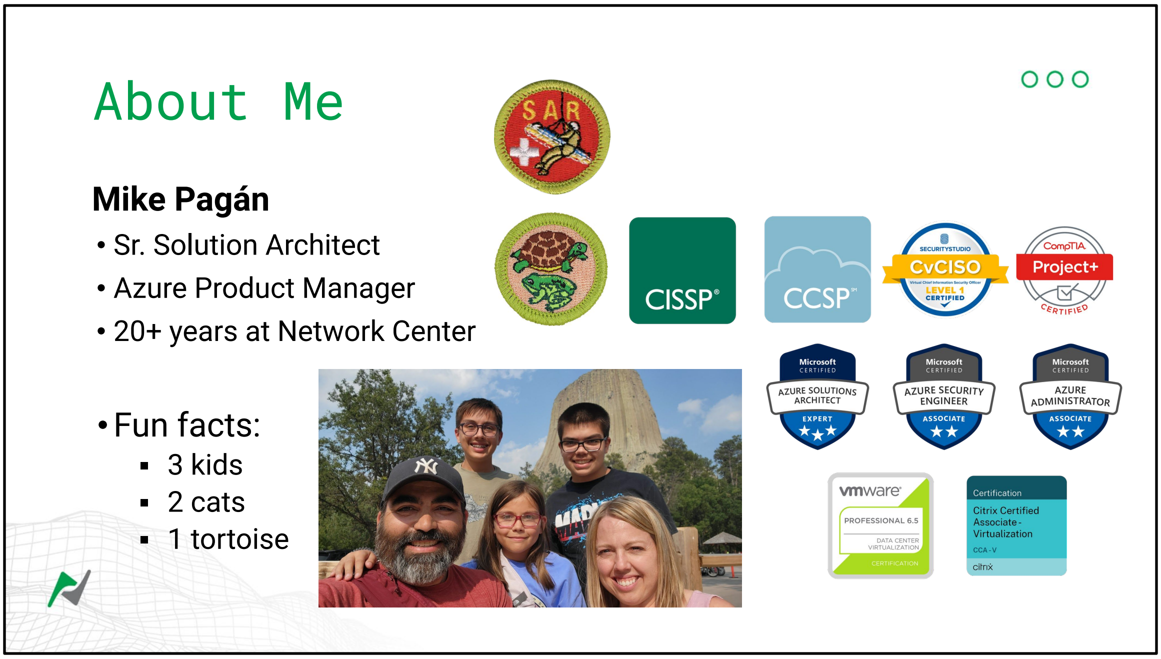
NETWORKCENTER
INCORPORATED

Choose Your Own ~~Adventure~~ Disaster: Ransomware

A Choose Your Own Disaster Story



About Me

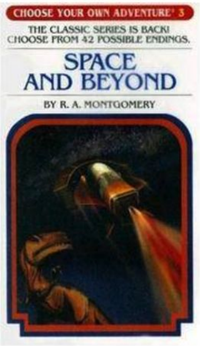
Mike Pagán

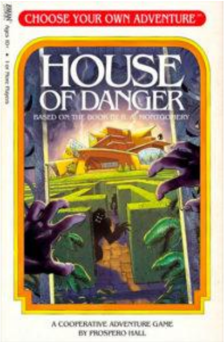
- Sr. Solution Architect
- Azure Product Manager
- 20+ years at Network Center

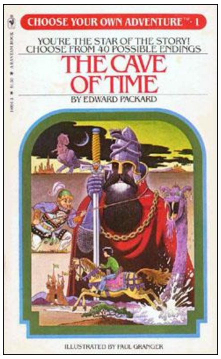
- Fun facts:
  - 3 kids
  - 2 cats
  - 1 tortoise

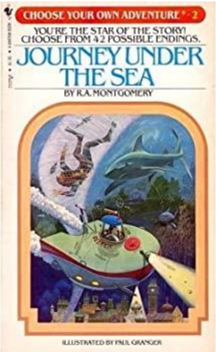
Outdoor enthusiast with a technology addiction

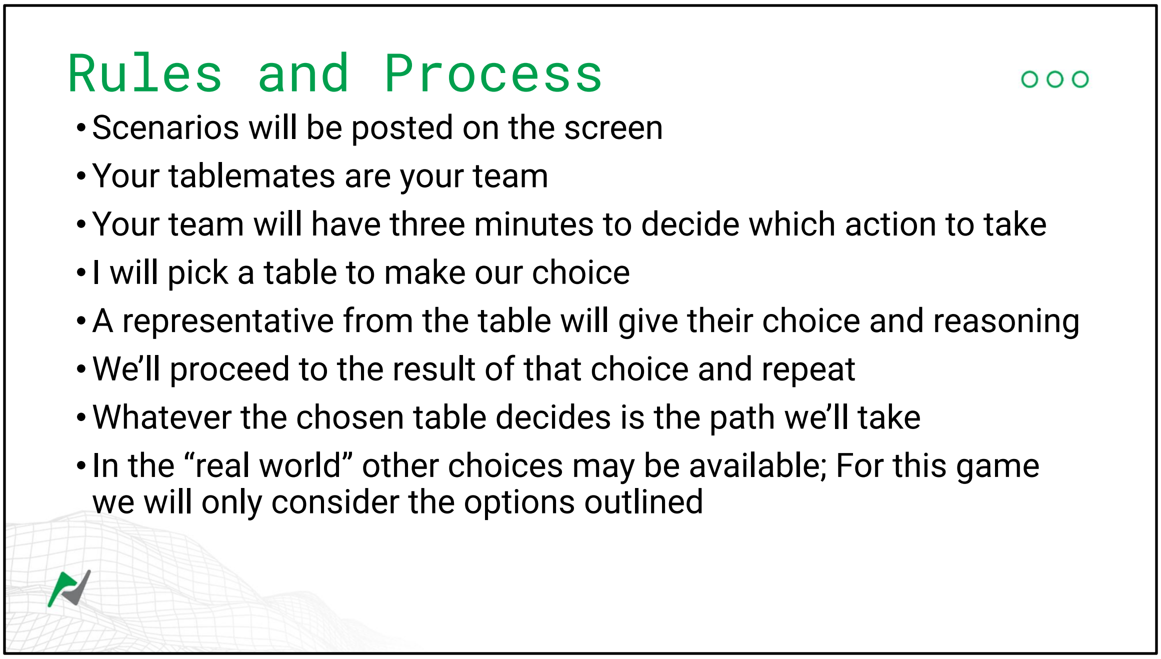
Anyone remember these?


CHOOSE YOUR OWN ADVENTURE 3
THE CLASSIC SERIES IS BACK!
CHOOSE FROM 42 POSSIBLE ENDINGS.
SPACE AND BEYOND
BY R. A. MONTGOMERY


CHOOSE YOUR OWN ADVENTURE
HOUSE OF DANGER
BASED ON THE BOOK BY R. A. MONTGOMERY
A COOPERATIVE ADVENTURE GAME
BY PROSPERO HALL


CHOOSE YOUR OWN ADVENTURE 1
YOU'RE THE STAR OF THE STORY!
CHOOSE FROM 40 POSSIBLE ENDINGS
THE CAVE OF TIME
BY EDWARD PACKARD
ILLUSTRATED BY PAUL GRANGER


CHOOSE YOUR OWN ADVENTURE 2
YOU'RE THE STAR OF THE STORY!
CHOOSE FROM 42 POSSIBLE ENDINGS.
JOURNEY UNDER THE SEA
BY R.A. MONTGOMERY
ILLUSTRATED BY PAUL GRANGER



Rules and Process

- Scenarios will be posted on the screen
- Your tablemates are your team
- Your team will have three minutes to decide which action to take
- I will pick a table to make our choice
- A representative from the table will give their choice and reasoning
- We'll proceed to the result of that choice and repeat
- Whatever the chosen table decides is the path we'll take
- 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 run through a cybersecurity tabletop exercise before?

WARNING: Audience participation is required!

Company Profile

- Global Manufacturer
- 2,000 Employees
- $100M in annual revenue
- Based Santa Catalina Island, CA
- Experienced a ransomware event less than 1 year ago and paid the ransom
- CISO was let go after last incident and position is currently vacant and the CIO is currently backpacking through Europe
- In-house Security Operations Center is staffed with employees new to the organization and with limited experience in the field
- 300 Servers
- 2250 workstations

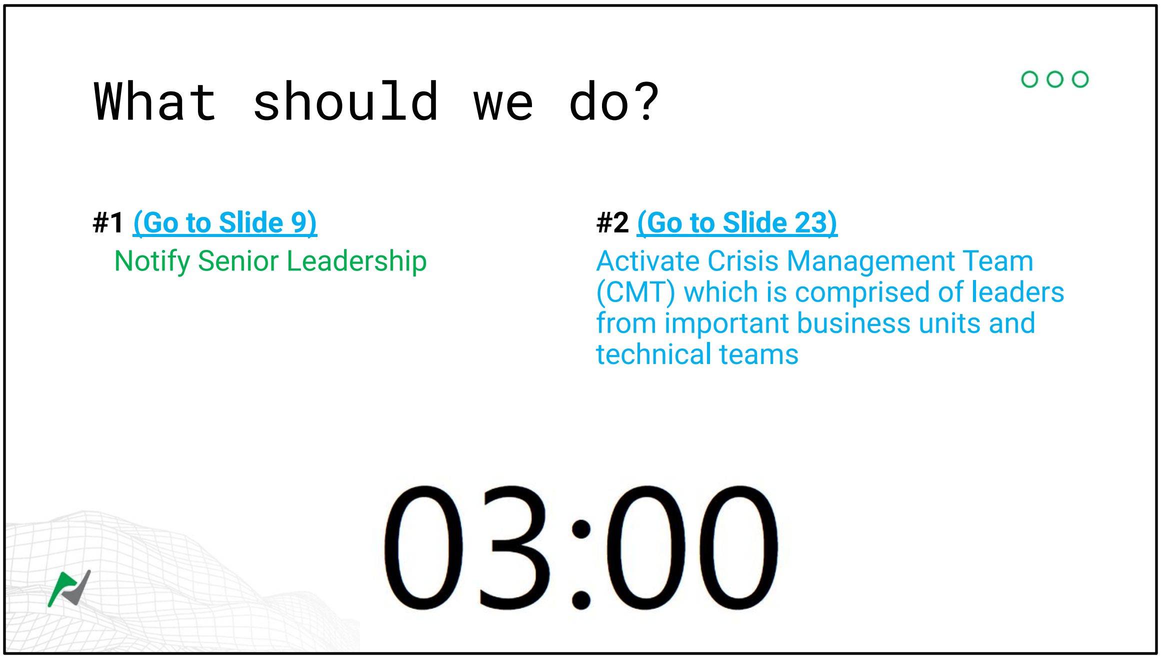
It started like a normal day

It’s the week of the Catalina Wine Mixer, which we sponsor. What started as a normal day starts to go sideways when our SOC analysts begin to see requests being made to a questionable domain.

Their analysis determines that the domain, while not known to be malicious, was only created a few hours ago and appears to be just a random set of characters. During the analysis, the number of requests made to this domain has steadily increased impacting approximately 1% of our user-based assets.

The security team puts a block in place for the domain only to see requests made to other unique domains.

What should we do?



What should we do?

#1 **(Go to Slide 9)**
Notify Senior Leadership

#2 **(Go to Slide 23)**
Activate Crisis Management Team (CMT) which is comprised of leaders from important business units and technical teams

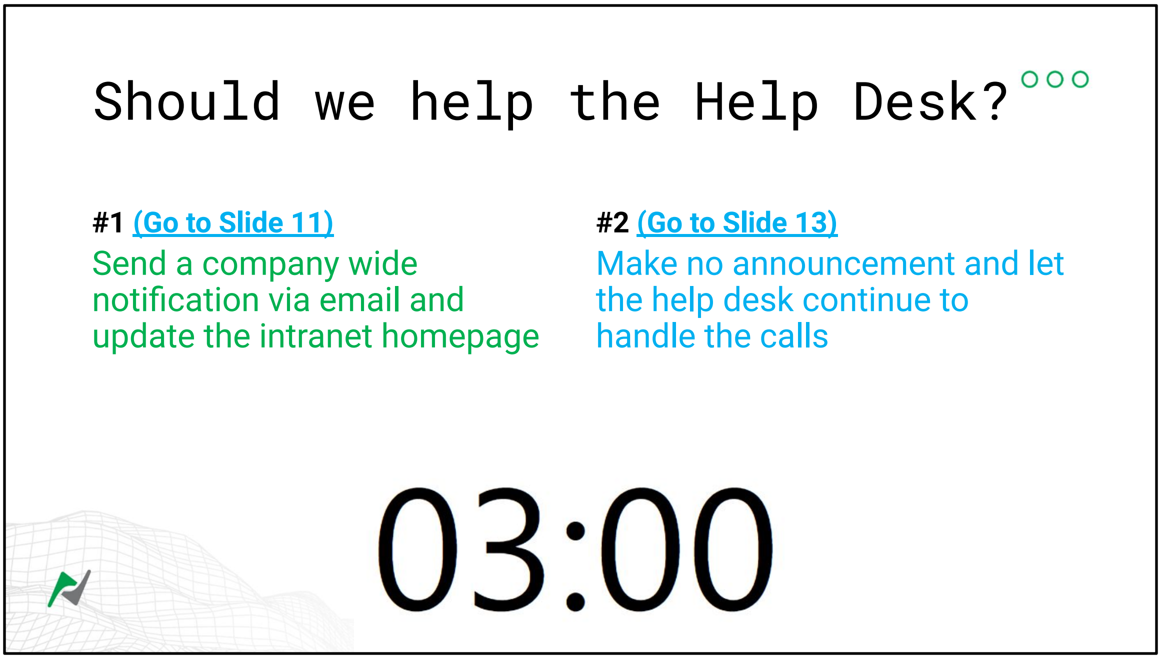
03:00

Senior Leadership

Senior Leadership, still stinging from the last breach, decides to shut down the internet. With the Internet down the company core business is offline, costing the organization $10k per hour due to lack of production.

In addition, IT helpdesk becomes inundated with complaints and questions from users. The Help Desk Manager attempting to stem the tide asks us to publish a company wide notification.

Should we help the help desk?



Should we help the Help Desk?

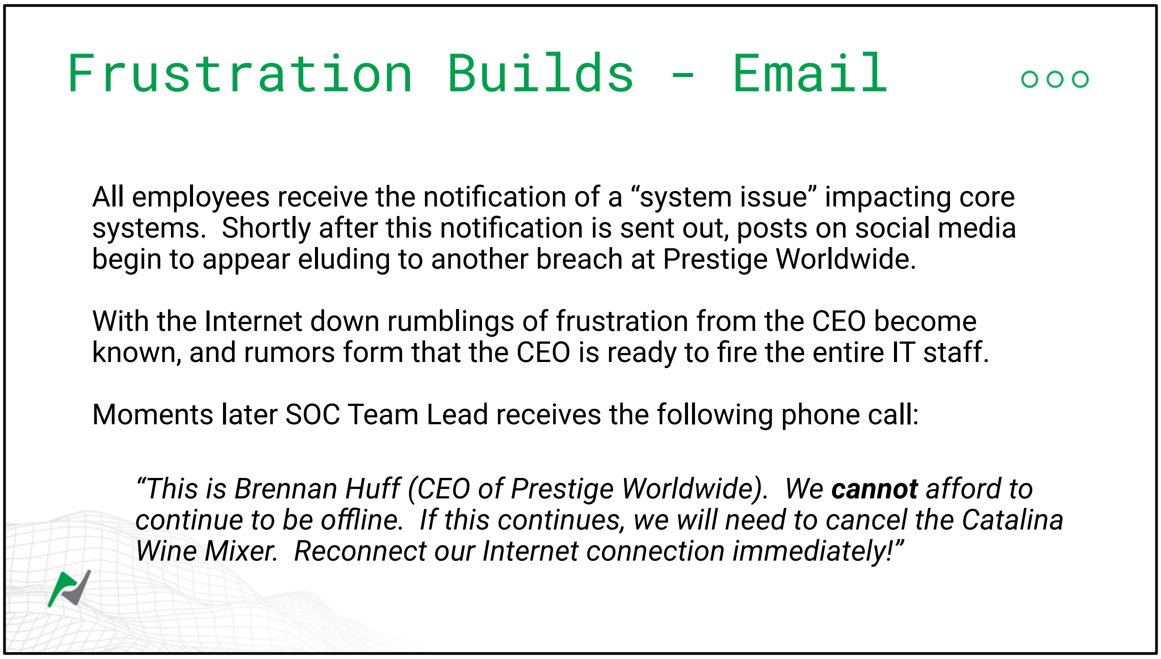
#1 (Go to Slide 11)

Send a company wide notification via email and update the intranet homepage

#2 (Go to Slide 13)

Make no announcement and let the help desk continue to handle the calls

03:00



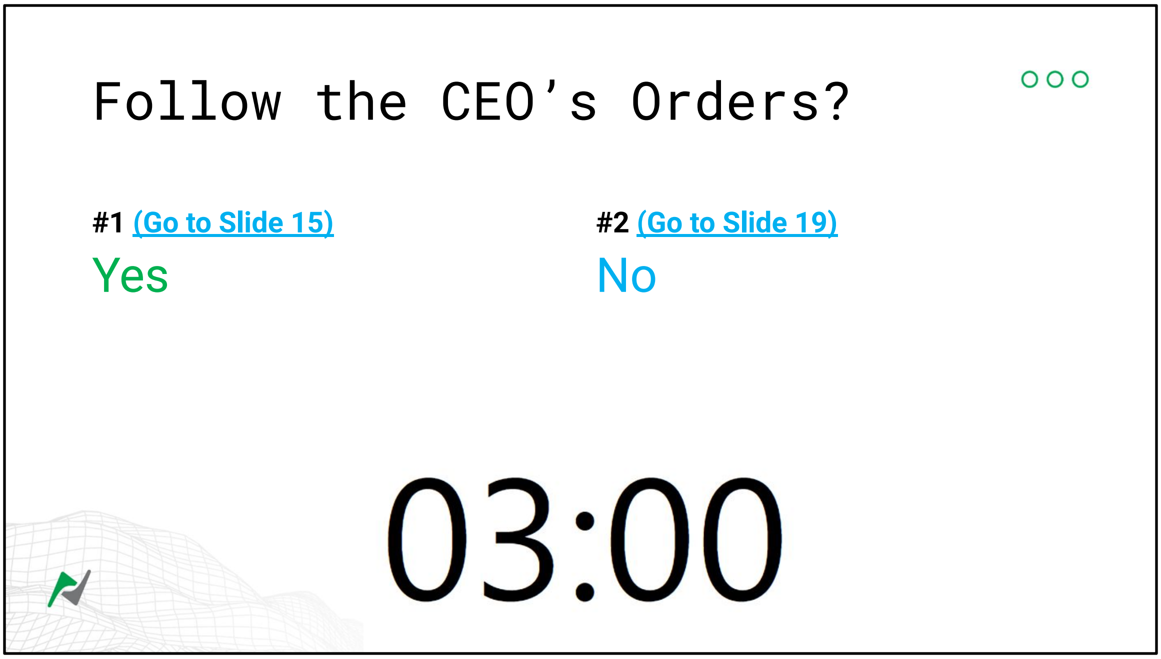
Frustration Builds - Email

All employees receive the notification of a “system issue” impacting core systems. Shortly after this notification is sent out, posts on social media begin to appear eluding to another breach at Prestige Worldwide.

With the Internet down rumblings of frustration from the CEO become known, and rumors form that the CEO is ready to fire the entire IT staff.

Moments later SOC Team Lead receives the following phone call:

> *“This is Brennan Huff (CEO of Prestige Worldwide). We **cannot** afford to continue to be offline. If this continues, we will need to cancel the Catalina Wine Mixer. Reconnect our Internet connection immediately!”*



Follow the CEO’s Orders?

#1 (Go to Slide 15)

Yes

#2 (Go to Slide 19)

No

03:00

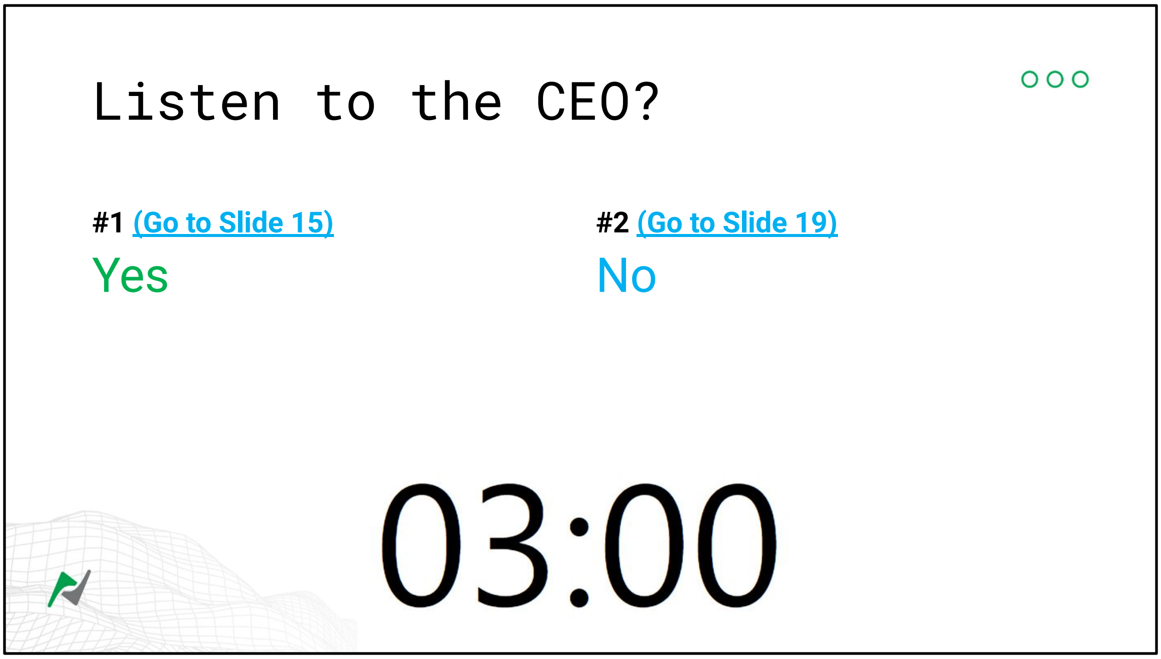
Frustration Builds - Silence

Without formal notification, the users are unable to perform their tasks and begin to gossip. Posts begin to appear on social medial eluding to another cyber incident at the company.

With the Internet down, rumblings of frustration from the CEO become known, and rumors form that the CEO is ready to fire the entire IT staff.

Moments later SOC Team Lead receives the following phone call:

> *"This is Brennan Huff (CEO of Prestige Worldwide). We* ***cannot*** *afford to continue to be offline. If this continues, we will need to cancel the Catalina Wine Mixer. Reconnect our Internet connection immediately!"*



Listen to the CEO?

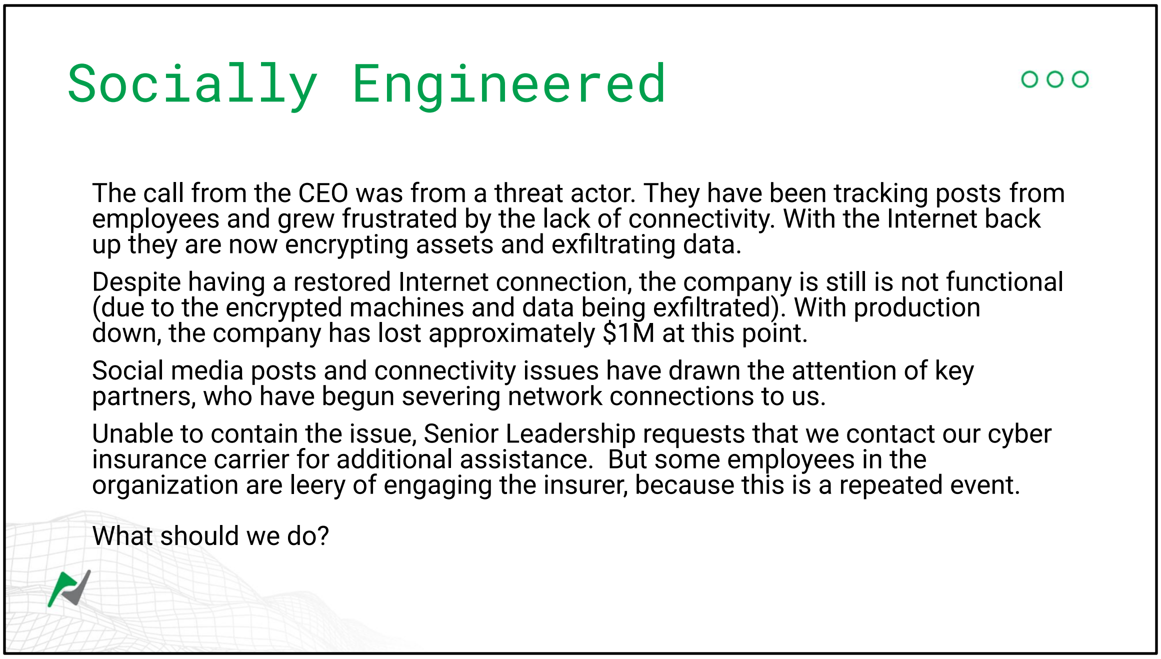
#1 (Go to Slide 15)

Yes

#2 (Go to Slide 19)

No

03:00



Socially Engineered

The call from the CEO was from a threat actor. They have been tracking posts from employees and grew frustrated by the lack of connectivity. With the Internet back up they are now encrypting assets and exfiltrating data.

Despite having a restored Internet connection, the company is still is not functional (due to the encrypted machines and data being exfiltrated). With production down, the company has lost approximately $1M at this point.

Social media posts and connectivity issues have drawn the attention of key partners, who have begun severing network connections to us.

Unable to contain the issue, Senior Leadership requests that we contact our cyber insurance carrier for additional assistance. But some employees in the organization are leery of engaging the insurer, because this is a repeated event.

What should we do?

Call cyber insurance carrier?

#1 (Go to Slide 17)

Yes

#2 (Go to Slide 18)

No

03:00

Insurance to the Rescue

Our cyber insurance carrier helps us engage an incident response (IR) team. The IR team begins to triage and forensic analysis on our systems. With their assistance they can determine the malicious file and remove it from our machines. However, that investigation took 24 hours of which production was down.

A minimal number of systems were encrypted but the IR team was able to help us mitigate the threat. The few encrypted machines were restored from backup successfully and we did not appear to lose any customer or proprietary information

With a second incident behind us even more positive change is implemented throughout our network but there is a sense that things could have been worse had we made different decisions along the way.

But most importantly, WE SAVED THE CATALINA WINE MIXER!!

(Go to Slide 34)

End of Days

With the Internet connection restored and without experienced incident response assistance, the hackers were eventually able to encrypt almost all desktops and servers. The cybersecurity insurance team was called a few days later, but by that point it was too late. The only option was to pay the ransom which was 25% of our annual revenue ($25M). In addition, the hackers were able to exfiltrate proprietary information on our customers and partners and post it on the dark web.

IT and cybersecurity teams were fired, and the company paid another $20M to an outside firm to outsource all IT and cybersecurity work.

After the second security incident in the last two years, the company was not able to recover, having lost the faith of our key business partners and customers. With all the lost revenue the company closes its doors 3 months later.

And the Catalina Wine Mixer never happens again.

(Go to Slide 34)

The Nightmare Continues

With the internet connection still down the company still is not functional. Production has been down for two hours.

Social media posts and connectivity issues have drawn the attention of key partners, who have begun severing network connections to us.

Unable to contain the issue, Senior Leadership requests that we contact our cyber insurance carrier for additional assistance. However, some employees inside the organization are leery of contacting our insurance carrier due to this being a second event.

Should we contact our insurer?

Call cyber insurance carrier?

#1 (Go to Slide 21)

Yes

#2 (Go to Slide 22)

No

03:00

Insurance to the Rescue

Our cyber insurance carrier helps us engage an incident response (IR) team. The IR team begins to triage and perform forensic analysis on our systems. With their assistance they can determine the malicious files and remove them from our machines. However, that investigation took 24 hours, all of which production was down.

A minimal number of systems were encrypted but the IR team was able to help us mitigate the threat. The few encrypted machines were restored from backup successfully, and we did not appear to lose any customer or proprietary information

With a second incident behind us even more positive change is implemented throughout our network, but there is a sense that things could have been worse if we had made different decisions along the way.

But most importantly, WE SAVED THE CATALINA WINE MIXER!!

(Go to Slide 34)

End of Days

With the Internet connection restored, and without experienced incident response assistance, the hackers were eventually able to encrypt almost all desktops and servers. The cybersecurity insurance team was called a few days later, but by that point it was too late. The only option was to pay the ransom which was 25% of our annual revenue ($25M). In addition, the hackers were able to exfiltrate proprietary information on our customers and partners and post it on the dark web.

IT and cybersecurity teams were fired, and the company paid another $20M to an outside firm to outsource all IT and cybersecurity work.

After the second security incident in the last two years, the company was not able to recover, having lost the faith of our key business partners and customers. With all the lost revenue the company closes its doors 3 months later.

And the Catalina Wine Mixer never happens again.

(Go to Slide 34)

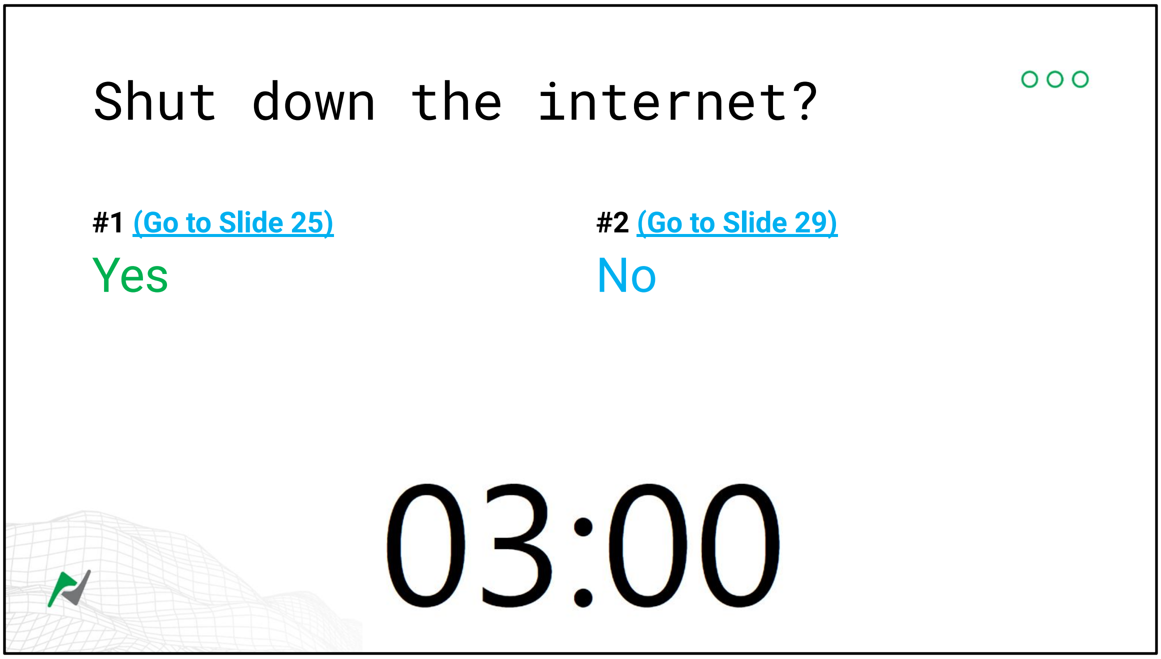
Crisis Management Team

The Crisis Management Team (CMT) takes over and decides to contact our security incident response (IR) team under retainer. The IR team implements a block rule for any uncategorized and newly formed domains and isolates all devices calling out to it.

But it is too late. Machines are being encrypted.

The CMT discusses shutting down the Internet connection to prevent further encryption, but our company needs this connection to produce and ship product.

What do we do?



Shut down the internet?

#1 (Go to Slide 25)

Yes

#2 (Go to Slide 29)

No

03:00

Fingers in the Dam

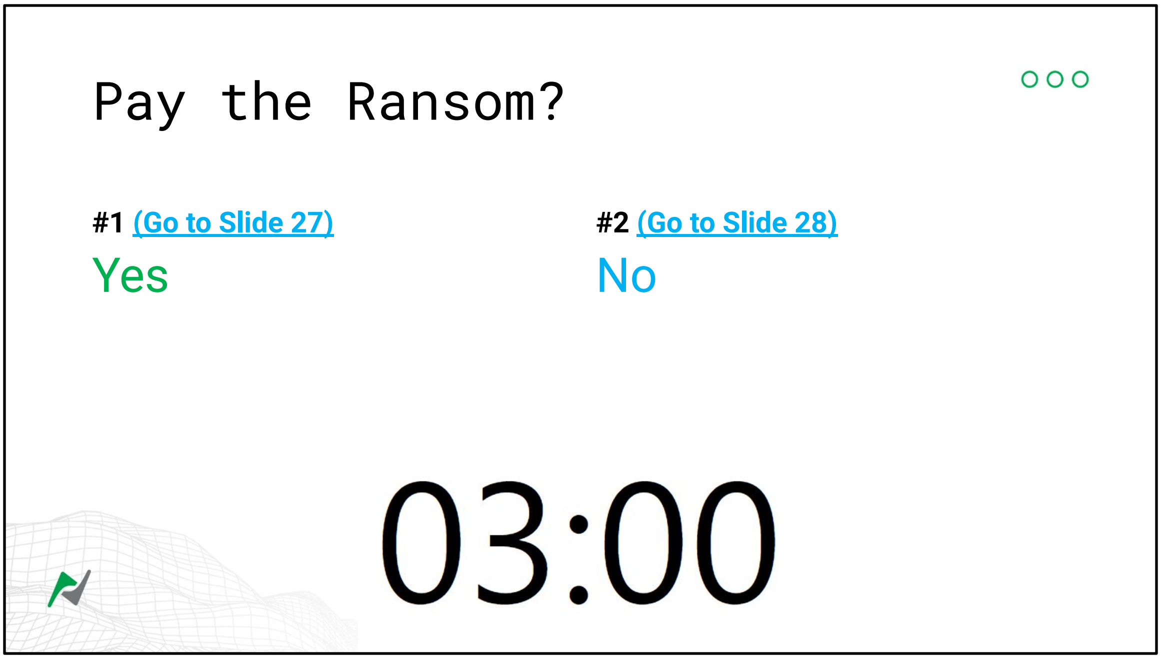
With the internet pipe down, we see fewer new devices being encrypted but production has stopped and without production we are losing $10K per hour.

We also have approximately 1,000 user devices and some backup servers compromised.

A ransom equal to 20% of our company revenue is requsted with a 24-hour deadline to comply. Our brand is being trashed by our partners and the public.

The CMT mulls paying the ransom.

Should we?



Pay the Ransom?

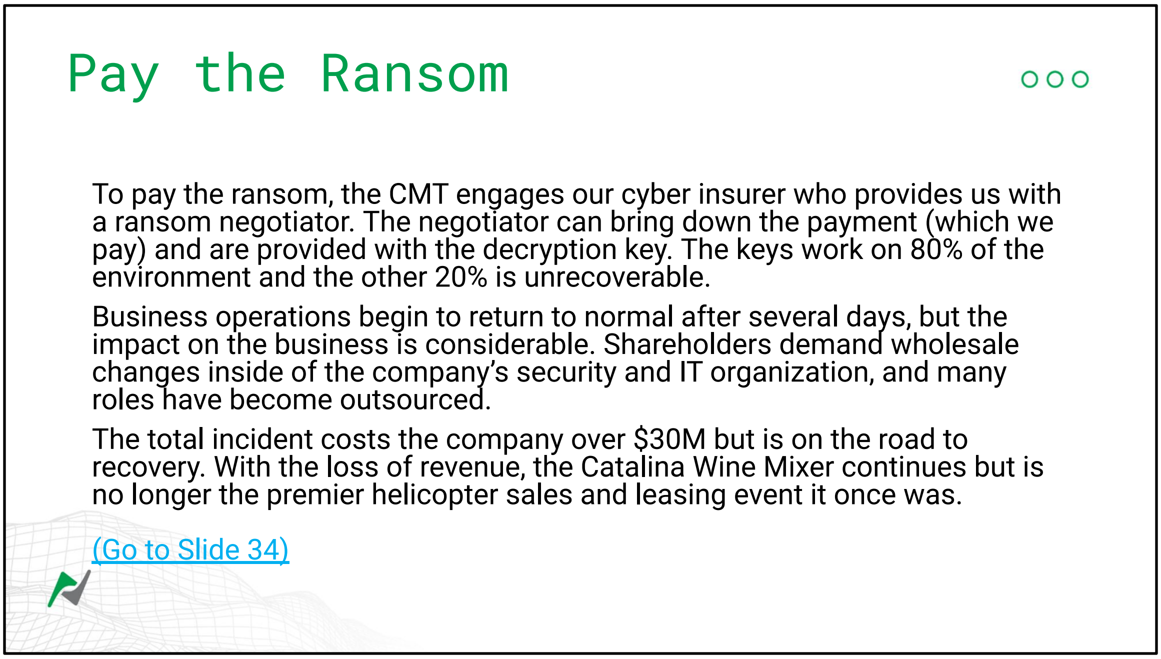
#1 (Go to Slide 27)

Yes

#2 (Go to Slide 28)

No

03:00



Pay the Ransom

To pay the ransom, the CMT engages our cyber insurer who provides us with a ransom negotiator. The negotiator can bring down the payment (which we pay) and are provided with the decryption key. The keys work on 80% of the environment and the other 20% is unrecoverable.

Business operations begin to return to normal after several days, but the impact on the business is considerable. Shareholders demand wholesale changes inside of the company's security and IT organization, and many roles have become outsourced.

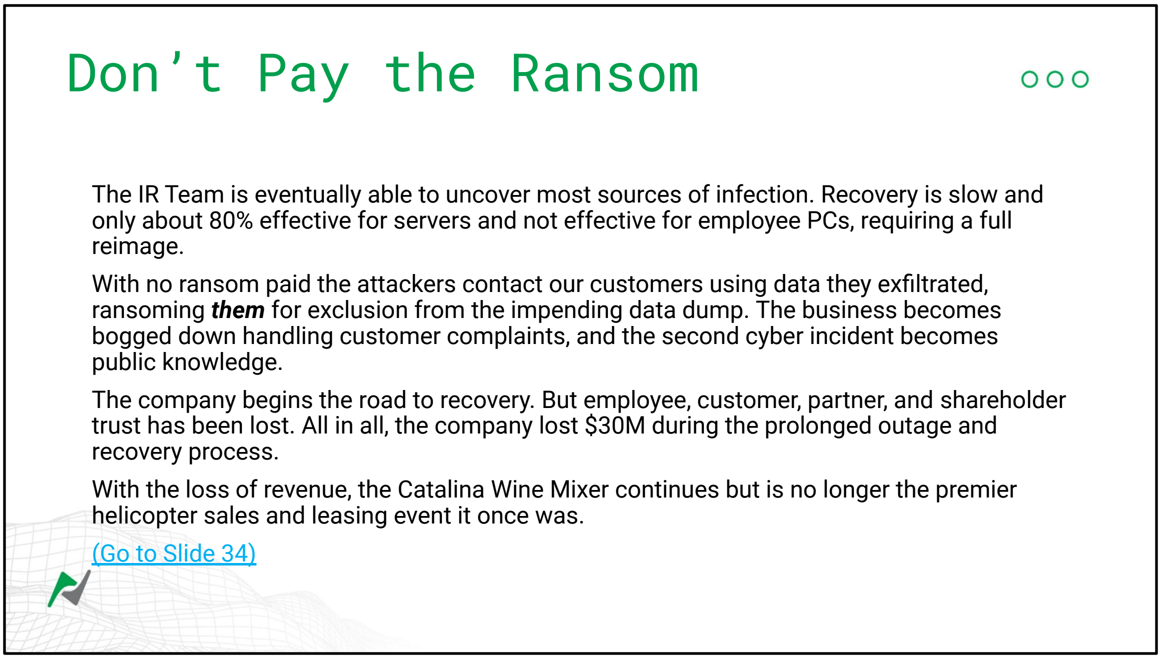
The total incident costs the company over $30M but is on the road to recovery. With the loss of revenue, the Catalina Wine Mixer continues but is no longer the premier helicopter sales and leasing event it once was.

(Go to Slide 34)

Buying large amounts of crypto takes time. Crypto is math and the math takes time to process especially for huge moves. Monero has less movement than BitCoin and takes more time as a result.

Many gangs will have you pay the origin provider directly and the payments are made in two parts.

Additional challenges might come in the form of penalties by the US government (Department of the Treasury's Office of Foreign Assets Control) for payment to sanctioned nations.



Don’t Pay the Ransom

The IR Team is eventually able to uncover most sources of infection. Recovery is slow and only about 80% effective for servers and not effective for employee PCs, requiring a full reimage.

With no ransom paid the attackers contact our customers using data they exfiltrated, ransoming ***them*** for exclusion from the impending data dump. The business becomes bogged down handling customer complaints, and the second cyber incident becomes public knowledge.

The company begins the road to recovery. But employee, customer, partner, and shareholder trust has been lost. All in all, the company lost $30M during the prolonged outage and recovery process.

With the loss of revenue, the Catalina Wine Mixer continues but is no longer the premier helicopter sales and leasing event it once was.

(Go to Slide 34)

Many ransomware attacks result in the usage of custom or modified encrypting engines. These engines, many times, corrupt files or specific types of files.

Double extortion (DE) is a ransomware attack technique in which cybercriminals not only encrypt a victim's files but also threaten to publish or sell the stolen data unless a ransom is paid. In other words, the attackers demand payment for both decrypting the victim's data and for not disclosing it publicly or to third parties.

Triple extortion is an extension of DE by which the attackers either: a) contact the customers of the business and attempt to extort them, and/or b) threaten to launch a DDoS attack against the organization’s web infrastructure.

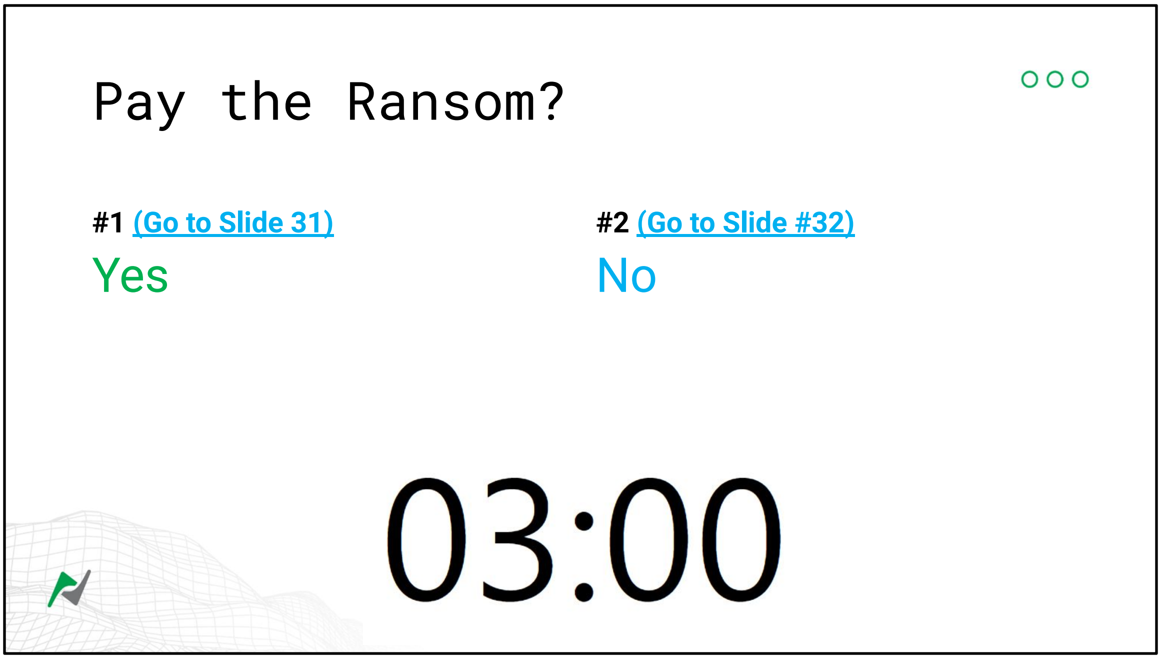
Fingers in the Dam

Devices continue to become encrypted at a rate beyond IT’s ability to resolve and all other attempts to contain the propagation have failed.

A ransom equal to 20% of our company revenue ($20M) is also requested with a 24-hour deadline to comply.

Our brand is being trashed by our partners and the public. The CMT mulls paying the ransom.

Should we?



Pay the Ransom?

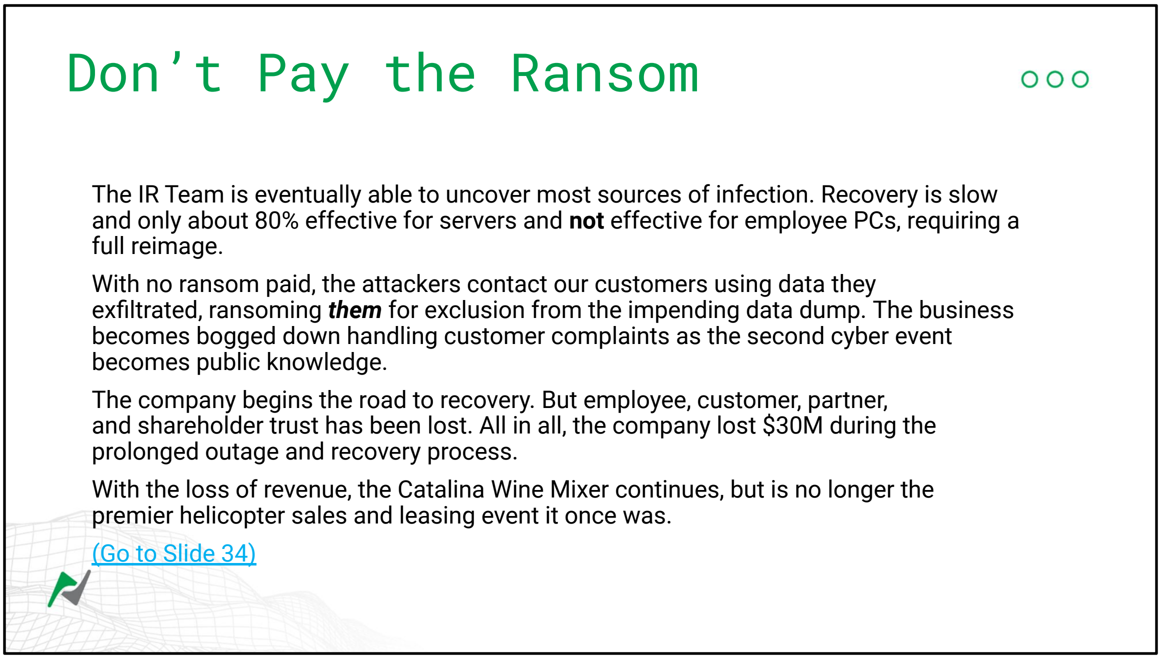
#1 (Go to Slide 31)

Yes

#2 (Go to Slide #32)

No

03:00



Don’t Pay the Ransom

The IR Team is eventually able to uncover most sources of infection. Recovery is slow and only about 80% effective for servers and **not** effective for employee PCs, requiring a full reimage.

With no ransom paid, the attackers contact our customers using data they exfiltrated, ransoming ***them*** for exclusion from the impending data dump. The business becomes bogged down handling customer complaints as the second cyber event becomes public knowledge.

The company begins the road to recovery. But employee, customer, partner, and shareholder trust has been lost. All in all, the company lost $30M during the prolonged outage and recovery process.

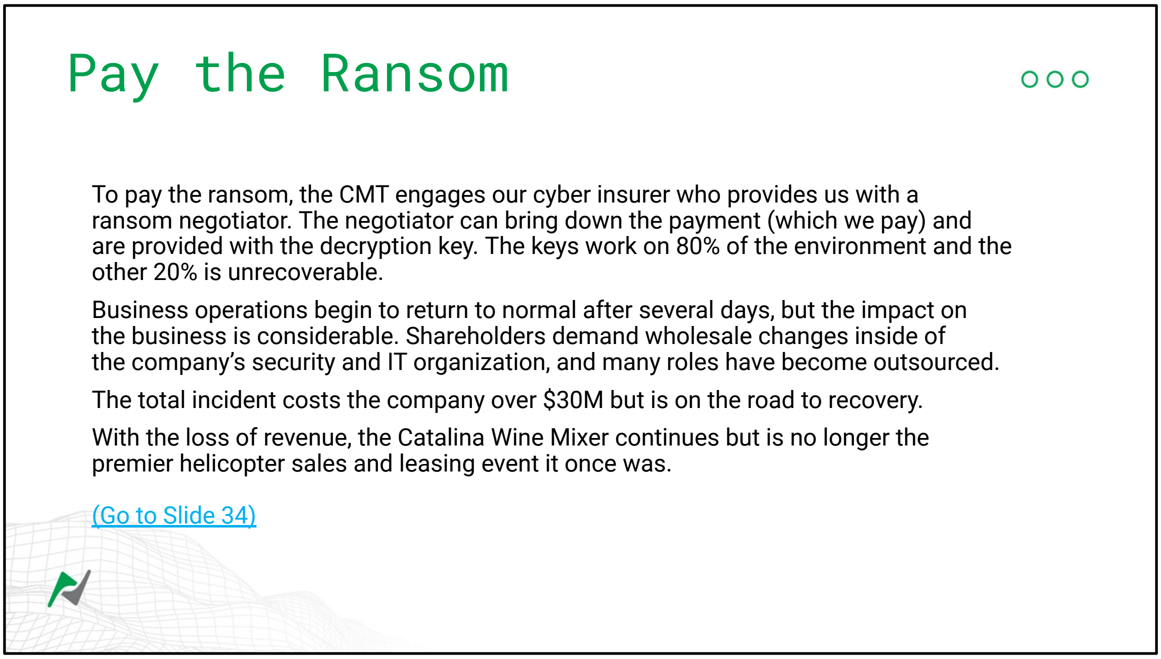
With the loss of revenue, the Catalina Wine Mixer continues, but is no longer the premier helicopter sales and leasing event it once was.

(Go to Slide 34)

Many ransomware attacks result in the usage of custom or modified encrypting engines. These engines, many times, corrupt files or specific types of files.

Double extortion (DE) is a ransomware attack technique in which cybercriminals not only encrypt a victim's files but also threaten to publish or sell the stolen data unless a ransom is paid. In other words, the attackers demand payment for both decrypting the victim's data and for not disclosing it publicly or to third parties.

Triple extortion is an extension of DE by which the attackers either: a) contact the customers of the business and attempt to extort them, and/or b) threaten to launch a DDoS attack against the organization’s web infrastructure.



Pay the Ransom

To pay the ransom, the CMT engages our cyber insurer who provides us with a ransom negotiator. The negotiator can bring down the payment (which we pay) and are provided with the decryption key. The keys work on 80% of the environment and the other 20% is unrecoverable.

Business operations begin to return to normal after several days, but the impact on the business is considerable. Shareholders demand wholesale changes inside of the company’s security and IT organization, and many roles have become outsourced.

The total incident costs the company over $30M but is on the road to recovery.

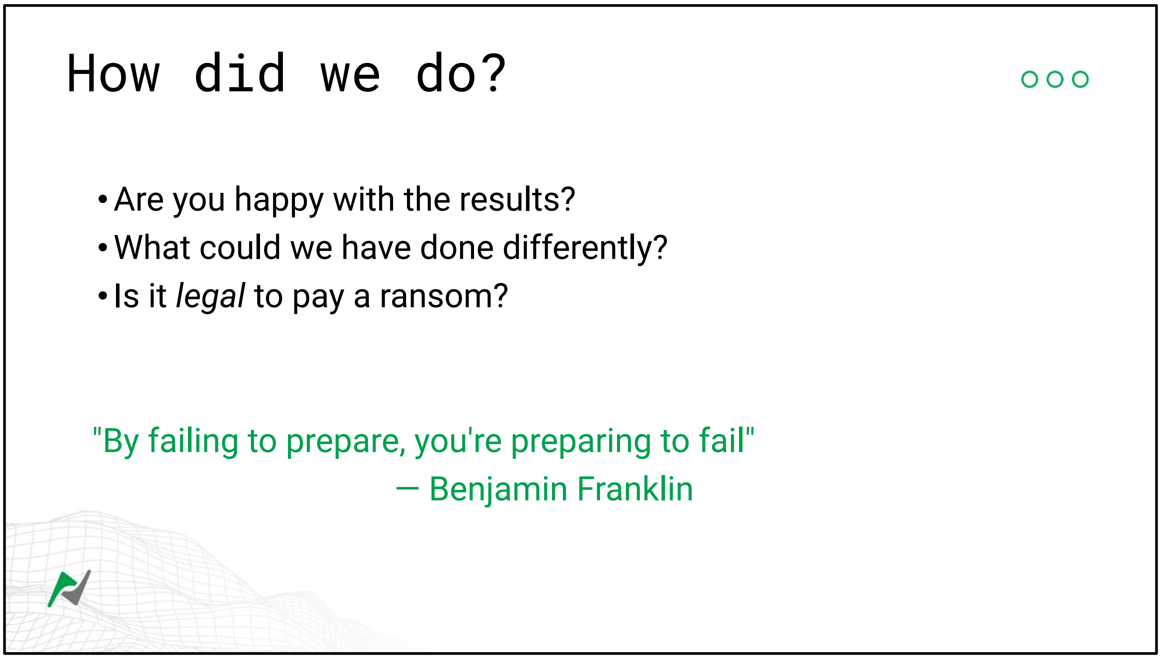
With the loss of revenue, the Catalina Wine Mixer continues but is no longer the premier helicopter sales and leasing event it once was.

(Go to Slide 34)

Buying large amounts of crypto takes time. Crypto is math and the math takes time to process especially for huge moves. Monero has less movement than BitCoin and takes more time as a result.

Many gangs will have you pay the origin provider directly and the payments are made in two parts.

Additional challenges might come in the form of penalties by the US government (Department of the Treasury’s Office of Foreign Assets Control) for payment to sanctioned nations.

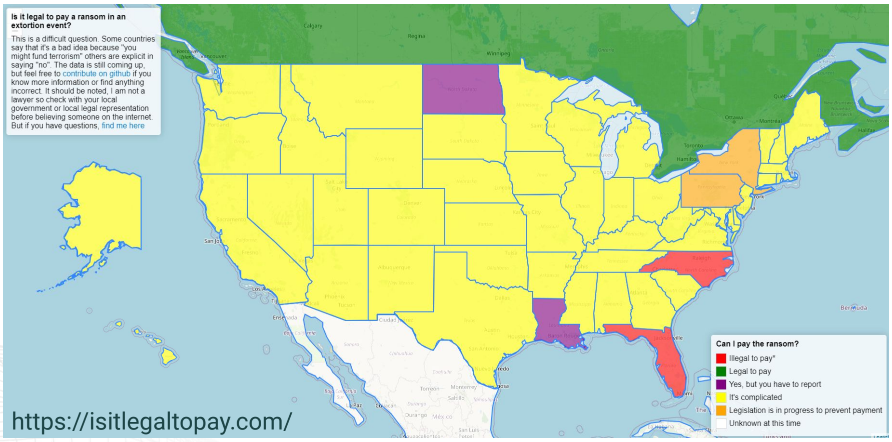


How did we do?

- 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?



Is it legal to pay a ransom in an extortion event?

This is a difficult question. Some countries say that it's a bad idea because "you might fund terrorism" others are explicit in saying "no". The data is still coming up, but feel free to contribute on github if you know more information or find anything incorrect. It should be noted, I am not a lawyer so check with your local government or local legal representation before believing someone on the internet. But if you have questions, find me here

Can I pay the ransom?

- 🟥 Illegal to pay*
- 🟩 Legal to pay
- 🟪 Yes, but you have to report
- 🟨 It's complicated
- 🟧 Legislation is in progress to prevent payment
- ⬜ Unknown at this time

https://isitlegaltopay.com/

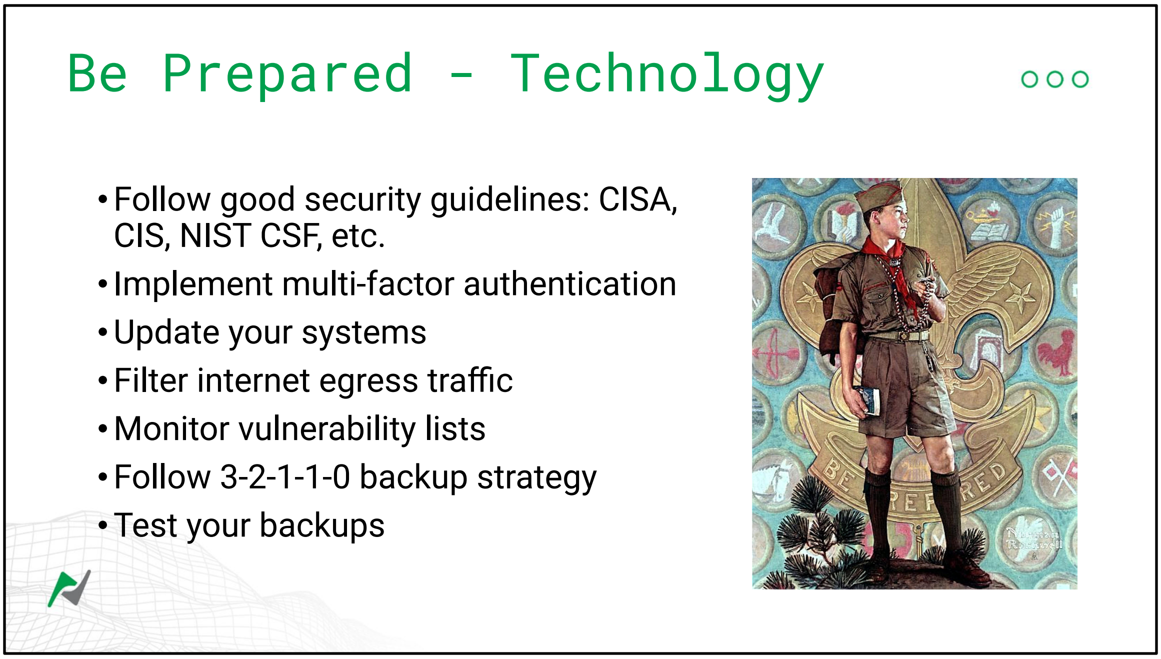
<u>N.D. Cent. Code §§ 51-30-01 et seq.</u>

Beginning August 1, 2021, when a cybersecurity event occurs, a licensee is required to report this event within 3 business days to the North Dakota Insurance Commissioner's office.

A licensee must report if:
North Dakota is the licensee's state of domicile, and it is reasonably likely any consumer could be materially harmed, or the licensee's operations are materially harmed.
The licensee reasonably believes the nonpublic information involved is of **two hundred fifty** or more consumers and:
-A cybersecurity event impacts the licensee for which notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body pursuant to any state or federal law.
-A cybersecurity event has a reasonable likelihood of materially harming any consumer residing in North Dakota.

Be Prepared - Planning

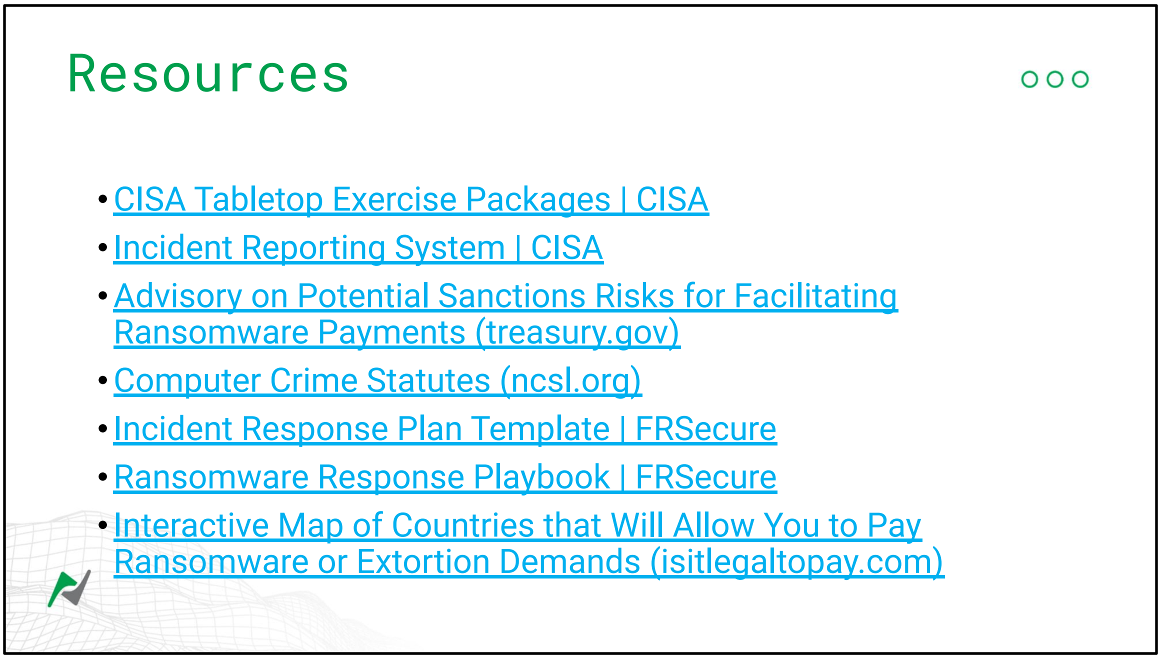
- Educate your employees
- Understand your environment/data
- Store incident response plan off-network
- Have a communications plan
- Know your cybersecurity insurance and law enforcement contacts
- Consider cybersecurity IR service retainer
- Complete a risk assessment



Be Prepared - Technology

- Follow good security guidelines: CISA, CIS, NIST CSF, etc.
- Implement multi-factor authentication
- Update your systems
- Filter internet egress traffic
- Monitor vulnerability lists
- Follow 3-2-1-1-0 backup strategy
- Test your backups

CISA = Cybersecurity and Infrastructure Security Agency
CIS = Center for Internet Security
NIST CSF = National Institute of Standards and Technology Cyber Security Framwork



Resources

- 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)

NETWORKCENTER
INCORPORATED

Thanks for Playing!

Mike Pagán

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