FLEXCARE FACT

Did you know that Clip Training is part of FlexCare? Clip Training is an employee training and enablement tool. They have great videos around the entire M365 stack that you can leverage through your FlexCare agreement. Pricing begins at $25/month for 50 users. If you are interested or want to learn more about Clip Training, please see your Account Rep.

NETWORKCENTER
INCORPORATED

Choose your own ~~adventure~~ disaster: Internet

A Recycled (Paper Company) Choose your own Disaster Story

About Me

Mike Pagán

- Sr. Solution Architect
- Azure Product Manager
- 20+ years at Network Center

- About me:
  - 3 kids
  - 2 cats
  - 1 tortoise

CISSP®

CCSP™

SECURITYSTUDIO CvCISO LEVEL 1 CERTIFIED

CompTIA Project+ CERTIFIED

Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

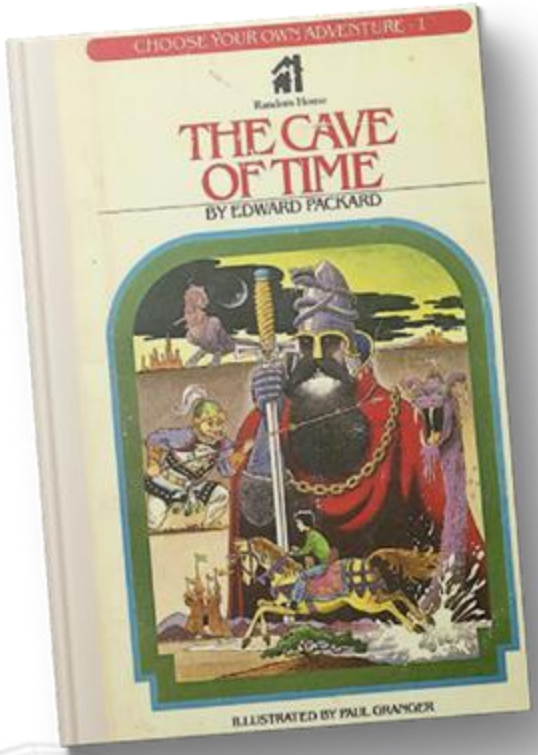
Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

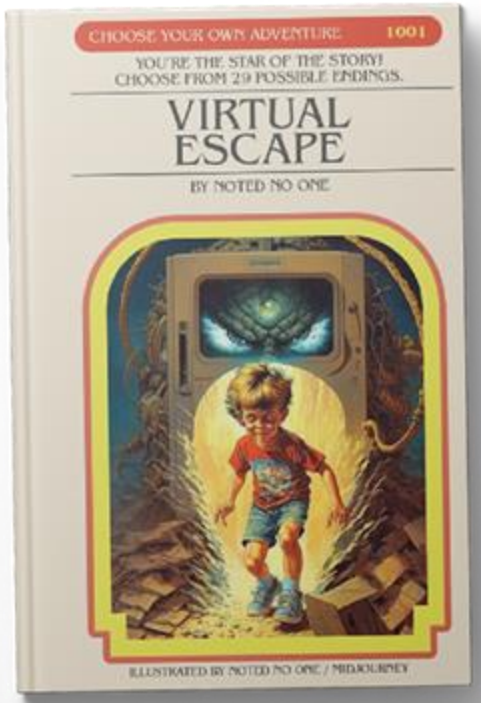
Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

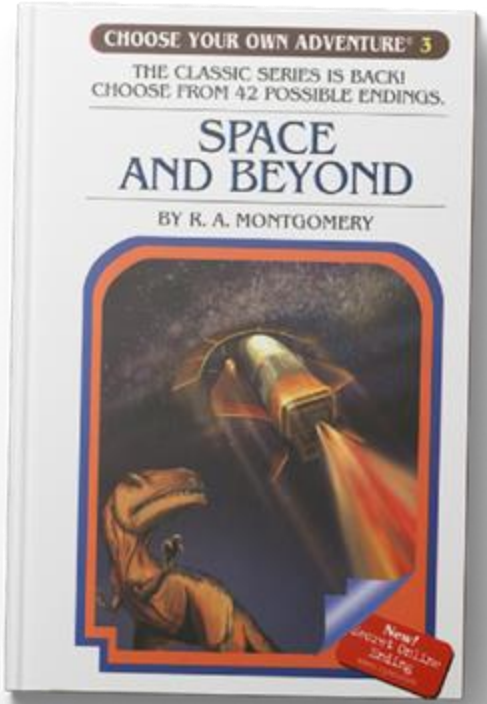
EC-Council CERTIFIED C|EH

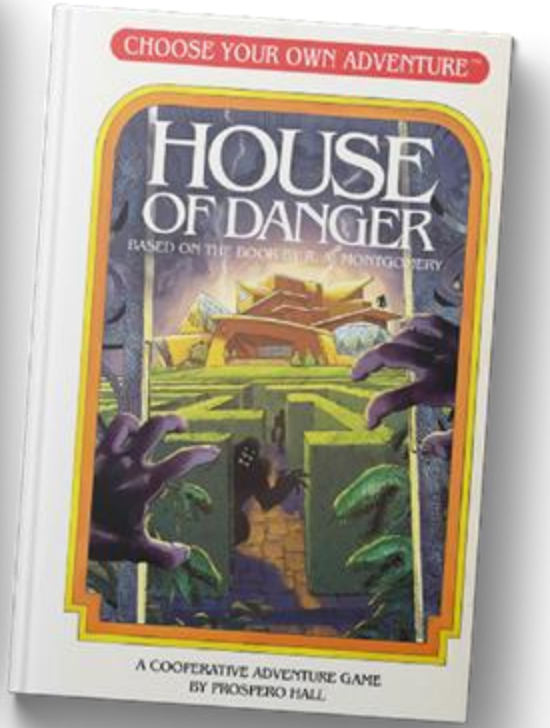
Certification
Citrix Certified Associate - Virtualization
CCA-V
citrix

A little nostalgia









Rules and Process

- Choices will be posted on the screen
- Your tablemates are your team
- Your team will have three minutes to decide which action to take
- We will discuss the choices and reasoning
- We will vote on the choice and continue the adventure
- In the “real world” other choices may be available; for this game we will only consider the options outlined

Before We Begin

Who has a cybersecurity incident response plan?

Who has gone through a cybersecurity tabletop exercise before?

WARNING: Audience participation is required!

Our Story Begins

The following is work of fiction. Any similarities to actual events or people or nationally syndicated television shows are purely coincidental.

Company Profile – Dunder Mifflin

- 60 Employees
- Paper/Paper Product Distributor
- $30M in annual revenue
- Based in Scranton, PA
- IT/Support team: One IT Admin (you)
- Partner with an MSP for helpdesk services

It started like a normal day…

Dunder Mifflin has recently been closing branches and going through budget cuts. This has put all projects on hold including the testing and rollout of new security solutions, including obtaining cyber insurance.

On the last day of the quarter, employees experience incredibly slow internet and Dwight (a salesperson) contacts their helpdesk for assistance.

The helpdesk suggests we reboot the firewall, which will take the internet offline for a while. Since it's been such a tough time with branches closing, the staff really need to close sales opportunities and fulfill orders to keep up their numbers. It's close to the of end of day and delays on entering orders could lead to sales teams staying late to catch up from the lost time.

What should we do next?

What do we do?

Have the helpdesk try to determine why the internet is slow.

Go to Slide 35

Have the helpdesk reboot the firewall now.

Go to Slide 20

Wait to reboot the firewall until tonight.

Go to Slide 10

Waiting it out

You try to make it through the day, but the internet is still crappy, and employees start complaining to management. Now, Angela in accounting is complaining that her files won't open, and her desktop wallpaper has been replaced with a "countdown clock." Panic ensues in the office as word spreads that it isn't just slow internet – we are experiencing a cyber attack.

You call your helpdesk for assistance, and they ask if you have cybersecurity insurance. Because of budget cuts your Branch Manager, Michael, said it was too expensive, so you do not have cybersecurity coverage. Your MSP recommends engaging an incident response firm for assistance immediately.

Do we call a cybersecurity incident response (IR) firm?

Next

Do we call an IR firm?

Yes

Go to Slide 12

No

Go to Slide 13

Yes

You call an incident response (IR) firm, and the initial block of labor is $36,000. It takes a day to get the paperwork finalized. The firm gets started deploying security agents and reviewing logs & systems. Your internet access is shutdown for two days while they perform their initial triage activities.

Slowly devices are allowed to come back online. After a week, you're fully up and running again. The IR firm was able to determine Toby from HR had brought a USB drive (to put his vacation pictures from Costa Rica on his work computer). The USB drive had malware, and that is how the bad actors got a foothold on your network.

You caught the malware ***before*** your server data was encrypted, but it appears that the bad actors exfiltrated data from your network. Do you know what they have? The IR firm can try to determine the information that was compromised. The follow up investigation will cost an additional $25,000.

Do you have the IR firm investigate?

Next

No

The helpdesk does their best by copying what they've seen other IR firms do in the past (deploying security agents, scanning systems for malware, patching everything, reimaging affected workstations, etc.) but they are not capable of determining initial point of compromise.

Because they cannot determine the source of the malware, they recommend restoring systems to before the presumed date of compromise to remove any unknown foothold the bad actors may have in your systems. Your systems would be restored to two weeks ago and data would need to be reentered or overlayed with known clean backups.

Do you restore your systems?

Next

Have the IR firm review the data?

Yes

Go to Slide 15

No

Go to Slide 16

Yes

You sign the additional work order for another $25,000, and the IR firm goes to work.

The IR firm starts by reviewing the uploaded sample data on the dark web. They also reach out and communicate with the bad actors and get a directory and file listing of the exfiltrated data. It takes another 4 days, but the IR firm has a list of the data that was stolen.

You finally catch a break. After reviewing the file listing and the "sample" from the bad actors, the various managers (data owners) determine that no employee or PII (Personally Identifiable Information) was compromised.

It is not all good news though, the remaining files included staff reduction plans, customer pricing information, and internal memos that will be damaging to the company's reputation. The data has not been released yet, so you have some time to plan how you'll deal with the internal and external fallout when this information becomes public.

End Scenario

No

You decided against having the IR firm attempt to discover what files were exfiltrated. You saved the $25,000, but you do not know what was taken.

By deciding to not attempt to review the information that was stolen, your company is blind to potential ramifications for the stolen data. Your Branch Manager, Michael, thinks you're in the clear, but then you start getting contacted by your partners about the breech. It turns out the bad actors have started contacting them and offered to sell them ***your*** data and to not release ***theirs.***

Because you don't know what was stolen and you have no control over if your partners (or your possibly your competitors) will buy the data, you may be at a disadvantage in future contract negotiations and have already started losing contracts.

Additionally, you are not able to determine the initial point of compromise or if the bad actors' foothold has been removed from your system. Have you done enough so this doesn't happen again?

End Scenario

Do you restore all systems to two weeks ago?

Yes

Go to Slide 18

No

Go to Slide 19

Yes

The helpdesk restores all your servers and reimages all your workstations. You lose two weeks of data and must reenter it or overlay more current data after it's scanned for malware. You are *fairly confident* that you have removed the bad actor's presence on your network.

The cost of the downtime and data entry is $120,000. You're back online and able to conduct business again. Things are returning to normal.

To help reduce the chances of this happening again, you add new security agents and monitoring services which cost $30,000/yr. You request a quote for cybersecurity insurance, but the premiums have doubled because of this event. Your company has avoided disaster, but the effects of this incident may last for years.

End Scenario

No

After the helpdesk finishes their cleanup tasks, you come in the following Monday morning and find your whole environment is encrypted by ransomware.

Your servers and workstations are unusable and critical services are offline. Not restoring your systems to a point before the breech left some malware on a system, allowing the bad actors to get back into the system. The bad actors figured out that their malware was discovered, so they encrypted everything, deleted your backups, and now have doubled the ransom.

You have the option to restore from a much older cloud backup which was not deleted and restore anything but that will take a week to get back up and running, that comes at a significant cost in labor and lost revenue. Paying the ransom is a viable option to save your business. You decide to bring in an incident response company to navigate the difficult decisions ahead

End Scenario

Still slow internet

This step took an hour with initially positive results.

…but the internet performance became slow again after about an hour. The original issue still exists, and the users are cranky.

Do you contact your helpdesk again?

Next

Contact your Helpdesk again?

Contact your MSP’s helpdesk.

Go to Slide 22

Explore the problem on your own.

Go to Slide 23

Contact MSP

After looking at the issue, your helpdesk reports more outbound traffic (HTTPS, specifically) than normal. The issue is tracked down to a workstation in the sales department, but the person who usually using this is out of the office today so there shouldn't be ***any*** traffic...

The helpdesk reports the outbound traffic is going to an odd site:

O4spiistorug1jq50600[.]appsync-api[.]us -west -2[.]verysekurecompany.biz

Based on the odd website, and the maxed outbound internet traffic, the helpdesk determines that someone is exfiltrating your data, which is causing your internet to slow. You also have some reports that a few workstations have been encrypted. Your helpdesk recommends getting a cybersecurity company involved immediately

Do you contact a cybersecurity company?

Next

Explore the problem on your own

You eventually get around to checking the firewall (after three meetings and fixing a printer jam)…

When you look at the firewall, you notice more outbound traffic (HTTPS, specifically) than normal. The issue is tracked down to a workstation in the sales department, but the person who usually using this is out of the office today so there shouldn't be ***any*** traffic...

The outbound traffic is going to an odd site:

O4spiistorug1jq50600[.]appsync-api[.]us -west -2[.]verysekurecompany.biz

You have seen a similar URL recently in a cybersecurity webinar and are worried that the traffic may be malicious. You suspect you are infected by malware. You remember from the webinar that a good first step is to isolate devices from the network, but that would take down business at the end of the quarter.

What do you do?

Next

Isolate all or slow machines only?

Isolate all machines.

Go to Slide 26

Isolate slow machines only.

Go to Slide 25

Slow machines only

The internet goes back to normal. Yay!

By only isolating the known slow devices, you are quickly able to restore internet service and determine that the slow workstations have been infected by malware.

Now you know what caused the slow internet and luckily most are not affected, but why was there that much outbound internet traffic? How did the malware get on one of your systems?

You know you are not capable of answering those questions with certainty. It may be time to bring in the experts.

Do you reach out to a cybersecurity company?

Next

Isolate all your machines

Business is impacted because no one can communicate with customers, close sales, or fulfill orders. You find other ways to access the internet for a few critical workstations with hotspots, then scan your workstations. You start with the workstation with the large amount of outbound traffic. In the process, you discover one workstation is infected with malware, but the rest are clean.

Now you know what caused the slow internet and luckily most are not affected, but why was there that much outbound internet traffic? How did the malware get on one of your systems?

You know you are not capable of answering those questions with certainty. It may be time to bring in the experts.

Do you reach out to an IR firm?

Next

Do you call an IR firm?

Yes

Go to Slide 28

No

Go to Slide 29

Yes

You sign a work order for $25,000 and the IR firm goes to work.

The IR firm starts by reviewing the uploaded sample data on the dark web. They also reach out and communicate with the bad actors and get a directory and file listing of the exfiltrated data. It takes 4 days, but the IR firm has a list of the data that was stolen.

You finally catch a break. After reviewing the file listing and the "sample" from the bad actors, the various managers (data owners) determine that no employee or PII (Personally Identifiable Information) was compromised. It is not all good news, the remaining files included staff reduction plans, customer pricing information, and internal memos that will be damaging to the company's reputation. The data has not been released yet, so you have some time to plan how to deal with the internal and external fallout when this information becomes public.

Additionally, the IR firm was able to determine the initial point of compromise and is very confident that the foothold the bad actors had in your system has been removed.

End Scenario

No

You decided against having the IR firm attempt to discover what files were exfiltrated. You saved the $25,000, but you do not know what was taken.

By deciding to not attempt to review the information that was stolen, your company is blind to potential ramifications for the stolen data. Your Branch Manager, Michael, thinks you're in the clear, but then you start getting contacted by your partners about the breech. It turns out the bad actors have started contacting them and offered to sell them ***your*** data and to not release ***theirs*.**

Because you don't know what was stolen and you have no control over if your partners (or your possibly your competitors) will buy the data, you may be at a disadvantage in future contract negotiations and have already started losing contracts.

Additionally, you are not able to determine the initial point of compromise or if the foothold the bad actors had in your system has been removed. Have you done enough so this doesn’t happen again?

End Scenario

Do you call an IR firm?

Yes

Go to Slide 31

No

Go to Slide 32

Yes

You call an incident response (IR) firm, the initial block of labor is $36,000. It takes a day to get the paperwork finalized. The firm gets started deploying security agents and reviewing logs & systems. After their forensics work, the IR firm recommends restoring your servers and reimaging your workstations. You accept their plan.

After a week, the company is back online. The IR firm was able to determine Toby from HR had brought in a USB drive and put his vacation pictures from Costa Rica on his work computer. The USB drive had malware, and that is how the bad actors got a foothold on your network.

The cost of the downtime, restoring of systems, and data reentry is $120,000 which brings you back online and able to conduct business again. Things are returning to normal. To help reduce the chances of this happening again, you add new security agents and monitoring services which cost $30,000/yr. You request a quote for cybersecurity insurance and the premiums have doubled because of this event. Your company has avoided disaster, but the effects of this incident may last for years.

End Scenario

No

The helpdesk does their best by copying what they've seen other IR companies do in the past (deploying security agents, scanning systems for malware, patching everything, reimaging affected workstations, etc.) but they are not capable of determining initial point of compromise. They recommend restoring your servers to 2 weeks ago and reimaging your workstations. You accept their plan.

The helpdesk restores all your servers and reimages all your workstations. You lose two weeks of data and must reenter it or overlay more current data after its scanned for malware. You're *fairly confident* you have removed the bad actor's presence on your network.

The cost of the downtime and data entry is $120,000 which brings you back online and able to conduct business again. Things are returning to normal. To help reduce the chances of this happening again, you add new security agents and monitoring services which cost $30,000/yr. You request a quote for cybersecurity insurance and the premiums have doubled because of this event. Your company has avoided disaster, but the effects of this incident may last for years.

End Scenario

No

You did catch the breach before all the servers end endpoints were encrypted, but data was exfiltrated. You patch all the servers, PCs and firewalls, but is that enough? What data was stolen?

Eventually you learn what data was stolen when a customer sends you a link to a security company that posts about data breaches. Now you rush to review the data for PII (Personally Identifiable Information), trade secrets and other sensitive information.

You've entered damage control time. By not being proactive and engaging a cyber security company, you are behind the 8-ball and your customers are not happy.

Also, you never find out how the bad actors got into your network…

End Scenario

Yes

You sign the additional work order for $25,000 and the IR firm goes to work.

The IR firm starts by reviewing the uploaded sample data on the dark web. They also reach out and communicate with the bad actors and get a directory and file listing of the exfiltrated data. It takes another 4 days, but the IR firm has a list of the stolen data.

You finally catch a break. After reviewing the file listing and the "sample" from the bad actors, the various managers (data owners) determine no employee or PII (Personally Identifiable Information) was compromised. It is not all good news, the remaining files included staff reduction plans, customer pricing information, and internal memos that will damage the company's reputation. The data has not been released yet, so you have some time to deal with the internal and external fallout when this information becomes public.

End Scenario

Ask MSP to find out

After looking at the issue, your helpdesk reports more outbound traffic (HTTPS, specifically) than normal. The issue is tracked down to a workstation in the sales department, but the person who usually uses it is out of the office today so there shouldn't be ***any*** traffic...

The helpdesk reports the outbound traffic is going to an odd site:

O4spiistorug1jq50600[.]appsync-api[.]us -west -2[.]verysekurecompany.biz

Based on the odd website and the maxed outbound internet traffic, the helpdesk determines someone is exfiltrating your data, which is causing your internet to slow. You also have some reports that a few workstations have been encrypted. Your helpdesk recommends getting an IR firm involved immediately

Do you contact an IR firm?

Next

Do you call an IR firm?

Yes

Go to Slide 37

No

Go to Slide 38

Yes

You call an incident response (IR) firm, the initial block of labor is $36,000. It takes a day to get the paperwork finalized. The firm gets started deploying security agents and reviewing logs & systems. Your internet access is shutdown for two days while they perform their initial triage activities.

Devices are slowly allowed to comeback online and after a week, you're fully up and running again. The IR firm was able to determine Toby from HR had brought in a USB drive and put his vacation pictures from Costa Rica on his work computer. The USB drive had malware, and that is how the bad actors got a foothold on your network.

You caught the malware ***before*** your server data was encrypted, but it appears the bad actors exfiltrated data from your network. Do you know what they have? The IR firm can try to determine what information was compromised. The follow up investigation will cost an additional $25,000.

Do you have the IR firm investigate?

Next

No

The Helpdesk does their best by copying what they've seen other IR companies do in the past (deploying security agents, scanning systems for malware, patching everything, reimaging affected workstations, etc.) but they are not capable of determining initial point of compromise.

They recommend restoring systems to two weeks ago, before the presumed date of compromise to remove any unknown foothold the bad actors may have in your systems.

Do you restore your systems?

Next

Do you restore all systems to two weeks ago?

Yes

Go to Slide 40

No

Go to Slide 41

Yes

The Helpdesk restores all your servers and reimages all your workstations. You lose two weeks of data and must reenter it or overlay more current data after it's scanned for malware. You're *fairly confident* you have removed the bad actor's presence on your network.

The cost of the downtime and data entry is $120,000. You're back online and able to conduct business again. Things are returning to normal.

To help reduce the chances of this happening again, you add new security agents and monitoring services which cost $30,000/yr. You request a quote for cybersecurity insurance and the premiums have now doubled because of this event. Your company has avoided disaster, but the effects of this incident may last for years to come.

End Scenario

No

After the helpdesk finishes their tasks, you head home for the weekend. When you come in the following Monday morning you discover your entire environment is encrypted by ransomware. Your servers and workstations are unusable and critical services are offline.

Not restoring your systems to a point before the breech left some malware on a system. Thus, allowing the bad actors to get back into the system. The bad actors figured out their malware was discovered, so they encrypted everything, deleted your backups, and have now doubled the ransom.

You have the option to restore from a much older cloud backup which was not deleted. You could restore everything, but that will take a week to get back up and running. Doing so also comes with a significant cost in labor and lost revenue. Paying the ransom is a viable option to save your business. You decide to bring in an IR firm to navigate the difficult decisions ahead.

End Scenario

Have the IR firm review the data?

Yes

Go to Slide 43

No

Go to Slide 44

Yes

You sign the additional work order for $25,000 and the IR firm goes to work.

The IR firm starts by reviewing the uploaded sample data on the dark web. They also reach out and communicate with the bad actors and get a directory and file listing of the exfiltrated data. It takes another 4 days, but the IR firm has a list of the stolen data.

You finally catch a break. After reviewing the file listing and the "sample" from the bad actors, the various managers (data owners) determine no employee or PII (Personally Identifiable Information) was compromised.

It is not all good news, the remaining files included staff reduction plans, customer pricing information, and internal memos that will damage the company's reputation. The data has not been released yet, so you have some time to deal with the internal and external fallout when this information becomes public.

End Scenario

No

You decided against having the IR firm attempt to discover what files were exfiltrated. You saved $25,000, but you do not know what was taken.

By deciding to not attempt to review the information that was stolen, your company is blind to potential ramifications for the stolen data. Your Branch Manager, Michael, thinks you're in the clear, but then you start getting contacted by your business partners about the breech. It turns out the bad actors have started contacting your business partners and offering to sell them ***your*** data and to not release ***theirs*.**

Because you don't know what was stolen and you have no control on if your customers (or your competitors) will buy the data, you may be at a disadvantage in future contract negotiations and have already started losing contracts.

Additionally, you are not able to determine the initial point of compromise or if the foothold the bad actors had in your system has been removed. Have you done enough so this doesn’t happen again?

End Scenario

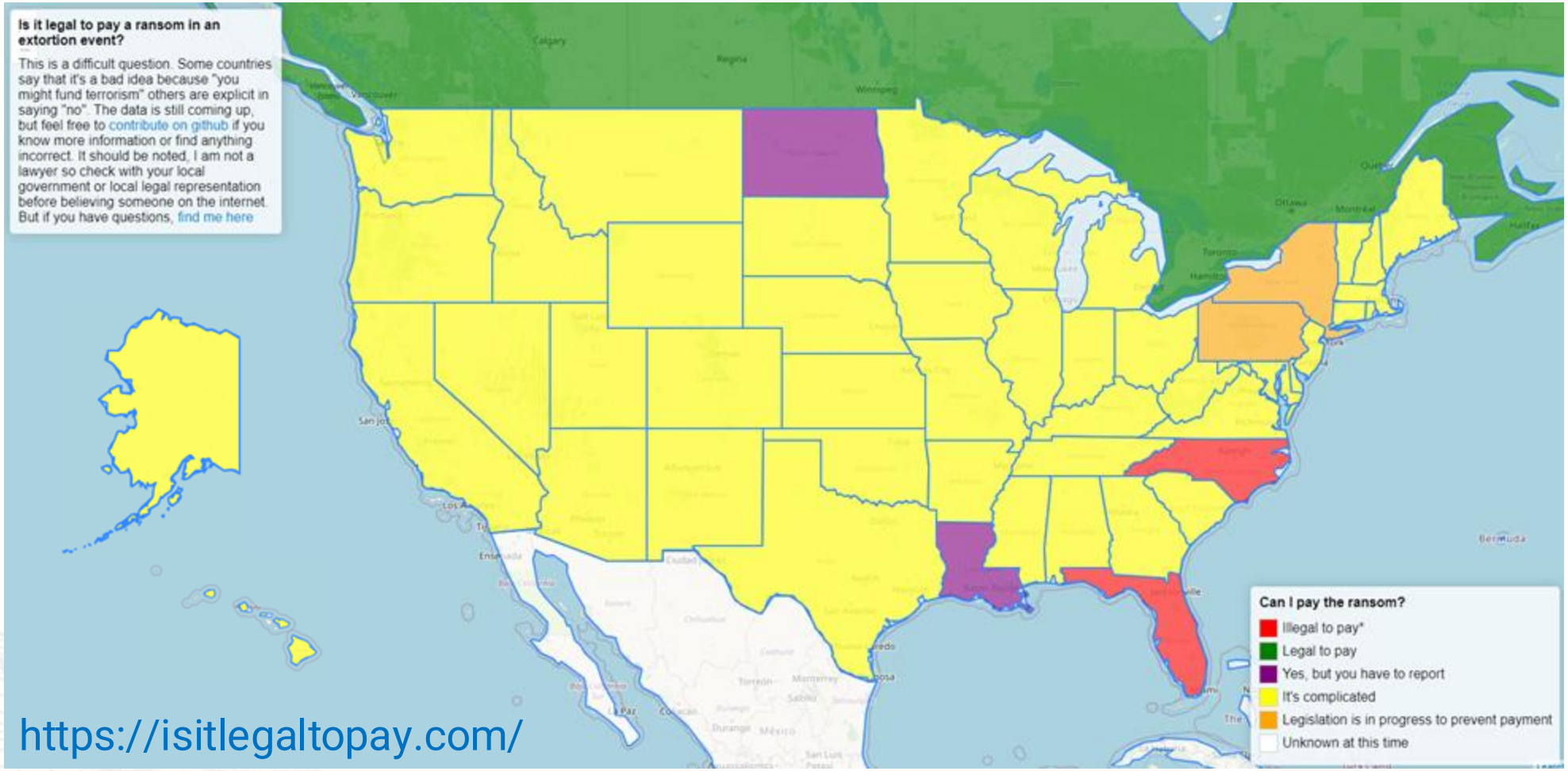
How did we do?

- Are you happy with the results?
- What could we have done differently?
- Is it *legal* to pay a ransom?

"By failing to prepare, you're preparing to fail"

— Benjamin Franklin

Is it Legal to Pay?



Be Prepared - Planning

- Understand your environment/data, then document it
- Store your incident response plan off-network
- Have a communications plan
  - Internal and external
- Know your security contacts:
  - Cybersecurity insurance provider
  - Incident response company
  - Law enforcement
- Consider cybersecurity IR service retainer

Be Prepared - Practice

- **Educate your employees**
- **Create an “no shame” culture**
- Complete a risk assessment
- Complete a Business Impact Analysis (BIA)
- Conduct annual tabletop exercises
- Conduct annual DR tests (full)
  - Preferably monthly automated restores
- Understand “normal”

Be Prepared - Technology

- **Implement multi-factor authentication**
- Follow good security guidelines: CISA, CIS, NIST CSF 2.0, etc.
- Keep your systems up-to-date
- Filter internet egress traffic
- Isolate your key assets
- Monitor vulnerability lists
- Follow 3-2-1-1-0 backup strategy
  - 3 copies of your data
  - 2 different storage media
  - 1 offsite, 1 immutable, 0 errors

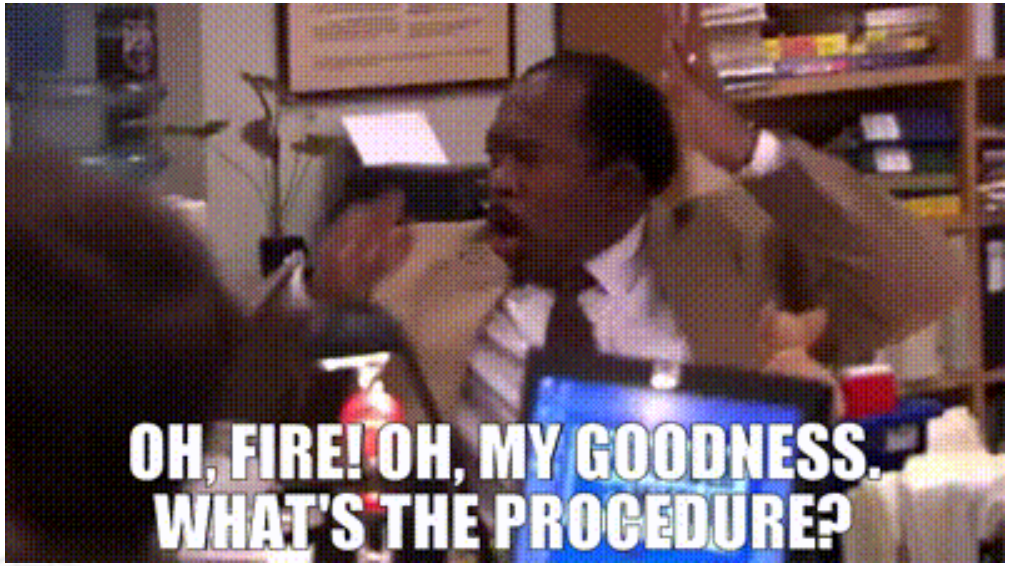
Resources (Planning)

- CISA Tabletop Exercise Packages | CISA
- Incident Reporting System | CISA
- Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (treasury.gov)
- Computer Crime Statutes (ncsl.org)
- Incident Response Plan Template | FRSecure
- Ransomware Response Playbook | FRSecure
- Interactive Map of Countries that Will Allow You to Pay Ransomware or Extortion Demands (isitlegaltopay.com)

Resources (Technical)

- Halcyon - Recent Ransomware Attacks
- Ransomware | Latest Threats | Microsoft Security Blog
- MITRE ATT&CK®
- Public Incident Response Resources / Public Playbooks · GitLab
- Known Exploited Vulnerabilities Catalog | CISA
- Cybersecurity and Infrastructure Security Agency (email subscriptions)
- NVD – Home (National Vulnerability Database - NIST)
- CVE Website

How Can I Be Prepared?



Three things:

- Make a plan
- Know your environment
- Who you gonna call?

NETWORKCENTER INCORPORATED

Thanks for Playing!

How to contact me

- mike.pagan@netcenter.net
- linkedin.com/in/mikep2/
- Twitter: @mjpagan

Decision Tree

Stats:

- 3 paths
- 10 total decisions
- 12 endings