterprise risk management
    - The key components identified in the cyber value-at-risk model concept follow:
      - Existing vulnerabilities and defense maturity of an organization
      - Value of the assets
      - Profile of an attacker

Principles of Effective Cybersecurity

Cyber Risk

- Quantifying Exposure – Wow!?!

Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

Cyber Risk

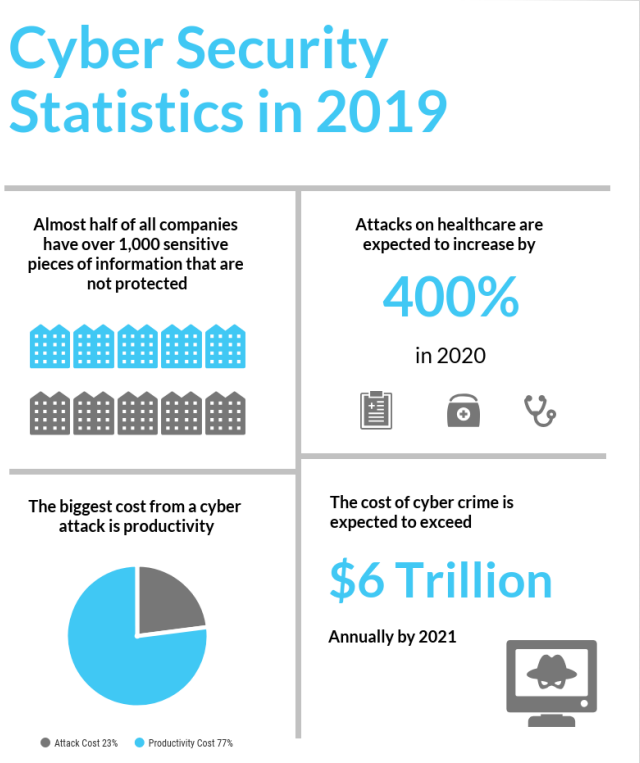
- Common Examples
  - Identity theft as a result of security breaches where sensitive information is stolen
  - Business interruption from a hacker shutting down a network
  - Damage to reputation
  - Costs associated with damage to data records caused by a hacker
  - Theft of valuable digital assets
  - Introduction of malware, worms and other malicious computer code
  - Human error leading to inadvertent disclosure of sensitive information
  - The cost of credit monitoring services
  - Lawsuits alleging trademark or copyright infringement

Principles of Effective Cybersecurity

Myth #1

It won’t happen to us!

- Common misconception
- Small doesn't mean overlooked
- We don't store anything significant
- All of our stuff is stored in "the cloud"
- My wife's cousin's son is really smart

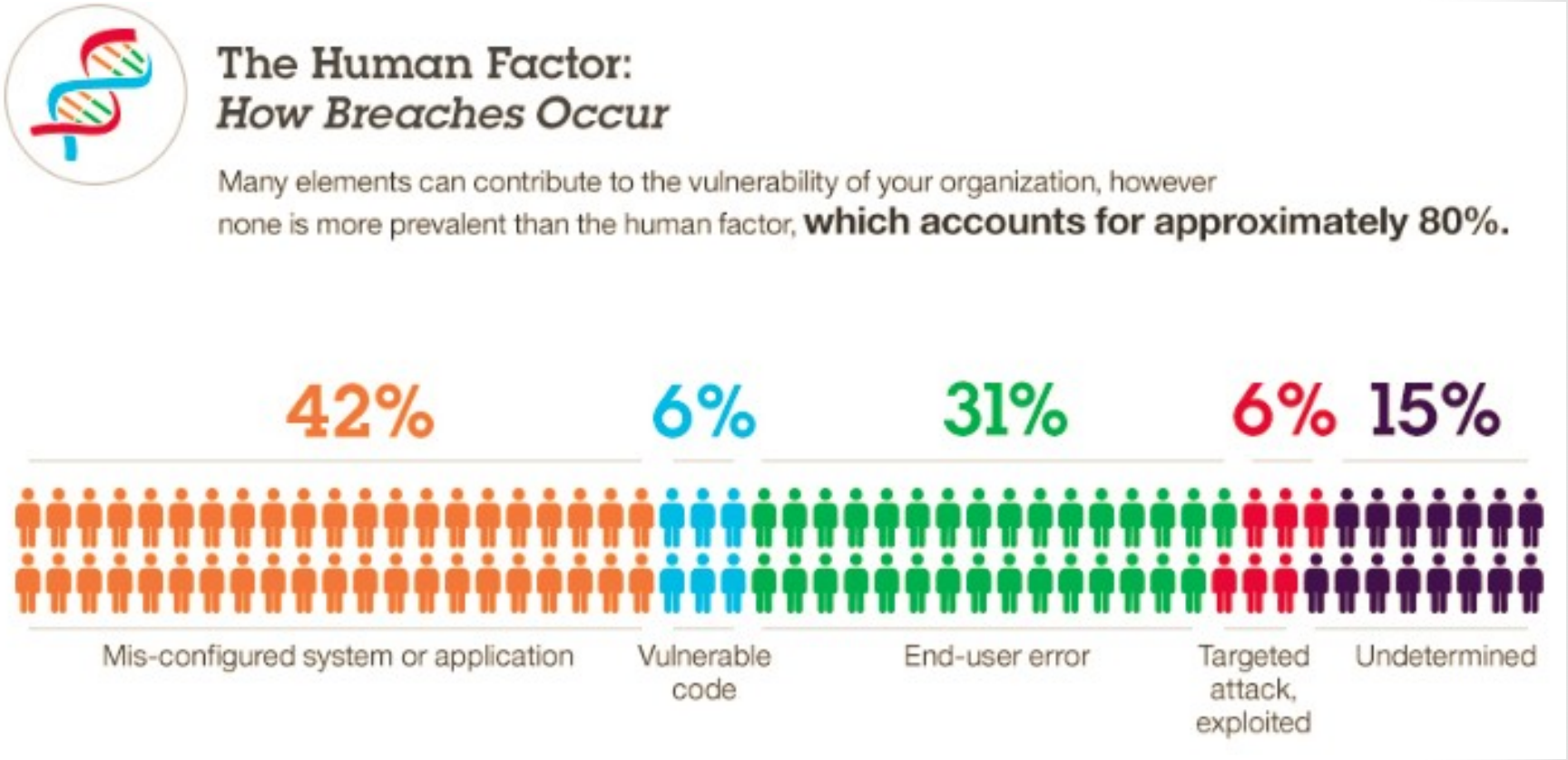


Small businesses suffer the majority of attacks - However, educational entities are a prime target

Principles of Effective Cybersecurity

Myth #1

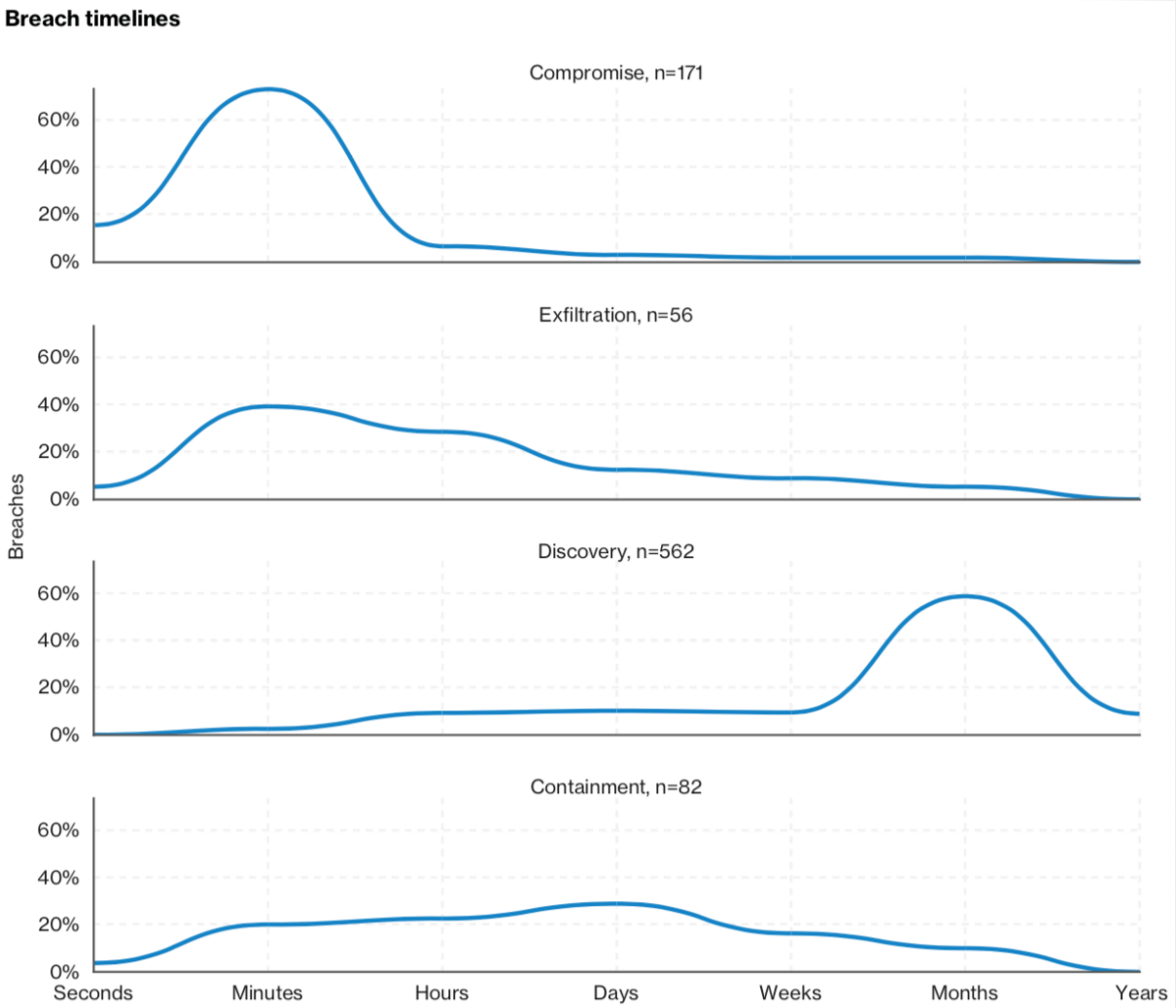
- We humans…



Principles of Effective Cybersecurity

Myth #1

- For how long?



Principles of Effective Cybersecurity

Myth #1

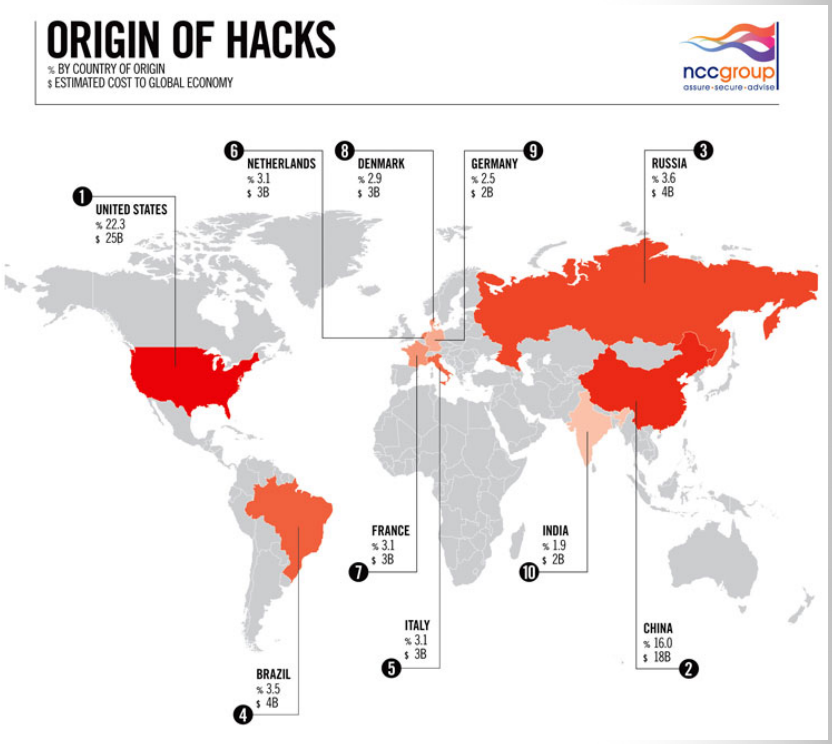
- Inconvenient truths…

Principles of Effective Cybersecurity

Myth #2

Attackers are geniuses from over there.

- Common misconception
- Media fuels misinformation
- The government is protecting us
- My vendor is protecting us
- We have great legal counsel

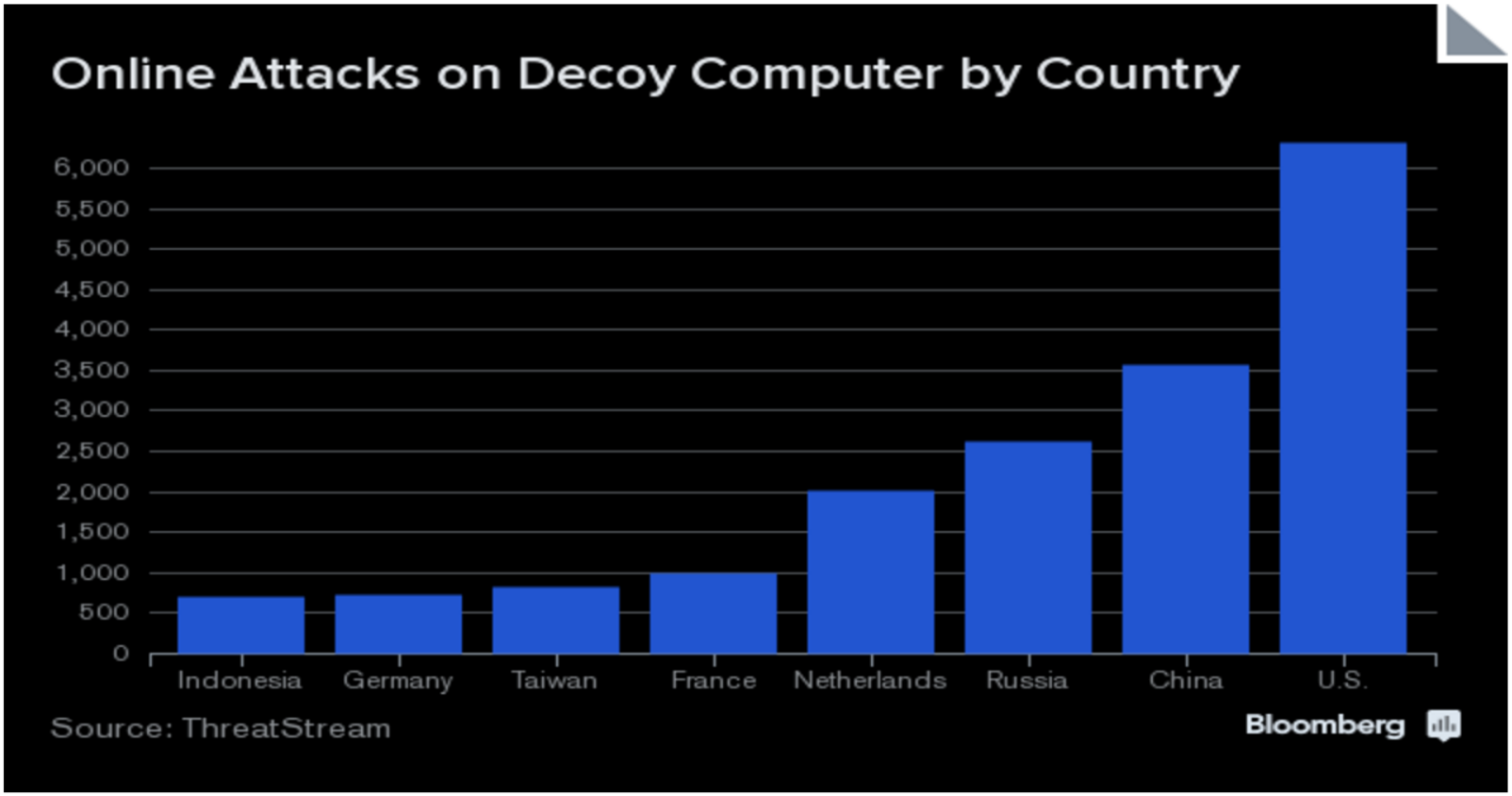


Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

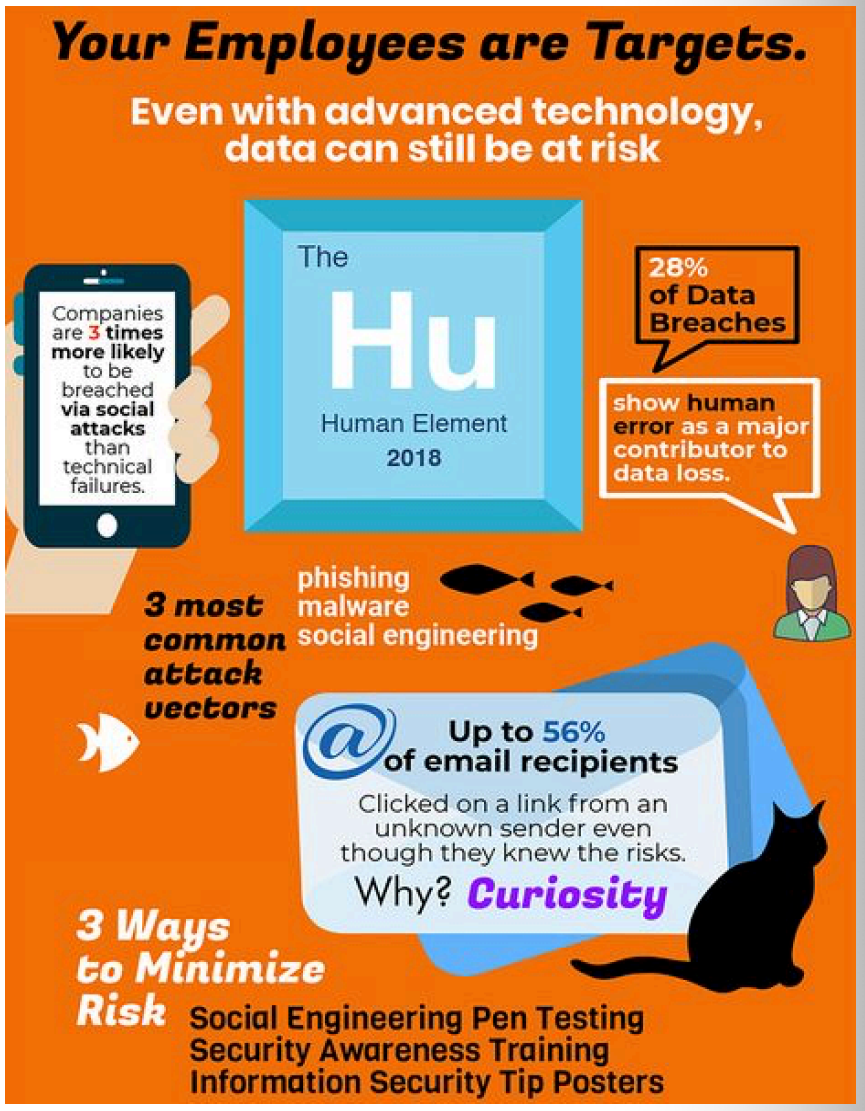
Myth #2

Attackers are geniuses from over there.



Principles of Effective Cybersecurity

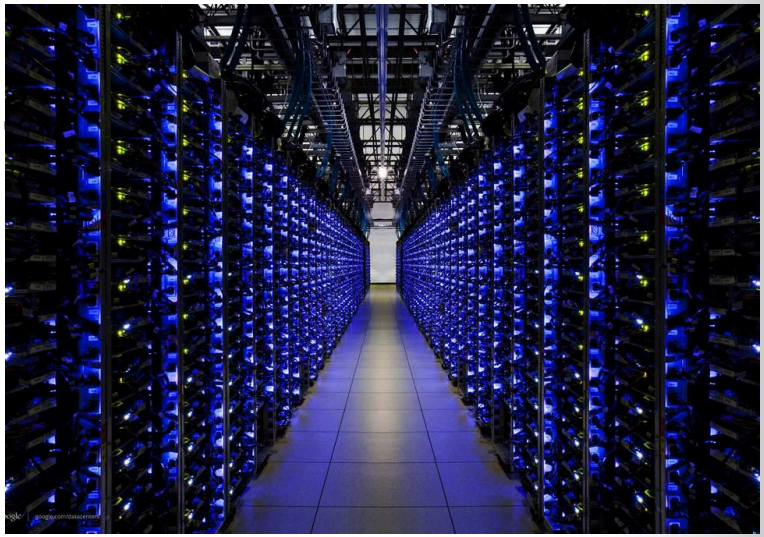
Myth #2 – Shore Up Internally



Principles of Effective Cybersecurity

Myth #3

But, We bought that thingy



- There isn’t a pill for every ill
- Do we know where our data is
- What are your regulatory issues
- Who manages your data, technology
- Can you afford subscription-based services

Principles of Effective Cybersecurity

Myth #3

But, We bought that thingy…

From Dr()p-B()x!! <Holli@ccmech.com>
Subject **Scan654464-87555!**
To

Reply | Reply All | Forward | More

Dropbox

You Have Received (5) pdf files sent to you via dropbox

Access File Here

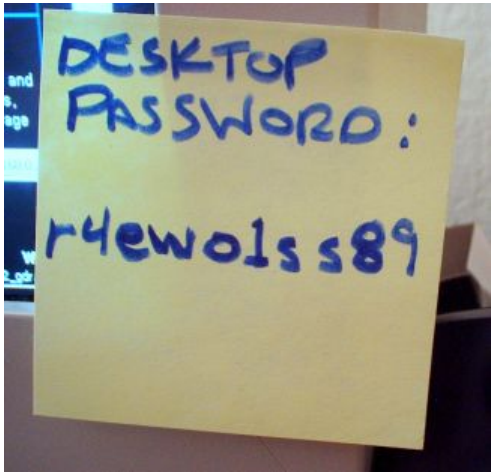
Happy Dropboxing!

File Will be deleted on =
5 March, 2018

Dropbox, Inc., PO Box 77767, San Francisco, CA 94107
© 2018 Dropbox.

2 Most Common Attacks

The two most common types of attacks combined account for **over 60% of all incidents.**



35%

MALICIOUS CODE

A term used to describe software created for malicious use. It is usually designed to disrupt systems, gain unauthorized access, or gather information about the system or user being attacked.

Third party software, Trojan software, keyloggers, and droppers can fall into this category.

28%

SUSTAINED PROBE / SCAN

Reconnaissance activity usually designed to gather information about the targeted systems such as operating systems, open ports, and running services.

Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

What's Hot

- Social Engineering – Phishing, Spear-Phishing
- Wifi Hijacking
- Side-Jacking
- Ransomware
- Poor patching practices
- Close loop on poor HR processes – know who's in, and who shouldn't
- BYOD
- Regulatory – FERPA, PCI, GLBA, HIPAA, EUGDPR, CIPA/COPPA, PPRA, AL-DB Act

Principles of Effective Cybersecurity

Ransomware attack targets Montgomery County government computer systems

Published: Tuesday, September 19th 2017, 10:45 am CDT
Updated: Tuesday, September 19th 2017, 11:15 am CDT

By WSFA 12 News Staff CONNECT

(Source: WSFA 12 News file photo)

MONTGOMERY CO., AL (WSF
Commission confirmed Tues
ransomware attack on its co
p.m. Monday.

"We're terribly sorry for this
information has been compr
Chief Information and Techn

Montgomery County pays ransom, regains files held hostage in cyber attack

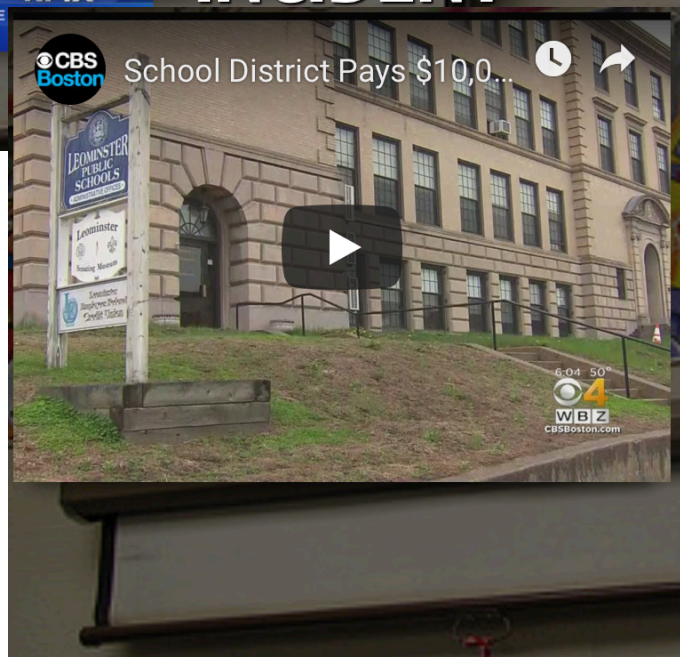
Published: Monday, September 25th 2017, 9:24 am CDT
Updated: Monday, September 25th 2017, 12:49 pm CDT

By WSFA 12 News Staff CONNECT

MONTGOMERY CO., AL (WSFA) - The ransomware attack that brought one of the largest counties in the state to a screeching halt has been resolved, both the cyber hacker and the county made good on their promises: the county paid more than $37,000 dollars in return, the files were returned.

Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS



Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

Summary of Effective Approaches

Here are a few tips to reduce your risks for cyber-attacks and data theft of sensitive customer information:

- Change the passwords you and your employees use to log into your technology systems on a regular basis
- Avoid emailing sensitive information, but if you do, use a secured email service
- Have employees lock their computer screens when they step away from their desks
- Avoid having unescorted/unsupervised visitors walking through your office
- Don't open strange email attachments or click unusual links in emails, especially from an unknown sender as they may be scams
- Have a written technology policy in place so that all of your employees understand the expectations and rules guiding how your business handles sensitive data

Loss of electronic data is not covered under most commercial theft policies because it is not a tangible asset, and most general liability policies also exclude coverage for your costs to notify customers of potential data theft, pay for the costs of investigating the loss or the costs of potential fines, penalties or lawsuits that result from a failure to protect the data. A cyber liability policy can provide your business with coverage that will help you cover several costs, including the expenses to inform your customers and regulatory authorities about the possible exposure of data.

Principles of Effective Cybersecurity

Summary of Effective Approaches

SECURITY AWARENESS TRAINING

More than ever, end-users are the weak link in your network security.

Principles of Effective Cybersecurity

ALABAMA ASSOCIATION OF SCHOOL BOARDS

Going phishing…

[EXTERNAL] AASB's 2019 March Academy Conference

A Alabama Association of School Boards <aasb@troy.edu>

Reply all

Thu 2/28, 5:03 PM

William Greg Price

Disclaimer: This email was sent from outside of your organization. Please do not open attachments or click links from an unknown or suspicious origin.

Dear AASB Members!

Thank you for registering for **AASB's 2019 March Academy Conference:**

Leadership for Financial Accountability. We have a packed agenda planned with the most current information on financial forecasting, best practices for handling cyber security threats, innovative ways to cut expenses and more! Join us Friday,March 1 and Saturday, March 2 at the Hyatt Regency Birmingham - the Wynfrey Hotel (6 training hours).

As part of the AASB Academy, we need you to verify your School Board Member Academy hours. Please visit this link: https://it.troy.edu/aasb/events.html. At the site you will need to select "Click Here To Update" near the middle of the page. The page will present Thank You is successful.

Don't forget about our exciting additional programs this year!

-AASB

2019 March Academy Conference: Leadership for Financial Accountability

Update your AASB Academy Profile

CLICK HERE TO UPDATE

Thank You

Principles of Effective Cybersecurity

Acknowledgements

- WEFUSA
- NAIC
- Verizon Data Breach Report
- IBM CyberThreat Report
- CSC
- Troy University
- Alabama Digital Forensics Institute
- Fabella Security

ALABAMA
ASSOCIATION OF
SCHOOL BOARDS

Conversations to take home

- Write down 1 – 2 things from this session that could lead

Q&A

Thank You!