



Data Breach Exercise

Eric Gray & Mike Tassey

Privacy Technical Assistance Center

Agenda

- Introductions
- Group Assignments
- Scenario Background
-  *MAGIC HAPPENS*
- Report Out & Discuss

Introduction

- Think of this as a “murder mystery dinner”
- You will be divided up into <X> number of groups
- Each group will assume the role of responsibility as leaders of the organization
- This exercise will expose you to a scenario which has the potential to be a data breach
- You must work together to develop appropriate steps and messaging (both internal & external) to address the scenario as it unfolds

Background

Your organization manages the Statewide Longitudinal Data System (SLDS) for the State of New Statia.

Your SLDS collects data from schools / districts statewide, as well as from several State Agencies like the Labor Department. You have several public facing web applications and several hundred node enterprise network which includes server assets located in a State maintained data center.

Background

Today is the 14th of May, 2017. You have all just gotten back from lunch and you receive a message that two employees laptops seem to have be affected by some malicious software that has prevented access to their machines.

The employees laptops are displaying a screen which warns them that their files have been encrypted and demands payment.



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Monday to Friday

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

Send \$300 worth of bitcoin to this address:



12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Background

Neither of these employees report that any sensitive information was present on either affected laptop. The employees involved both work in HR.

With the end of the day approaching, you are now on the hot seat to determine what to do now... you have three days to pay the ransom of \$300.00 then it doubles before being erased the day after.

Group Exercise: What Now?

Given what we know so far, what is your assessment of the situation? Has there been a data breach? What should you do as an organization if anything?

Consider:

- What is a breach?
- What actually just happened?
- What are your first steps to respond?

Talk It Over

10 Minutes

Let's Chat

- What is a breach?
- What actually just happened?
- What are your first steps to respond?

The Event Evolves

As you wrestle with the two laptops you know about, reports begin to come in that other machines in the environment are also being affected by the malware. These are no longer just workstations that are turning up infected.

One server in particular is a legacy machine with an unknown amount of data on its storage. This device is no longer in production, and is not on the enterprise backup system. No one is sure exactly what is on the machine, but its folder structure .

Group Exercise: What Now?

So it looks like this is bigger than a couple of computers? At this point you want to be thinking about how to get on top of this thing. Do you have a strategy? What about the servers that are already hit?

Consider:

- Clearly this thing is self-perpetuating, what now?
- Has data been breached?
- What is your strategy to break the kill chain?

Talk It Over

10 Minutes

Let's Chat

- How is this malware spread?
- Has any data been breached?
- What is your strategy to break the kill chain?

World-wide Impact

It appears that this malware is hitting around the world, using a vulnerability affecting Microsoft operating systems to infect other systems once it is triggered like a worm. There was a patch available two months ago, but that patch had not been deployed to older machines in the organization.

Several production machines, including a key database server, have been affected by the malware. Normal operations are impacted by the lack of availability of data and key systems.

Group Exercise: What Now?

Okay, the malware has put a big monkey wrench in the works. You are missing some key data that you need. What are you going to do? Who do you tell?

Consider:

- Do you pay the ransom to maybe get back the data?
- Do you call the authorities? If so, who?
- How you will address recovery efforts? Who, what, why and when?

Talk It Over

10 Minutes

Let's Chat

- Do you pay the ransom? What if there are no backups?
- Do you involve the authorities?
- What about your partner organizations? Do you notify them?

News Travels Fast

Word has gotten out that the organization has fallen victim to WannaCry. You have reporters calling expecting details. Do you put out a statement? What do you say publicly about the event?

Consider:

- What messaging you will use both internally & externally
- Whether or not this is a Data Breach?

Let's talk about our plans

Who wants to go first?

For More Information

PTAC website @ <https://studentprivacy.ed.gov>

Resources include:

- [Data Breach Response Training Kit](#)
- [Breach Response Checklist](#)
- [FERPA Online Training & videos](#)
- [Recorded Webinars](#)

Contact Us:

PrivacyTA@ed.gov / [1-855-249-3072](tel:1-855-249-3072)

