Data Breach Awareness Exercise

Vermont

Ross Lemke
Privacy Technical Assistance Center

United States Department of Education
Privacy Technical Assistance Center

Who are we?

- PTAC is a technical assistance center under the Student Privacy Policy Office (SPPO)
- Provide guidance on FERPA, student privacy & data security
- Resources on our website: https://studentprivacy.ed.gov/
  - Trainings and Webinars
  - Documents
  - FAQs
- We are not the FERPA Police

Structure of Today's Activity

- Review of data breaches in education
- Provide the Exercise Scenario Background
- Walk through the content and deliberate as a group on response activities
- Discuss best practices to reduce the risk of a data breach

Where We Stand

- 350+ breaches in the last three years
- Millions of student & staff records compromised
- Increased focus for W2 scams, ransomware, and incidents related to remote learning
- Education is no longer unknown to the bad guys
- FBI has issued several advisories warning of targeting by cyberattacks specifically at schools

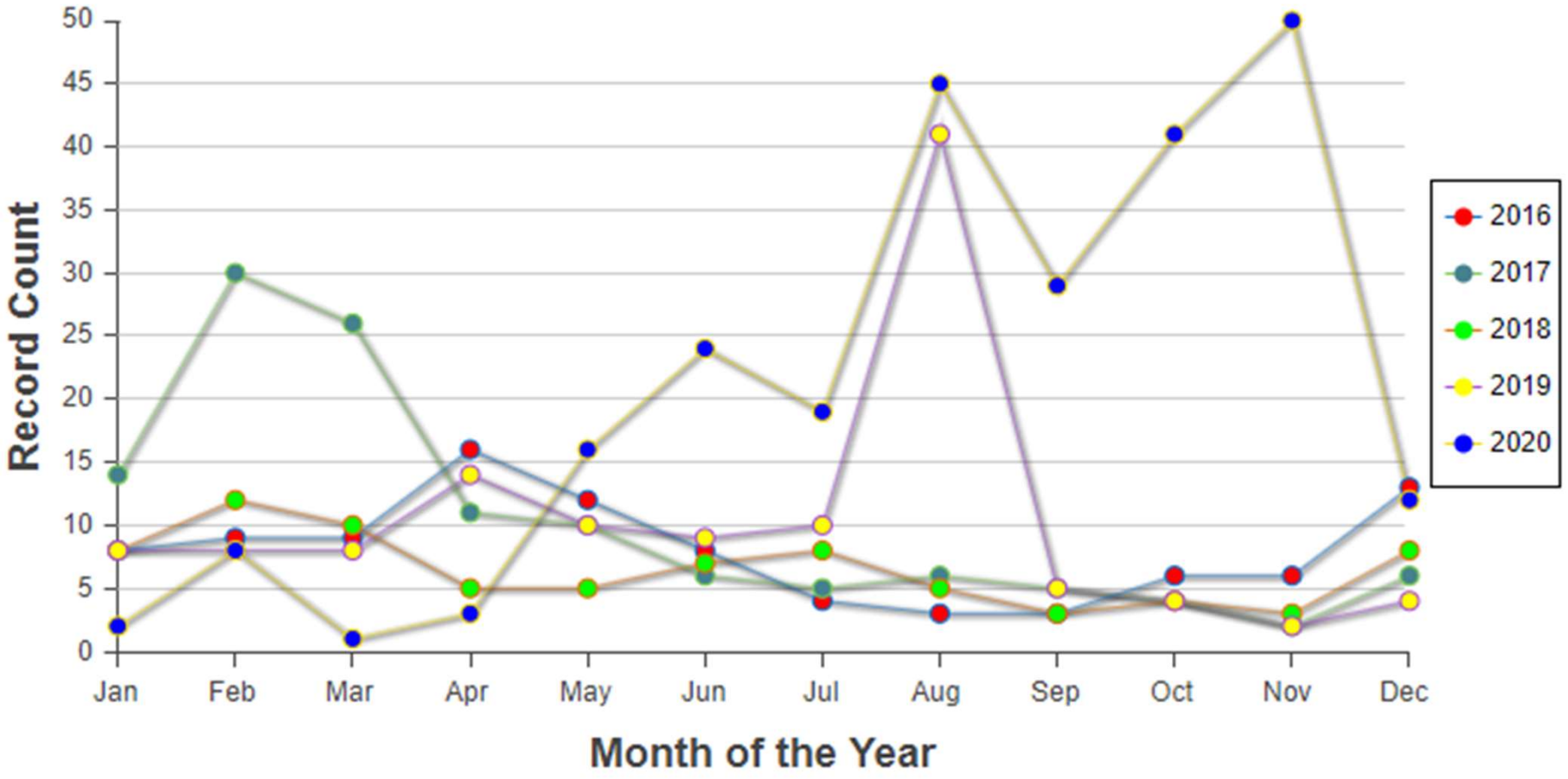
The Challenges

Remote learning & working is much more prevalent

- New technology platforms/software
- New reliance on enterprise systems, partners, vendors, and staff
- Staff training challenges
- New / Different attack surface & risks

Reported Data Breaches in Schools

How does this translate to schools



* Source: Identify Theft Resource Center (https://www.idtheftcenter.org/)

Problems in ED Data Systems

- A ton of old or unpatched software
- IoT devices in schools include:
  - Server room cameras & sensors
  - School surveillance systems
  - Access card readers
  - Modems (UPnP hackable)
  - HVAC / Boilers
- Hundreds of forgotten servers / computers
- Passwords
- Vendor vulnerabilities
- People

Data Breach Scenario Exercise

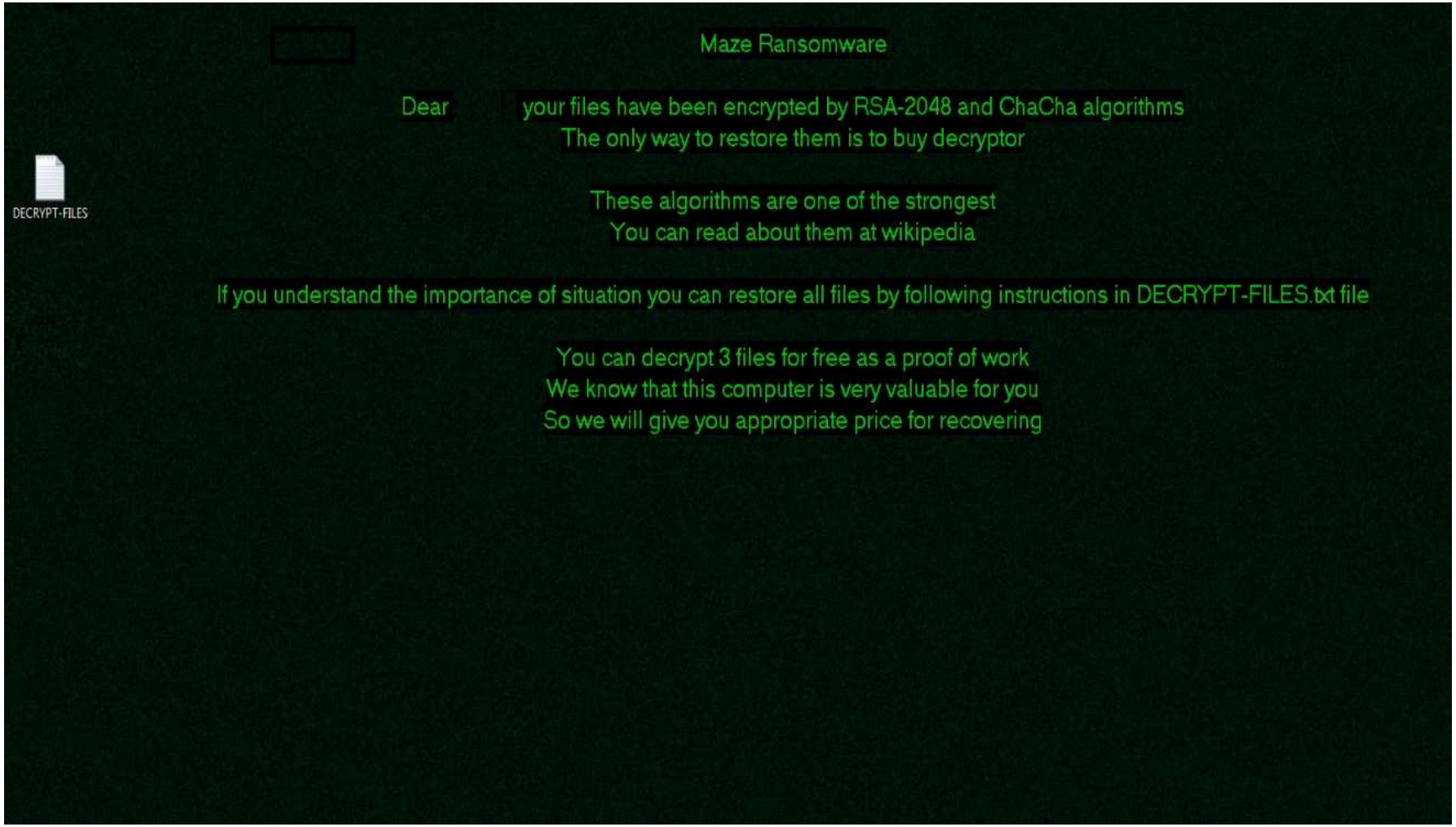
Background

It is Monday afternoon in mid-2020, and due to the COVID health emergency your school is not having in-person classes and most teachers are working mostly at home.

You rely heavily on your remote computing solutions now with most staff telecommuting and leveraging partner systems for distance learning activities.

Background

- The IT manager receives a call from a teacher who came in to pick up some lesson plans from her desk at school
- She claims that her computer's background has been changed and there is now a message being displayed:


Maze Ransomware
Dear
your files have been encrypted by RSA-2048 and ChaCha algorithms
The only way to restore them is to buy decryptor
These algorithms are one of the strongest
You can read about them at wikipedia
If you understand the importance of situation you can restore all files by following instructions in DECRYPT-FILES.txt file
You can decrypt 3 files for free as a proof of work
We know that this computer is very valuable for you
So we will give you appropriate price for recovering
DECRYPT-FILES

Background

- The IT staff audits the school's systems and finds 23 computers which are now exhibiting the notification screen for the Maze ransomware

Let's Regroup – What do we know?

- Our school has been the apparent victim of a ransomware attack
- At least 23 computers have already been infected
- Some of these systems have not been accessed in some time

Question: What is the first step here?

A. Wipe the affected machines and reinstall the software

B. Immediately shut down the school connection to the internet and report the issue to the FBI

C. Initiate your incident response process, validate the facts and move to isolate and contain the threat

Let's Put our Heads Together

Things to discuss:

- What are the root causes of these types of incidents?
- How can we control the event and reduce damage?
- Who do we need to tell, and what are the next steps?

Scenario Exercise

You quickly validate that the computers in question are indeed encrypted, and your investigation identifies that you have seen significant data transfers which appear to be data exfiltration.

Most of these connections app come from a machine in the sc department which has not been encrypted. This machine belon the science teacher who runs th school robotics club.

Scenario Exercise

The computer also has Remote Desktop enabled, allowing the teacher to log in remotely with his students and interact with several robots in the classroom as part of the club's extracurricular activities.

Question: How could this machine have been compromised?

A. The teacher's home computer was compromised, and attackers were able to obtain his school login and password to simply log in to this school computer
B. The teacher did not use a complex password and attackers were able to guess the password by trying common passwords
C. Attackers exploited a 0-day vulnerability in the RDP protocol to gain access to the machine

Scenario Exercise

This machine is found to contain instances of BEACON malware, malicious PowerShell scripts and files containing data encrypted from other machines in the school.

Logs show that this machine has had interactions with many of the school's systems and there are indications that the attackers used a stolen account to log into the system and harvested credentials from the machine which were then used to traverse the network.

Scenario Exercise

The attackers claim to have copies of all the encrypted data and are demanding 50k dollars in bitcoin in exchange for the decryption keys and promise not divulge the data.

Your logs confirm that the attackers have been able to exfiltrate large amounts of sensitive data from various staff computers as well as several network shares containing student data.

Let's Regroup – What do we know?

- Attackers likely gained a foothold in the system via RDP and were able to harvest credentials, giving them further access to the school's network
- They were additionally able to exfiltrate large amounts of sensitive data
- The attackers are demanding 50k in exchange for the decryption keys and a promise to delete the data stolen

Question: What is the best response here?

A. Force a password reset across the domain, including service accounts and reinstall the infected machines immediately

B. Separate the affected machines from the network, contain the infection by implementing egress filtering to cut off command and control, validate backups

C. Cancel classes and notify the public of the breach, report the incident to the police, and hire a third-party response firm

Let's Put our Heads Together

Things to discuss:

- Is this bigger than just the affected machines? How?
- Do you consider paying the ransom?
- Is this something that needs to involve law enforcement?
- Does this threat impact our ability to conduct learning?

Scenario Exercise

You identify that the attackers wer present in the environment for at least two weeks prior to the discovery of the encrypted deskto Investigators identify several domain accounts seemingly created by the attackers

The Active Directory appears to be compromised, at least insofar as the attackers had permissions to create administrative accounts.

Scenario Exercise

The good news: You have good backups from a time before the initial infection.

The bad news: Your Active Directory is potentially compromised, and you are faced with reconstituting everything from backups

Scenario Exercise

Recovery of the AD will take several days to accomplish, and unfortunately this will necessitate the need to turn off remote access and your distance learning platform for a couple of days.

This will necessitate notification of the public.

Let's Regroup – What do we know?

- The attackers were able to access the Active Directory and compromise critical accounts
- Reconstituting these critical enterprise systems will take some time and bring core school processes to a stop, including necessitating school closures for several days
- Notifications will have to be made

Question: What is the best approach to notifying parents and the public?

A. The principal sends out a notice to parents informing them of the school closure due to a data breach incident and refers questions to the incident manager for clarification

B. District Public Affairs / Communications team develops and disseminates a clear and concise message explaining the closure and directing parents to the website/s for more information

C. The incident manager calls the local paper and TV station and asks them to let the public know that school is cancelled

Let's Put our Heads Together

Things to discuss:

- Is this a data breach?
- What is the best messaging for communicating with our parents and the public the situation?
- What if any state laws may apply here?
- Are there things that we can do immediately to reduce the risk of a recurrence?

Post Exercise Questions

- Do your organizations have Incident Response Plans that address ransomware?
- Do you conduct periodic exercises to test your IR capabilities?
- What are some ways a school or district can communicate information about an incident most effectively?

Post Exercise Questions

- What are some of the things this organization could have done better?
- What can organizations do to increase the likelihood of detection?
- Does your state's data breach law impact your data breach response process? How?

Reducing the Risks

Best Practices for Making Yourself a Harder Target

United States Department of Education, Privacy Technical Assistance Center

Standards Are Your Friends

Reliable data security programs all have one thing in common… control:

- *Create standard software loads & enforce them*
- *Document Ports, Protocols & Services*
- *Police for compliance*

Process changes through a formal risk process

Perform Annual Risk Assessments

"The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact."

-National Institute of Standards and Technology (NIST)

What is a Risk Assessment?

Formal organizational process involving leadership, IT, and organizational stakeholders

Four stages:

- **Identification** – *finding, documenting, and categorizing risks*
- **Analysis –** *ascertaining the nature of the risks and determining their potential impact and effects*
- **Evaluation –** *applying organizational risk tolerance and existing controls to the risk to determine significance*
- **Control –** identifying and applying mitigating controls to reduce the risk based on analysis

"Cyber actors likely view schools as targets of opportunity, and these types of attacks are expected to continue through the 2020/2021 academic year"

- FBI / CISA / MS-ISAC

Schools are now a <u>focus</u> of cyber-attackers

- **Most of the reported cyber attacks against K12 schools were ransomware attacks**
- **Education accounts for more ransomware attacks than any other industry**
- **The pandemic has made us more likely to be attacked successfully and less likely to be able to operate through the event**

Top 5 Ransomware Defense Best Practices

- **Backups:** Frequent, Separate & Tested
- **Incident Response Plan:** Germane, Legally Sufficient, Trained
- **Accountability:** Leadership, Policy, Compliance
- **Awareness:** Annual, Mandatory, Assessed
- **Patching & Updates:** Trusted, Timely, Tracked

Final Food for Thought

- You should have an incident response plan in place and train to it
- Every organization should have some form of data privacy & security awareness training for all employees, at all levels
- Clearly understand the legal requirements for compliance with all applicable federal, state and local laws
- Consider calling PTAC, we can help!!!

PTAC Resources

- **Data Breach Response Checklist**
  https://studentprivacy.ed.gov/resources/data-breach-response-checklist
- **Downloadable Data Breach Training Kits**
  https://studentprivacy.ed.gov/resources/data-breach-response-training-kit
- **PTAC Student Privacy Training**
  - ***Videos*** - https://studentprivacy.ed.gov/content/guidance-videos
  - ***Online Training Modules*** - https://studentprivacy.ed.gov/content/online-training-modules

My Information

Ross Lemke

Director, Privacy Technical Assistance Center

(855) 249-3072
(202) 260-3887

privacyTA@ed.gov

https://studentprivacy.ed.gov

P0wn3dSchools

CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center

(855) 249-3072
(202) 260-3887

privacyTA@ed.gov

https://studentprivacy.ed.gov

Fax: (855) 249-3073