Cybersecurity: The Human Factor

Lucas Anderson
TASB Risk Fund
TASA/TASB txEDCON 2020

This information is provided for educational purposes only to facilitate a general understanding of the law or other regulatory matter. This information is neither an exhaustive treatment on the subject nor is it intended to substitute for the advice of an attorney or other professional advisor. Consult with your attorney or professional advisor to apply these principles to specific fact situations.

© 2020 Texas Association of School Boards, Inc. All rights reserved.
Agenda

Cyber threat environment
Hacker philosophy
Psychology of cyber attacks
Case studies
Prevention
Best practices
Fund offerings
Questions?
Ground rules

Session is pre-recorded

Lucas is here with us live!

Throw any questions into chat for real time response

Unclear concepts? Please ask for clarification!

Grab contact info and reach out!
Cyber threat environment: Attack surface

WWW invented in 1989
• First website went live in 1991
• Now 1.2 billion websites

6 billion internet users by 2022 (75% of projected global population)

Microsoft – data volumes 50% greater in 2020 than they were in 2016

IoT – data big bang
• 2 billion objects in 2006
• 200 billion in 2020

Statistics from Cybersecurity Venture – Cybercrime Magazine 2019 Annual Report
Cyber threat environment: Statistics

Annual losses in 2015 - $3 trillion dollars
Annual losses by 2021 - $6 trillion dollars
  • More profitable than the global trade of all major illegal drugs

Greatest transfer of economic wealth in history
Fastest growing crime in the US
  • Government declared cyberthreat a national emergency

Spending on cybersecurity $1 trillion from 2017-2021
1.5 million vacant cybersecurity positions worldwide
Half of all cyberattacks target small business and governments

Statistics from Cybersecurity Venture – Cybercrime Magazine 2019 Annual Report
Cyber threat environment: Education

348 publicly disclosed incidents against schools in 2019
- 3x the amount from 2018
- 1/day in 2019

As of 2016 education is the most targeted sector for ransomware
- Incidents doubled from 2018-2019

 Millions of taxpayer dollars lost in business email compromise (BEC)
- Highest loss - $3.7 million dollars – Scott County Schools, Kentucky

Statistics from K12 Cybersecurity Resource Center 2019 Annual Report
Hacker philosophy: Varieties

Black Hats
• Your stereotypical bad guy.

White Hats
• Good guys! Ethical hackers working on identifying vulnerabilities

Gray Hats
• Between black and white hats. Somewhat unethical. Publish vulnerabilities. Not profit driven.

Script Kiddies
• Low skilled, but unpredictable and not ethical. Kids with dangerous toys. Immature.
Hacker philosophy: Varieties

Cyberspies
• Intelligence and military operatives of governments. Engaged in state-level espionage.

Cyberterrorists
• Exactly what it sounds like. Fear and political outcomes are their objectives.

State-Sponsored Hackers
• Sponsored by governments as ‘hidden hands.’

Organized Crime
• The mafia now has skin in the game. Why not?
Hacker philosophy: Motivation

Hackers objectives:

- Profit
- Skill development
- Goal achievement
- Fun
- Anonymity
Hacker philosophy: Methods

How to achieve these objectives?

Emotional levers

• Fear
• Perception of authority
• False trust
• Confusion

Cost/benefit analysis

• Risk avoidance
• Lowest hanging fruit approach
Case study: Fear

NetWalker – June 2020
• Michigan State University
• UCSF
• Columbia College Chicago

Demanded ransom
• Not for access
• To prevent exposure
• Dark web publication

Images courtesy of Insidehighered.com
Case study: Fear (cont.)

Widespread sextortion – 2020

- Attacker has a ‘valid’ old password
- Remote access tool
- Keystroke logger
- Hacked your webcam
- ‘Recorded’ you on illicit website
- Pay up or vid goes to your contacts
Case study: Authority

Ygnacio Valley High School – May 2018

• Phishing email from “IT”
• “Compromise” in logins!
• New passwords
• False site
• Access to grade systems
• Grade hacking
Case study: Authority (cont.)

Centenela Valley Union High School District – Lawndale, CA - 2019

- Spoofed supervisor email
- W2s
- Social security numbers
- Addresses
- Other personal information
- All staff
Case study: Trust

A Texas district in Rio Grande Valley – March 2019

- Employee directed to fraudulent Frost bank website
- Processing routine automated clearinghouse (ACH) payments
- $1.2 million to Turkey
- Additional $300k
- All stopped by secret service
Case study: Trust (cont.)

East Texas school district – October 2018

- Business email compromise
- New routing numbers
- New bond for stadium
- From “established construction partner”
- $600k lost via ACH
- Secret service brought in
Case Study: Confusion

West Carrollton ISD (Ohio) – August 2020

- Facebook post
- Offers livestream of district sports
- Link to pay site
- No actual stream!

Image courtesy of WDTN News 2 – Dayton, Ohio
Prevention: Training

FERPA/HIPAA
Cybersecurity awareness
Data classification
Data retention/disposal policies
Vendor risks
Physical theft/sabotage
Cybersecurity event drills
Prevention: Processes & regulations

- HIPAA/FERPA
- Least privilege
- Multi-person verification
- Data classification
- Acceptable use policy
Prevention: Technical

Email security policies
- Data loss prevention
- External banners

Web filtering
- Black/Whitelisting

Updates
- Routine and verified

Backups
- Onsite/offsite?
- Actionable?
Prevention: Preparation

Audits
- Critical infrastructure

Disaster recovery plans
- Offsite location
- Deployable fleet

Cybersecurity drills
- Designated personnel
- Points of contact
Best practices

Cybersecurity is not just a technical problem
  • People as first line of defense!

A culture of cybersecurity
  • Training

Requires understanding your district’s risks
  • Audits
  • Drills

Adequate
  • Financial protection (coverage)
  • Procedures (backups/patches)
  • Budget
Fund offerings

• Coverage
  • Liability
  • Claims process

• Training
  • District specific/needs based
  • DIR Certified - SafeSchools

• Resources
  • Guides
    • Cybersecurity plans
    • Backups/data loss prevention

• Publication
• Webinars
Questions?
Contact information:

Lucas Anderson  
Privacy and Cyber Risk Consultant  
Lucas.Anderson@tasb.org  
512.505.2893