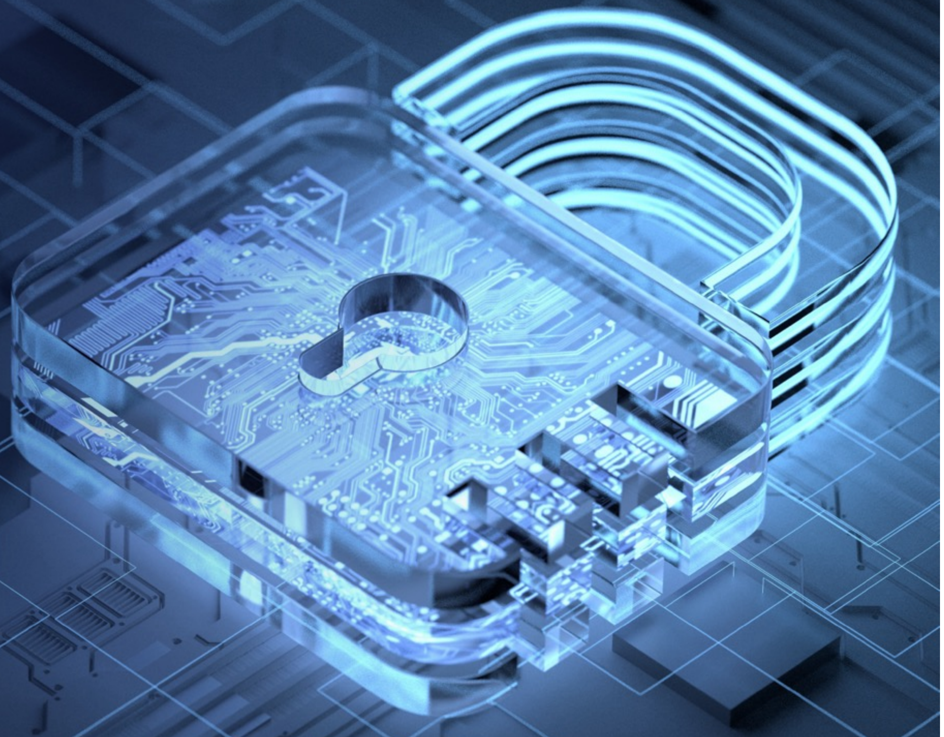
11:11 SYSTEMS

COMPROMISED DATA RECOVERY

Table-Top Exercise

It's Everyone's Business!



Oct 2, 2024

Compromised Data / Cyber Incident – Risk Level (High / Very High)

Inherent Risk Level: High / Very High

Threat: Malicious security attack / cyberattack (externally or internally)

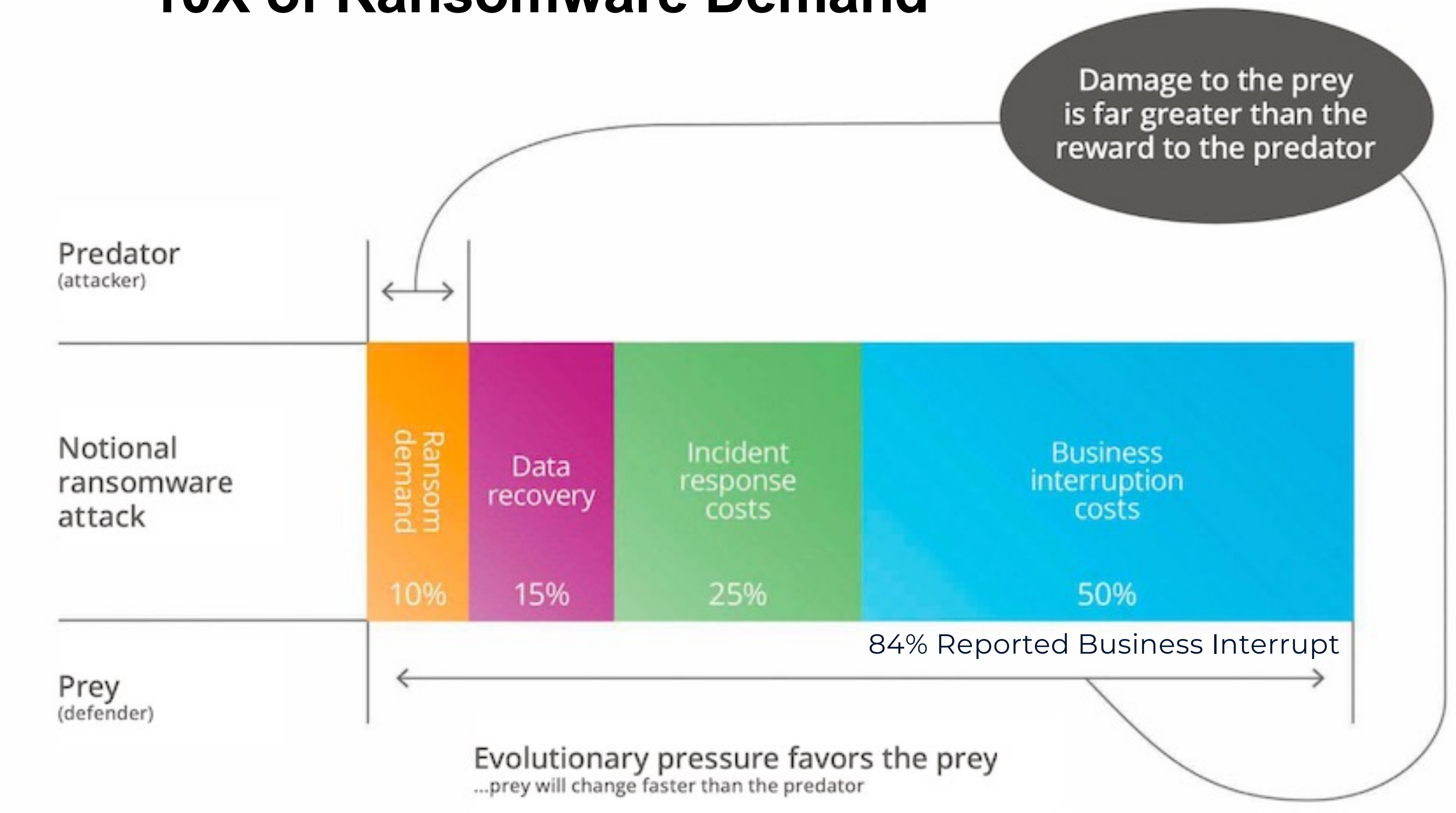
Threat Likelihood (High): Multiple attack vectors

- Internal / Insider (rogue employee / contractor, privileged access, etc.)
  Network connected, understands current defenses, IT environment awareness, etc.
- External / Threat Actor (black hat hacker, bad actor, etc.)
  Highly intelligent, undetected intruder / dwell time, plan a targeted attack, etc.
- External / Malware (ransomware, data-wiping, keylogging, trojan horse, worm, etc.)
  Ever-changing malware (detection tools lagging-behind), zero-day attack, etc.

Threat Impact (V. High): Compromised vital data (both, production & backup data)

True Cost of a Compromised Data Event

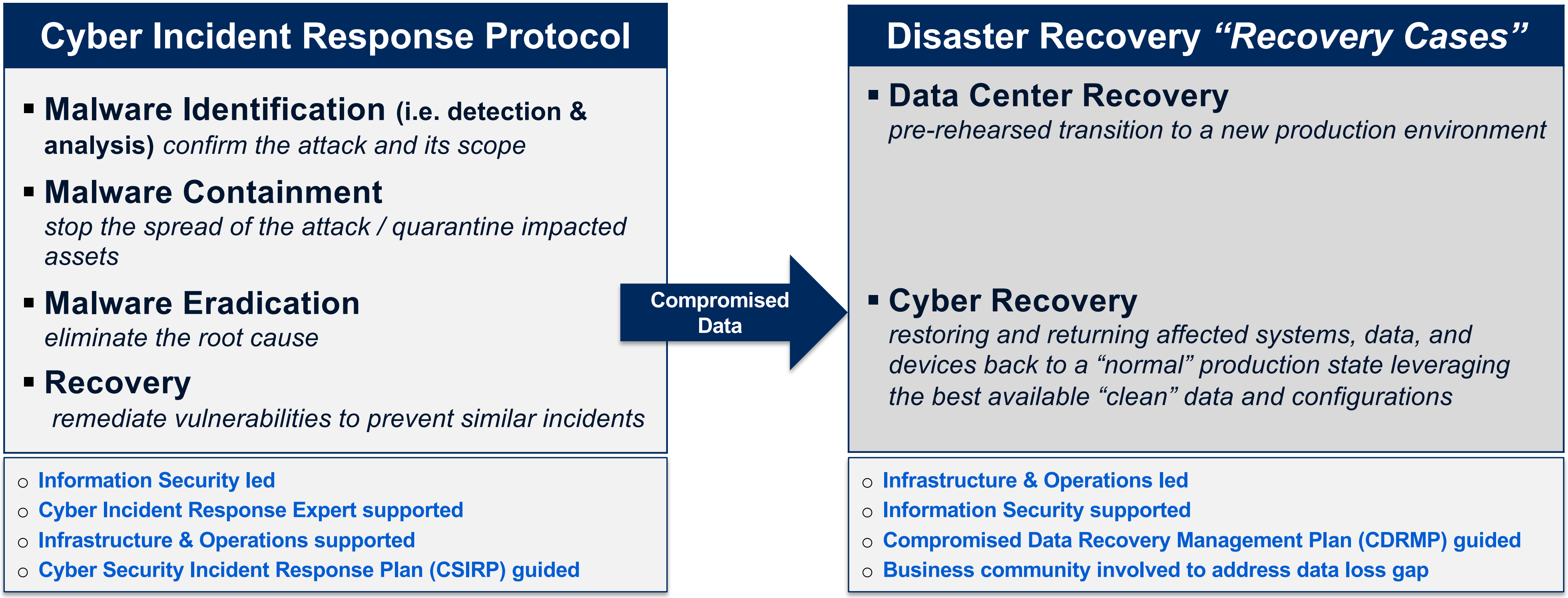
10X of Ransomware Demand


Damage to the prey is far greater than the reward to the predator
Predator
(attacker)
Notional ransomware attack
Ransom demand
10%
Data recovery
15%
Incident response costs
25%
Business interruption costs
50%
84% Reported Business Interrupt
Prey
(defender)
Evolutionary pressure favors the prey
...prey will change faster than the predator

Disaster Recovery vs Cyber Compromised Data Recovery

	Disaster Recovery	Compromised Data Recovery
Triggering Event:	Datacenter compromising event e.g., fire, flood, power loss	Data compromising event e.g., ransomware, wiper malware, rogue employee
Production Impact:	Production shift to a "new place" Production shift to a pre-determined Disaster Recovery site	Data recovery ”in place” Malware-free data is re-patriated back to the production environment
Data Currency:	Most current replica or backup data available at the Disaster Recovery site	Most currently available "clean" backup data
Recovery Objectives:	✓ RTOs ✓ RPOs Assumes successful prior test experiences with a proven technology	X RTOs — Recovery time is predicated on duration of malware clearing activities; potentially a week or more ? RPOs — Data loss can be days, weeks, or more depending on backup compromising actions of perpetrators

There are multiple workstreams within a Cyber Incident Response protocol …… and a linkage to DR is essential



Cyber Incident Response Protocol

- **Malware Identification (i.e. detection & analysis)** *confirm the attack and its scope*
- **Malware Containment** *stop the spread of the attack / quarantine impacted assets*
- **Malware Eradication** *eliminate the root cause*
- **Recovery** *remediate vulnerabilities to prevent similar incidents*

- ○ **Information Security led**
- ○ **Cyber Incident Response Expert supported**
- ○ **Infrastructure & Operations supported**
- ○ **Cyber Security Incident Response Plan (CSIRP) guided**

Disaster Recovery *"Recovery Cases"*

- **Data Center Recovery** *pre-rehearsed transition to a new production environment*
- **Cyber Recovery** *restoring and returning affected systems, data, and devices back to a "normal" production state leveraging the best available "clean" data and configurations*

- ○ **Infrastructure & Operations led**
- ○ **Information Security supported**
- ○ **Compromised Data Recovery Management Plan (CDRMP) guided**
- ○ **Business community involved to address data loss gap**

11:11 SYSTEMS

11:11 Systems' Compromised Data Recovery Good Practice Framework

Identify ***Vital Data Asset Requirements***	**Protect** ***Data Protection / Backup Methods***	**Respond** ***Compromised Data Incident Response***	**Recover** ***Compromised Data Recovery Execution***
VDA Identification *Assessment Criteria and Process*	**Unchangeable Data** *Immutability*	**Response Scope** *Compromised Data Recovery Requirements*	**Clean Room Enablement** *Isolated Recovery Environment*
VDA Interdependencies *Workflow Requirements*	**Unreadable Data** *Encryption*	**Response Plan** *Compromised Data Incident Response & Data Recovery Management Plans*	**Clean Data Identification** *Immutable Backups Forensics Analysis*
VDA Requirements *Approved Scope*	**Inaccessible Data** *Authentication Controls*	**Response Tracks** *Compromised Data Recovery Options*	**Clean Data Recovery** *Compromised Data Recovery Execution*
VDA Technical Profile *Technical Recovery Requirements*	**Unreachable Data** *Air Gapped Cyber Data Vault*	**Response Advisors/Break Glass** ATOD Expertise to Leverage for Incident Response, Coaching & DFIR	**Cyber Recovery Readiness** *Recovery Lifecycle Management*
VDA Data Profile *Data Protection Requirements*	**Uncompromised Data** *Anomaly Detection*	**Response Exercises** *Response Plan, Tracks, and Options*	**Cyber Recovery Tests** *Recovery Capabilities Verification*

Vital Data Assets (VDAs) are an organization's "must-have" / "mission-enabling" data requiring advanced levels of protection and recovery preparedness

What is Your Organization's Confidence Level You Can
Manage Through and Recover From a Ransomware Event?

Exercise Ground Rules

- Suspend REALITY for the next 60 minutes!

  Accept the Scenario “as is”

  What is discussed here, stays here!

- Focus on what your organization does / doesn’t have in place today, not fixing the scenario

- This is not a TEST – no right or wrong answers!

- The focus is on sharing, learning and increasing awareness for all in the room

Stage Setting

- Underlying scenario: data compromising cyber intrusion (Ransomware)

- Situations like this demand that you respond quickly and address diverse challenges

- This exercise will touch on issues related to technology, business interruption, and more

- The exercise timeline will span multiple days following an initial attack

Let’s Begin!

Start of Day 1

Oct 3, 2024

An IT issue arises

Day 1

8:30AM

9.05AM

9:30AM

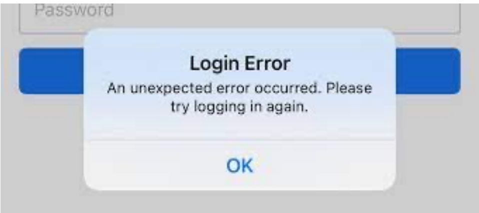
10:00AM

11:00AM

12:00PM

6:00PM

- After multiple attempts, several users can’t log into the network; what would they do?



Password

Login Error

An unexpected error occurred. Please try logging in again.

- What action would IT take?

Situation Alert!

Day 1

8:30AM

9.30AM

10:00AM

11:00AM

12:00PM

6:00PM

- The issue appears to be spreading with larger numbers of personnel reporting access and availability issues
- Infrastructure and Operations (I&O) team members have also been disrupted with some unable to work due to access issues
- **Security sees indicators of compromise / potentially malicious activity**

Pause for Discussion – Round 1

- What is the most important concern?
- Is there a process for handling this situation?
- Are any escalations required, and to whom?
- What departments may be impacted by the disruption?
- What if any communications are needed? (What? How? Whom?)

Day 1

8:30AM

9:30AM

10:00AM

11:45AM

12:00PM

6:00PM

IN CASE OF CDR

Initial Co

Day 1

8:30AM

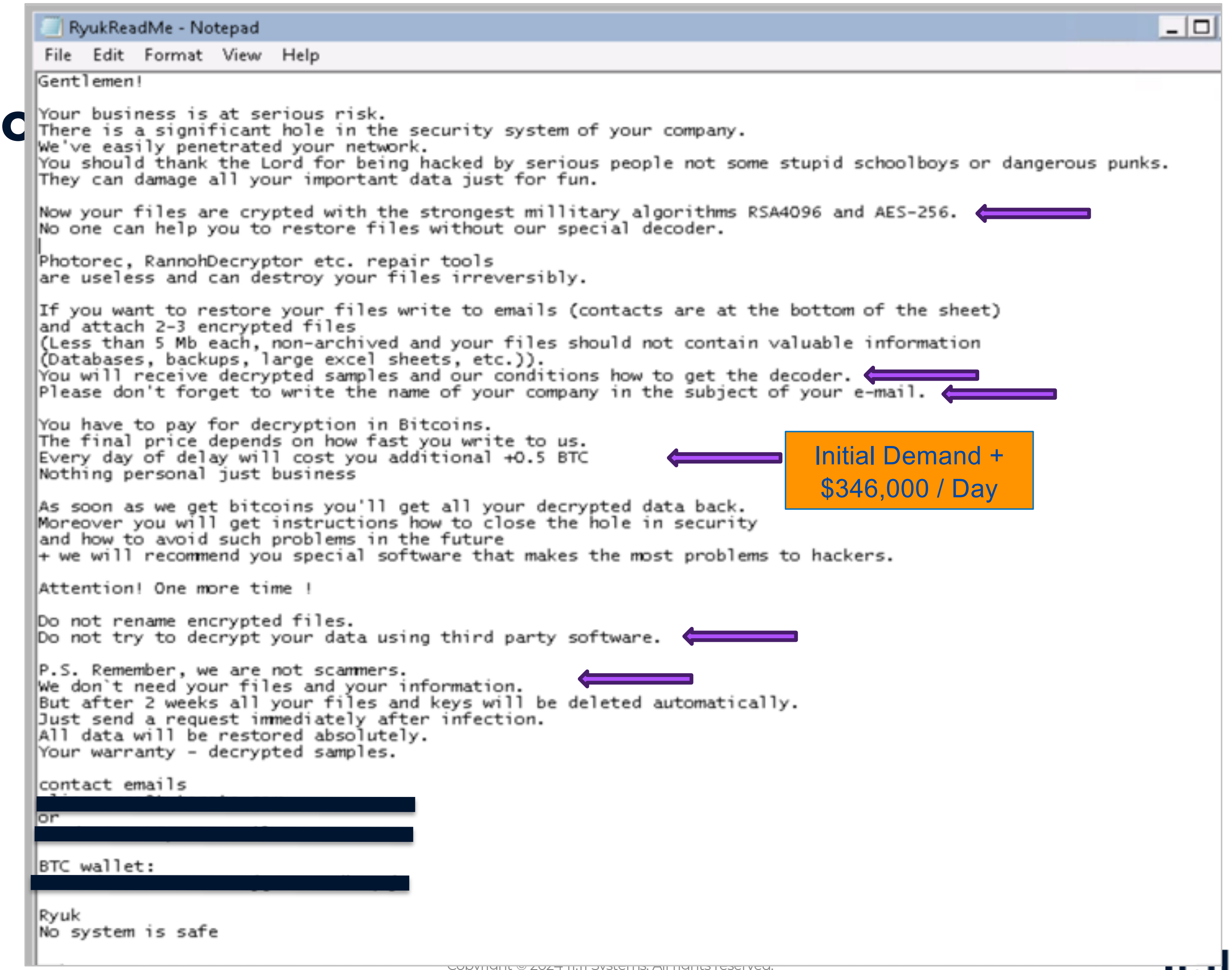
9:30AM

10:00AM

11:00AM

12:45PM

6:00PM



```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don`t need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
[redacted]
or
[redacted]

BTC wallet:
[redacted]

Ryuk
No system is safe
```

Initial Demand + $346,000 / Day

SYSTEMS

Pause for Discussion – Round 2

- **What is the most important concern**?
- Is there / what is the protocol for handling this situation?
- **Do you feel confident that you can distinguish a legitimate email from a phishing campaign?**
- Are any escalations required, and to whom?
- Is Crisis Management engaged?
- Is the Recovery team engaged?
- Would the Cyber team Lead reach out to the Crisis Management Team Leader?
- What departments may be impacted by the disruption?
- **What if any communications are needed? (What? How? Whom?)**

Day 1

12:00PM

1:00 PM

2:00 PM

3:00 PM

4:00 PM

5:00 PM

6:00PM

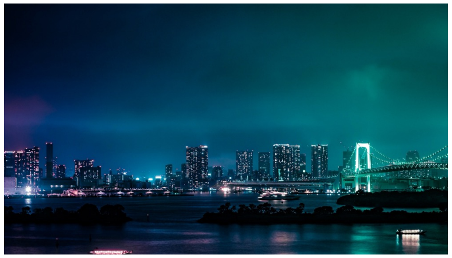
- The Cyber team has determined that an employee opened a phishing email and downloaded ransomware.
- The phished employee has not reported the incident to the team, which extends the impact area and risk.
- The ransomware spread through the employee's workstation.
- As part of containment, email and shared drive access has been restricted to prevent the further spread of the ransomware.

11:11 SYSTEMS

Pause for Discussion – Round 3

- With email shut down, how will employees be notified and kept abreast of the situation?
- How are you communicating about the event status?
- What will they be told?
- How does this affect our previous decisions?
- Do we have a clear understanding of what vital data assets may have been compromised?
- What if any, communications are now needed? (What? How? Whom?)

End of Day 1 Reporting



Day 1

12:00PM

1:00 PM

2:00 PM

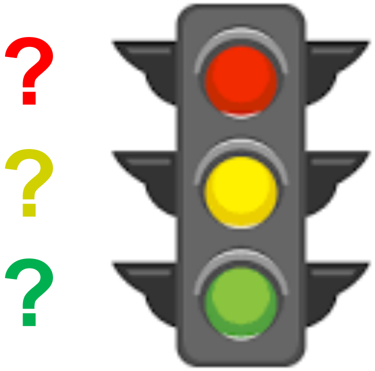
3:00 PM

4:00 PM

5:00 PM

6:00PM

- ~50% of endpoints encrypted (“crypted”)
- ~60% of servers



Downtime Impact / Who is Impacted?

Day 1

8:30AM

9:30PM

10:00AM

11:00AM

12:00PM

6:00PM

- Our Internal team / people
- Our Clients
- Others? (3rd Parties)

Over night …

Night 1

6:00PM

12:00AM

8:00AM

Who is Engaged in What?

11:11 SYSTEMS

Start of Day 2

Morning Briefing

Day 2

9:00AM

10:00AM

12:00PM

3:00PM

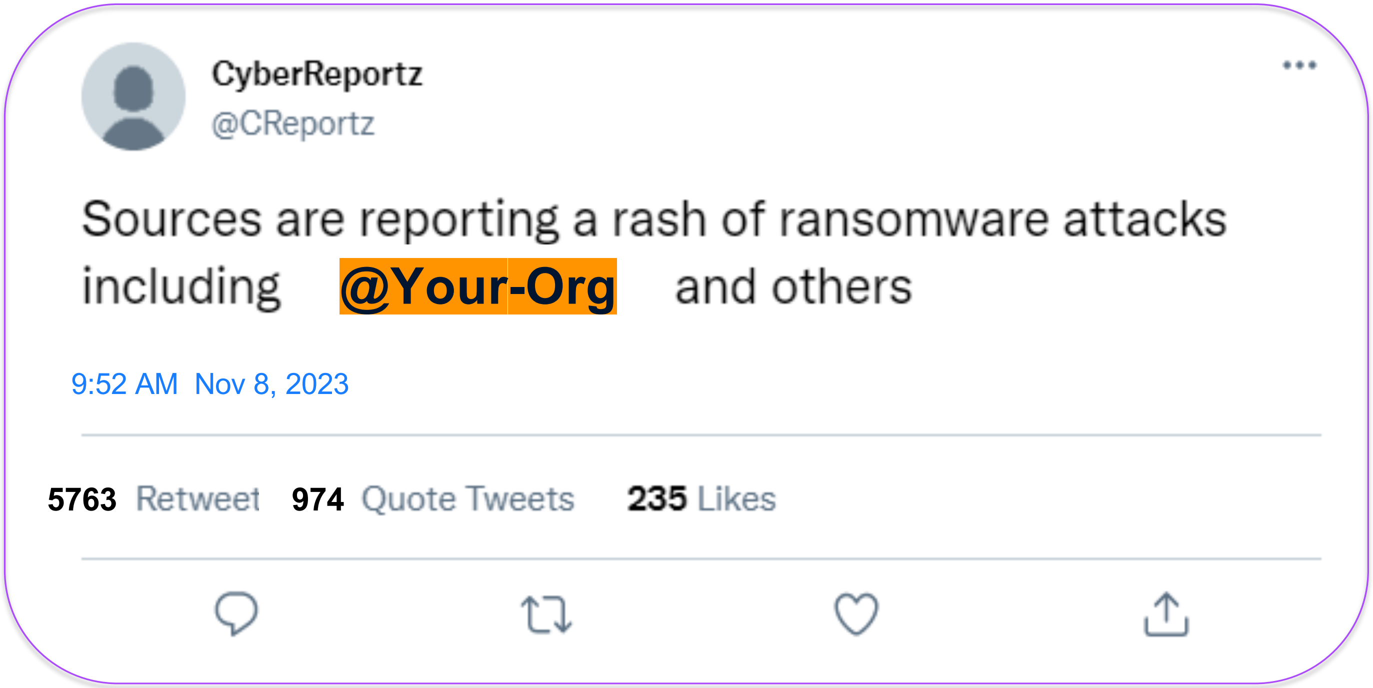
5:00PM

- We have isolated / **locked down** our network
- Work is underway to establish clean network segments
- Encrypted and unencrypted devices are still being identified
- **The digital forensics & IR firm (3rd Party) team has been engaged, analyzing logs, and collecting evidence**
- The extent of compromise is still being evaluated

Social Media Leak

Day 2

- 9:00AM
- **9:52AM**
- 12:00PM
- 3:00PM
- 5:00PM



CyberReportz
@CReportz

Sources are reporting a rash of ransomware attacks including **@Your-Org** and others

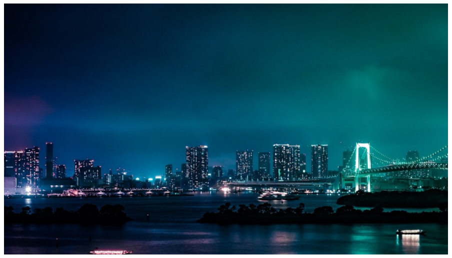
9:52 AM Nov 8, 2023

5763 Retweet **974** Quote Tweets **235** Likes

Pause for Discussion – Round 5

- What is the most important concern?
- Who is dealing with the media and social media?
- What is the protocol for handling this situation, and who will be involved in decision-making?
- What kind of a problem does this news story present for us?
- How might this information have gotten out, and is there anything that could have been done to prevent it?
- What if any, communications are needed?
  (What? How? Whom?)

End of Day 2 Reporting



Day 2

8:00AM

10:00AM

12:00PM

3:00PM

5:00PM

- We have been the victims of a successful cyber attack
- News of it has leaked out
- We are not yet in control of the situation,
  but we are **working diligently / around the clock.**

Downtime Impact

Day 2

8:30AM

9:30PM

10:00AM

11:00AM

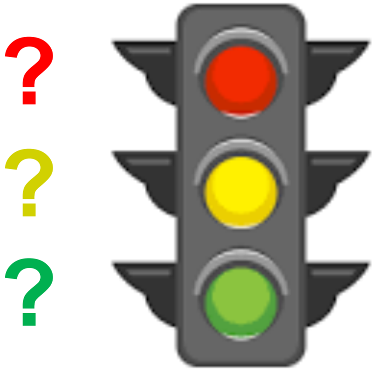
12:00PM

6:00PM

- Our Internal team / people:
  - Are we still able to Transact Business?
  - Is the DR team engaged?

- Our Clients?

- Others? (3rd Parties)?



Over night …

Night 2

6:00PM

12:00AM

8:00AM

What are our various teams working on?

Discovery!

Night 2

6:00PM

3:00AM

8:00AM

Our backups have also been compromised by the attack!

11:11 SYSTEMS

Start of Day 3

Morning Briefing

Day 3

9:00AM

10:00AM

3:00PM

5:00PM

Our backups have been compromised!

11:11 SYSTEMS

About Our Data and Data Recovery

Day 3

9:00AM

10:00AM

3:00PM

5:00PM

- Vital Data Assets:
  Not Identified / Not Protected

- IT/I&O/DR readiness:
  Unsure – determining BU status

- Recovery Point Objectives
  Unsure – determining BU status

- Business Readiness
  - 3rd Day In – What are we capable of doing?

RING RING RING...

Day 3

9:00AM

10:00AM

3:00PM

4:00PM

5:00PM

Guess Who?

- We haven’t responded to their demand! Ransom is $10M + 3 Day Delay = $11M

Plan

Day 3

9:00AM

10:00AM

3:00PM

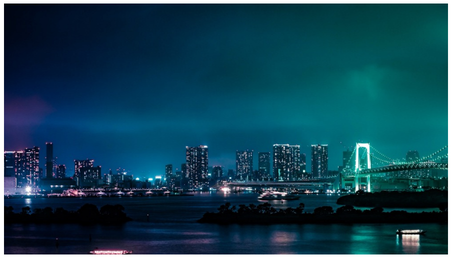
4:00PM

5:00PM

- What circumstances could drive you to consider making the payment in return for a decryptor?
- Who would guide you through the process if you decide to make the payment and make sure you are not paying an entity on the OFAC (Office of Foreign Assets) list?
- Who would make the crypto payment for you?

11:11 SYSTEMS

End of Day 3 Reporting



Day 3

8:00AM

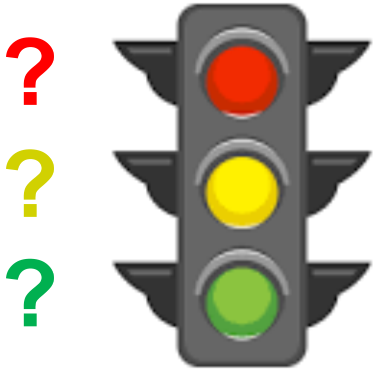
10:00AM

12:00PM

3:00PM

5:00PM

- We have data loss
- The perpetrators reached out with their demand



Day 4

Ransom = $10M + 4 Days @ $346,000 / day
$ 11,384,000

Where are we?

Day 4

9:00AM

12:00PM

3:00PM

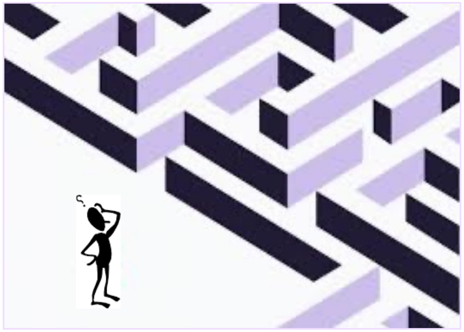
5:00PM

- Best backups we have are from 5 weeks ago
- The cost of downtime is escalating
- Our attackers are seeking payment

11:11 SYSTEMS

Compromised Data Recovery Strategy Options

One or more strategy options may need to be concurrently undertaken to minimize recovery time and operational downtime



IT Led Data Recovery

- *Restore* data from …
  - latest backups at points-in-time < or = to RPO values
  - backups at specified points-in-time > or >>> than RPO values
- *Decrypt* compromised data utilizing acquired decryption key

Business Led Data Recovery

- *Reenter* data directly from source materials
- *Recreate* data …
  - from internal sources
  - based on external outreach to customers, 3rd party providers, etc. [proactive]
  - following post-intrusion inquiry from customers, 3rd party providers, etc. [reactive]
  - by manual means (e.g., re-inventory a warehouse)

Collaborative Data Recovery

- *Reprocess* transactions …
  - from on-network sources
  - re-obtained from external sources
- *Rebuild* lost data from up-stream or down-stream systems

11:11 SYSTEMS

Start of Day 5

Ransom = $10M + 5 Days @ $346,000 / day
$ 11,730,000

PAY!

Start of Day 7

Descriptor Delivered!

Day 10

10:00AM

10.30AM

4:00PM

5:00PM

6:00PM

- Where will decryption occur?
- How confident are you that they will work?
- If they don’t, now what?

A Few Additional Discussion Topics

Day 10

10:00AM

10.30AM

2:00PM

4:00PM

6:00PM

- Press Releases / External Comms
- Employee Notifications
- SEC New Reporting Requirement
- Board Communications

Critical Systems Restored

Day 10

10:00AM

10.30AM

4:00PM

5:00PM

6:00PM

After Action Debrief

- What went well during the exercise?

- What needs improvement?

- Is everyone comfortable with your organization’s current plans and procedures?

- What specific remediation actions do you believe are necessary?

THANK YOU

11:11 SYSTEMS