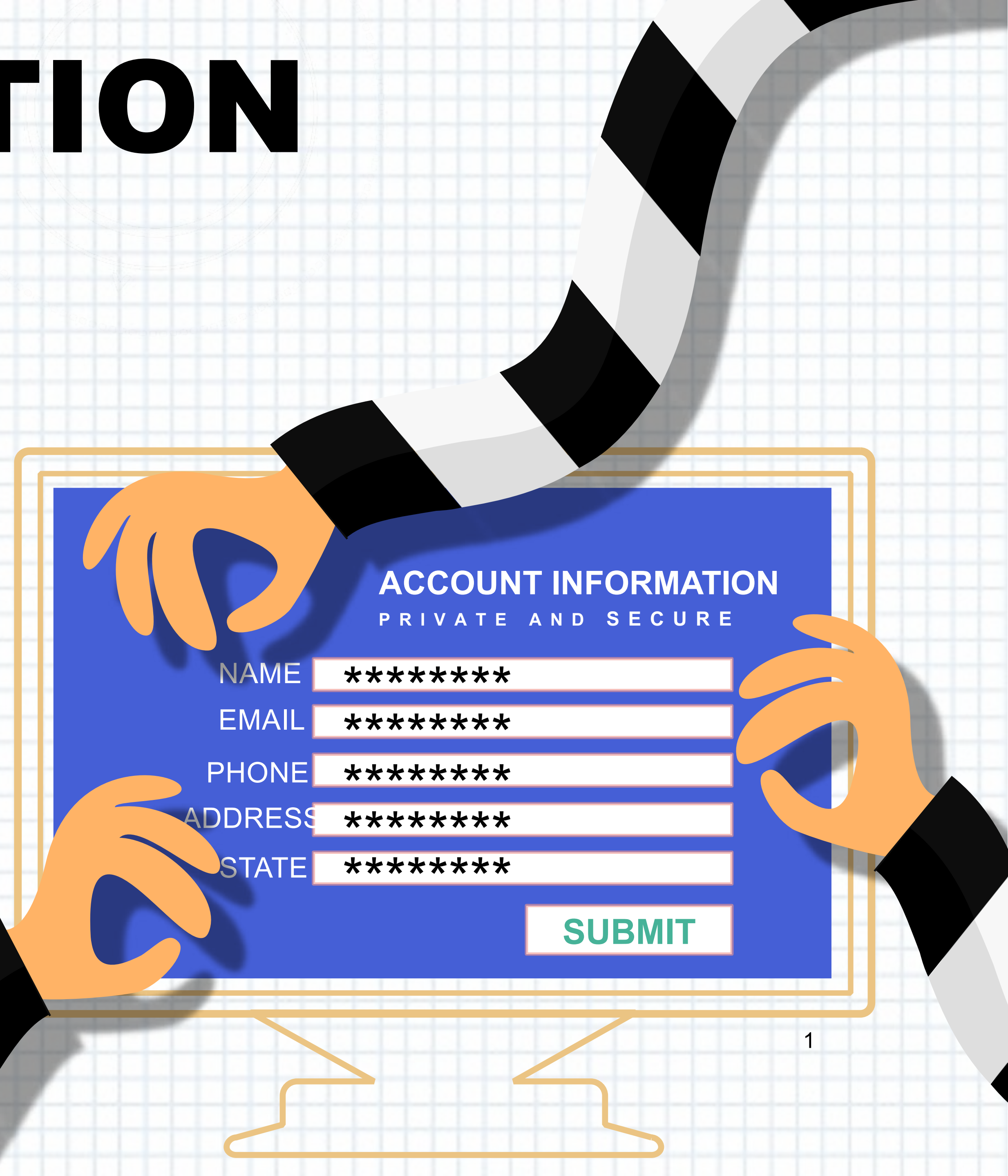
DATA PROTECTION

MODEL BOARD POLICY & ADMINISTRATIVE REGULATION

AASB ANNUAL CONFERENCE NOVEMBER 2022



AGENDA

1. Introduction
2. Tabletop Exercise
3. Model Policy (What is it?)
4. Relevance (Why is this important to me?)
    - Alaskan examples
    - Insurance Trends/Qualifications
    - Attacks and Risks
5. Available Resources (How will you do this?)
    - Implementation
    - Funding
6. Questions

TABLETOP EXERCISE

GUIDELINES:

1. This exercise will be held in an open, no-fault environment. Varying viewpoints are expected.

2. Respond to the scenario using your knowledge of existing plans and capabilities, and thoughts from your own experience.

3. This exercise is an opportunity to discuss and present multiple options and possible solutions and/or suggested actions to resolve or mitigate a problem.

4. There is no hidden agenda, and there are no trick questions.

5. The scenario has been developed in collaboration with subject matter experts.

CYBER ATTACK

Day 45

Following the most recent pay date, a report from Human Resources indicates that 38 employees did not receive their paychecks, despite having up-to-date account information and enabling direct deposit for their accounts.

IT staff receive an unusually high number of reports from faculty and staff who are unable to access their employee accounts. Staff members are seeing error messages that their credentials are invalid, or their account no longer exists in the system.

Day 46

Faculty and staff who are still logged in to the system cannot access their school emails, curriculum materials, and student grades on their local drives or the online school platform. They are presented with the following message on their devices:

"We own your data. For $350,000 in Bitcoin, your files will be returned. Submit payment to the wallet below within 96 hours, or everything will be posted for sale to the highest bidder. Don't believe us? We will publish some of your data every 24 hours."

CYBER ATTACK

Day 47

The Technology Director for your school District confirms the incident and says that the IT staff is working to solve the issue as quickly as possible.

Day 48

The attackers publish a sample of exfiltrated student data from your school on a hacker forum. They also claim they will release more data every 4 hours until the ransom is paid.

A social media post begins trending with **#SchoolHacked** and a screenshot of the hacker forum. The screenshot includes student names, telephone numbers, and addresses from your schools. Parents of the listed students angrily call the school, and many want to involve local law enforcement.

DISCUSSION

1. What are your priorities based on these events?
2. What actions would your School District take to minimize the incident’s impact on school operations?
   a. When would you consider instructing students not to use school-issued devices?
   b. Do you have backups to facilitate school system recovery? How long would it take to recover/restore systems?
3. What actions would be taken based on your School District’s incident response plan?
   a. What ransomware policies and procedures are included in your incident response plan?
   b. Does your District have a cyber insurance policy and what does it cover?
4. What is the decision-making process for ransomware payment?
   a. How are your cyber insurance providers involved in your procedures?
   b. What are the advantages/disadvantages to agreeing/refusing to pay?
   c. What are the potential legal and reputation ramifications?
5. When do you contact law enforcement during a cyber incident?
6. What concerns would arise with sensitive and/or personal information of students being available online?
   a. How does your District monitor social media?
   b. How would your District’s Superintendent or Public Information Officer respond to the social media posts and parent complaints?

WHAT?

1. AASB model Board Policy and Administrative Regulation 3522 for Data Protection
    - Complimentarily provided to all Alaska school districts via AASB
    - Hosted on the ALASBO website: http://www.alasbo.org/resources/bp-ar-3522-district-data-protection-program/
2. Foundationally created from the Matanuska-Susitna Borough School District operational BP and AR
3. Joint effort between AASB, ALASBO, Alaska Technology Directors, ASTE, and the Alaska Schools Data Protection Working Group

Advocates for Alaska's Youth
association of ALASKA school boards

ALASBO

AK Technology Directors

ASTE
alaska society for technology in education

RELEVANCE

1. LA Unified School District (LAUSD), which is the second largest district in the nation, was attacked 9/3/22 which put a spotlight on groups that are dedicated specifically targeting K-12 school districts.

2. CISA (Cybersecurity & Infrastructure Security Agency) created a joint statement on September 6th (https://www.cisa.gov/uscert/ncas/alerts/aa22-249a) along with the FBI and MS-ISAC (Multi-State Information Sharing and Analysis Center) to warn of the frequent targeting of K-12 educational institutions.

3. National organizations advocating to the FCC to allow cybersecurity to be funded through E-Rate include SHLB, COSN, SECA, and SETDA - https://www.cosn.org/cosn-news/statement-from-the-consortium-for-school-networking-cosn-state-e-rate-coordinators-alliance-seca-state-educational-technology-directors-association-setda-and-schools-health-libraries-broad/

ALASKAN EXAMPLES

2021

1. MAY - Department of Health and Social Services – Malware attack
2. MAY - Alaska State Court System – investigation ongoing - Malware
3. OCT - Alaska Seafood Marketing Institute
4. OCT – Alaska Division of Elections (also in 2016)

2019

5. SEPT - City of Unalaska - $3M Phishing Scam
6. MAR – Ketchikan Port and Harbors Dept - $20K loss from spoofed email
7. JAN – Alaska Department of Revenue Website – data breach

2018

8. JULY - City of Valdez
9. JULY - Matanuska-Susitna Borough – Phishing, Ransomware
10. MAY and FEB - University of Alaska – Hack/Phishing

CYBER INSURANCE TRENDS

- Organizations seeking cyber insurance have ***more than doubled*** in the last 4 years
- The cost for premiums has ***nearly doubled*** each of the last 3 years

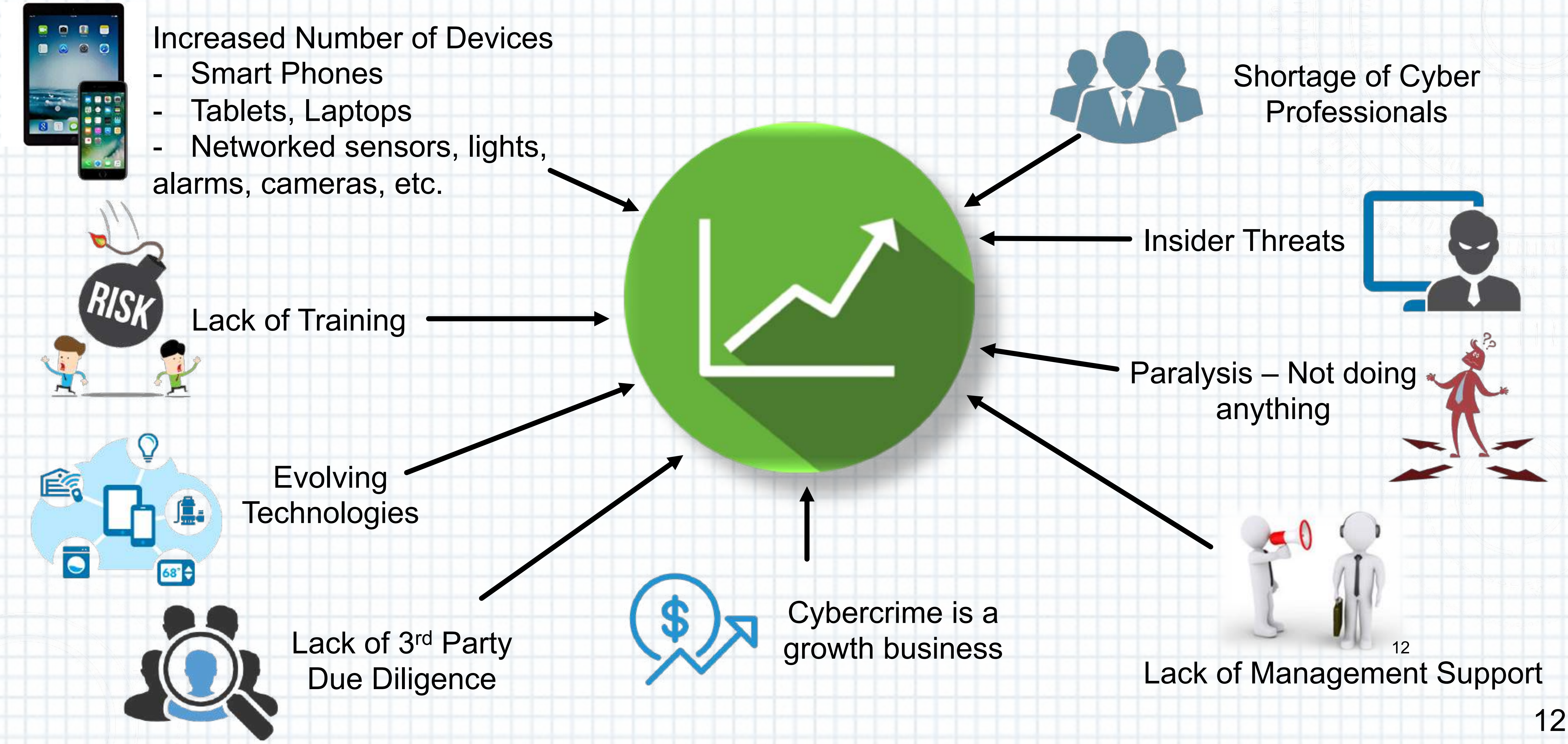
- In 2021 cyber-attacks were up 15% over 2020 – trend is increasing
- Cyber insurance market growing: $7.6 bn (2021) to $36.8 bn (2028)
- Insurers are constraining and qualifying coverages – must meet minimum requirements

INSURANCE QUALIFICATIONS

COVERAGE ***MAY NOT BE OFFERED*** IF THE FOLLOWING KEY CONTROLS ARE NOT PRESENT:

1. **Multi-Factor Authentication** (MFA) to secure:
   - ✓ Remote **network access**
   - ✓ **Email remote access** and access to email through a web app on a non-corporate device
   - ✓ **Access to backups**
   - ✓ **Domain/network administrator accounts**
2. **Endpoint Detection and Response** (EDR)
3. **Data** must be **backed up offline** or using a **third-party backup/storage application/software**

ATTACKS ON THE RISE



Increased Number of Devices
- Smart Phones
- Tablets, Laptops
- Networked sensors, lights, alarms, cameras, etc.

Lack of Training

Evolving Technologies

Lack of 3rd Party Due Diligence

Cybercrime is a growth business

Shortage of Cyber Professionals

Insider Threats

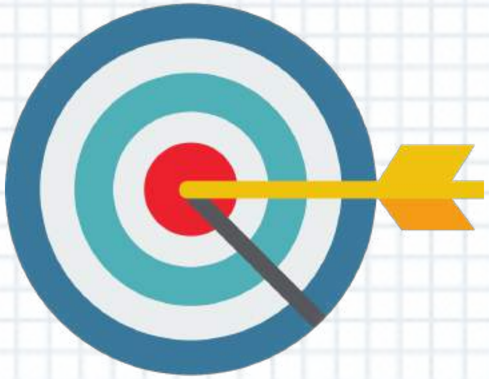
Paralysis – Not doing anything

Lack of Management Support

K-12 RISKS & THREATS

Who are the attackers?

1. Internal
2. External



What do they want?

1. Student Data
2. Money

How are they doing it?

1. Malware Attacks
2. Phishing
3. Spoofing

What are their motivations?

1. Money
2. Anger
3. Accidental
4. Boredom

AVAILABLE RESOURCES

Funding

1. RUS Grant
2. Movements to include in E-Rate
3. ESSER

Implementation Support

1. ALASBO Webinars to Support Implementation
2. State drafting Cybersecurity Strategic Plan

THE FIVE MOST EFFICIENT CYBER DEFENDERS ARE: ANTICIPATION, EDUCATION, DETECTION, REACTION AND RESILIENCE. DO REMEMBER: "CYBERSECURITY IS MUCH MORE THAN AN IT TOPIC.” - STEPHANE NAPPO

And the gold medal for the quickest opening of a dodgy email goes to...