Ransomware Crisis Management Tabletop Exercise

October 2nd, 2025

Agenda

- Introductions
- Cyber Threat Environment
- The Main Event
- What did we lean?

Presenters & Facilitators

- **Kelly Geary**, Esq. CIPP/US,ACP,CCP, Managing Principal, EPIC Insurance Brokers & Consultants
- **Brandon LaSpina**, Senior Analyst, EPIC Insurance Brokers & Consultants
- **Nico Clark**, Senior Analyst, EPIC Insurance Brokers & Consultants

Cyber Threat Environment

Warm Up Questions

Question #1

What is the average ransomware payment?

A.) Between $100K-300K

B.) Between $500K-$800K

C.) Between $1M-$2M

D.) Between $5M-$10M

B: Between $1M-$2M

Question #2

What is the average downtime from a ransomware attack in 2025?

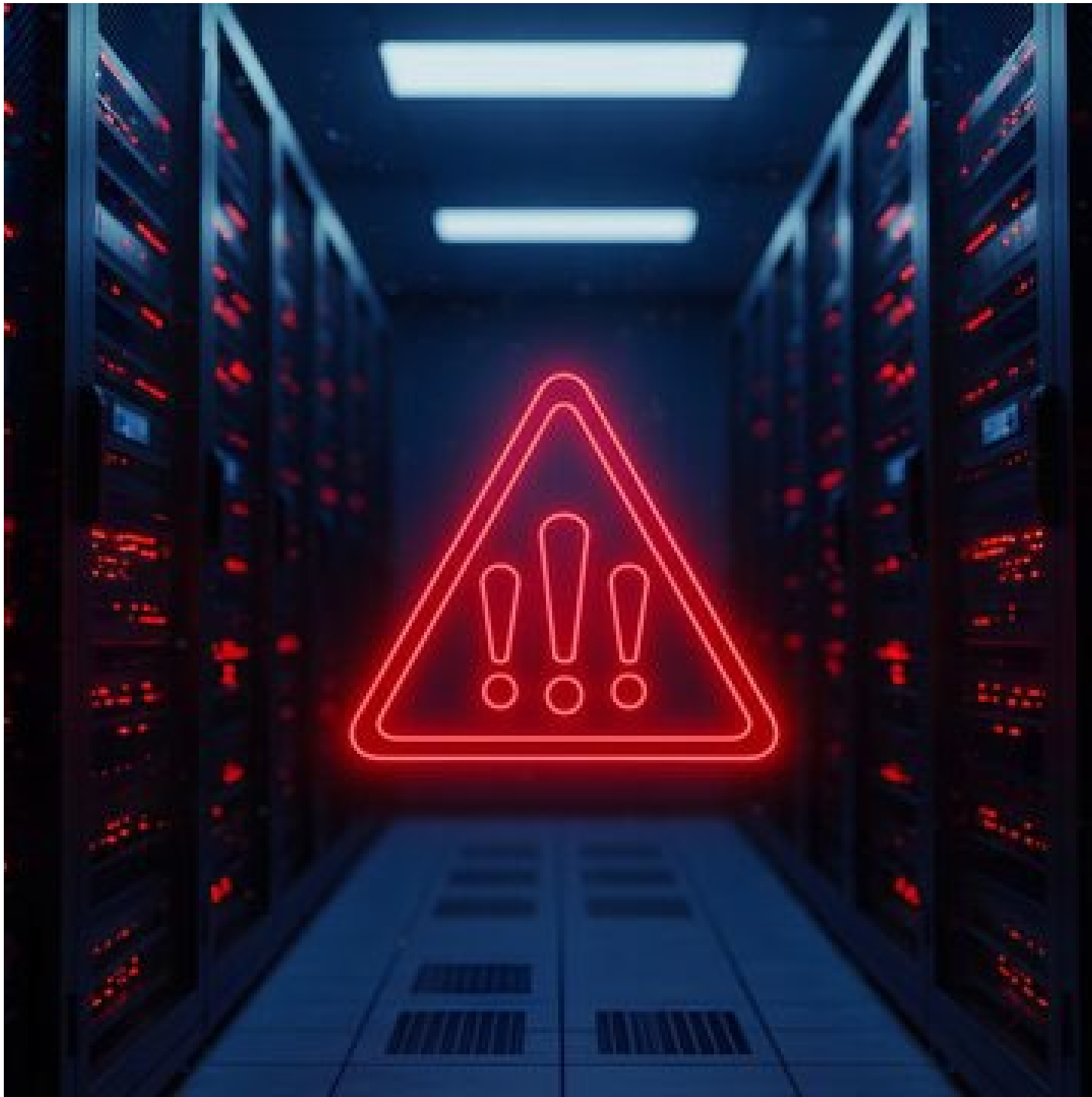
A.) 2 days

B.) 7 days

C.) 15 days

D.) 23 days

D: 23 days



Question #3

What is the average cost for financial firms to recover from a ransomware attack? (not including ransom payment)

A.) $2.58 Million

B.) $3.52 Million

C.) $5.13 Million

D.) $8.21 Million

A: $2.58 Million *in 2024*

Question #4

What is the single largest ransom payment ever made by a company?

A.) $50 Million

B.) $75 Million

C.) $100 Million

D.) $175 Million

B: *In 2024, an undisclosed Fortune 500 company paid* ***$75 million***

Question #5

What is the most targeted country for ransomware attacks?

A.) USA

B.) China

C.) Switzerland

D.) Canada

A: USA

Emerging Risks

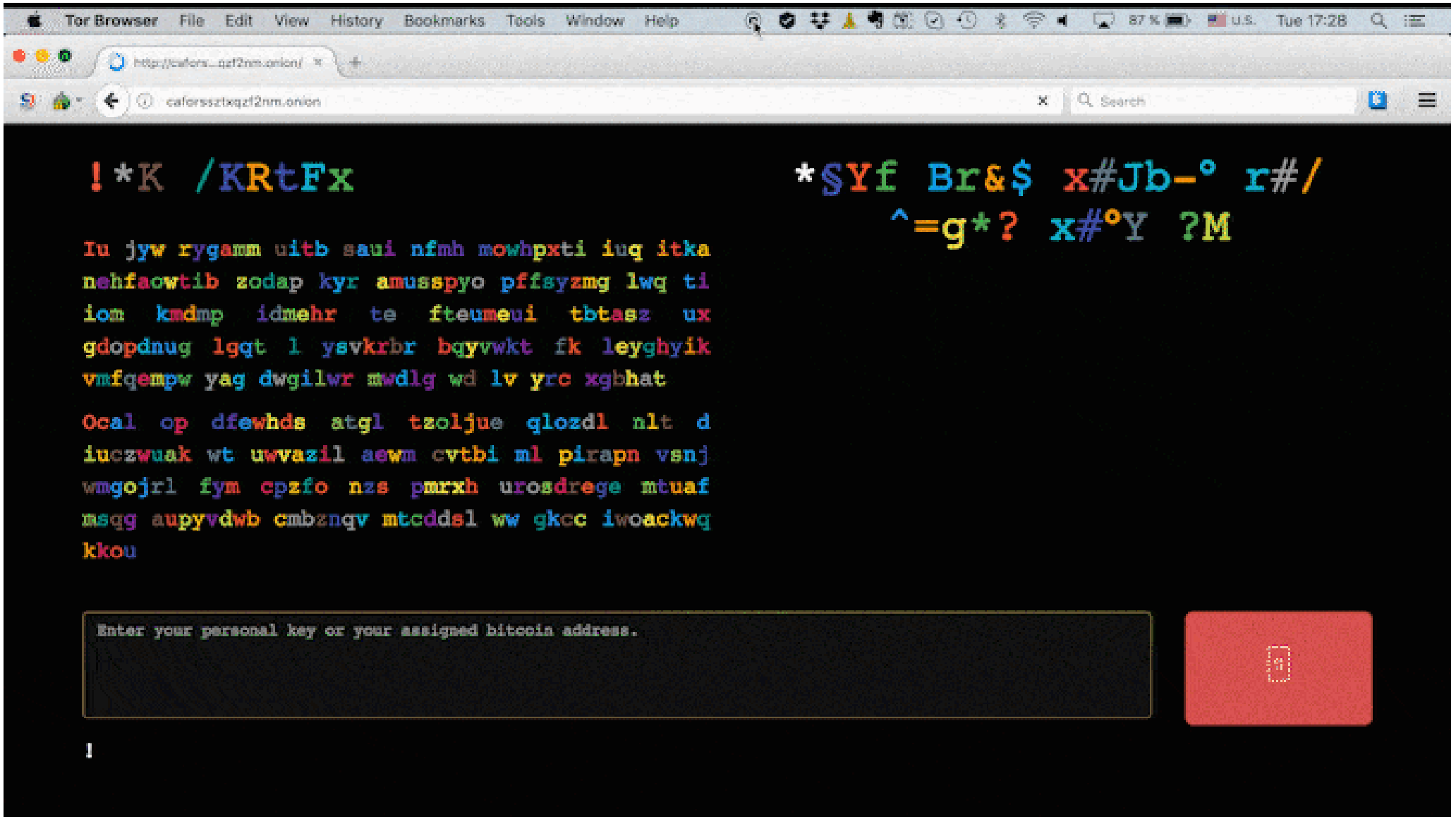
- Artificial Intelligence/GenAI
- Mis/Disinformation
- Third-Party Risk/Vendor Risk
- Cyber Crime – Social Engineering/Deep Fake/Ransomware
- Insider Threats
- Privacy/Technology Regulatory Environment

What is a Tabletop Exercise

- A **tabletop exercise (TTX)** is a discussion-based, role-playing activity that simulates a real-world emergency to test an organization's emergency response procedures. Like a Fire Drill.
- TTXs are usually held in an **informal setting**, such as a classroom, conference room, or around a table, and are led by a facilitator.
- Participants, who may play their own roles or others, **respond to scenarios** presented by the facilitator.
- The goal is to **encourage dialogue, decision-making**, and collaboration among participants, and to ensure that emergency response teams are informed and aligned on their roles during a crisis

THE MAIN EVENT


WARNM


Tor Browser File Edit View History Bookmarks Tools Window Help
Tue 17:28
caforssztxqzf2nm.onion
Search
!*K /KRtFx
*$Yf Br&$ x#Jb-° r#/
^=g*? x#°Y ?M
Iu jyw rygamm uitb saui nfmh mowhpxti iuq itka nehfaowtib zodap kyr amusspyo pffsyzmg lwq ti iom kmdmp idmehr te fteumeui tbtasz ux gdopdnug lgqt l ysvkrbr bqyvwkt fk leyghyik vmfqempw yag dwgilwr mwdlg wd lv yrc xgbhat
Ocal op dfewhds atgl tzoljue qlozdl nlt d iuczwuak wt uwvazil aewm cvtbi ml pirapn vsnj wmgojrl fym cpzfo nzs pmrxh urosdrege mtuaf msqg aupyvdwb cmbznqv mtcddsl ww gkcc iwoackwq kkou
Enter your personal key or your assigned bitcoin address.
!

Team Bank Names

1. Mo' Money, Mo' Problems Bank – Rainbow Team
2. Oopsie Financial – Light Blue Team
3. Zero Balance Bank - Orange Team
4. Patch & Pray Savings – Royal Blue Team
5. Pennywise Savings – Purple Team
6. Trust Us Bank – Yellow Team
7. Interestingly Low Bank – Lime Green
8. Ransom & Co. Bank – Hot Pink Team
9. Under the Mattress Credit Union – Black Team
10. Savings and Shenanigans Bank – White Team

Bank Profile

- Northeast Regional Savings Bank operates around 50 branches
- The bank employs approximately 500 to 600 full-time staff, managing total assets of about $7 billion and generating roughly $35 million in revenue
- As a community bank, it offers personal and business banking services, along with wealth management solutions
- IT department is overseen by the Chief Information Officer, alongside a dedicated Risk Manager
- While online and mobile banking services are available, the bank does not use biometric data for its employees or banking customers

The Tabletop Team

- Human Resources Director
- Marketing Director
- Legal/Risk –Risk Officer
- Bank Executives – CEO, CFO

Scenario

- The banks' network has been compromised, and all **servers and data are inaccessible**.
- All data has been **encrypted**.
- All users and communication on the network are **offline**, including remote users.
- A screen lock shows a **ransom** demand for **$4 million** to a bitcoin address.
- You have **48 hours to pay,** or the data will be released.
- We don't know if data has been exfiltrated.

Scenario- Additional Information

- The bank has a cyber insurance policy which renewed on **July 1, 2025**
- The bank filed a **claim, which was paid** under the cyber policy in **August 2025** for **$250,000** for a another incident.
- The bank does not have an **Incident Response (IR)** plan.

IT Room Camera

IT Status Day 0 (4 Hours)

- Everything continues to be **offline,** and team is internally investigating the extent of the issue.
- The IT team has **contacted the outsource IT** provider to help. Is this a good idea?
- IT is getting very defensive and not providing any further details

Day 0 (4 Hours) Questions

- **Human Resources**
  - How are you communicating with employees?
  - What are you communicating, if anything?
    - Do employees go home, come to the office, etc.?
- **Marketing Communications**
  - What is your message to vendors, clients and adversaries?
  - What, if anything, is being posted to your social media/website?
- **Executive Committee**
  - What are your thoughts on paying the ransom demand?
- **Legal/Risk**
  - Who are you contacting at this stage?
    - What are you telling the people you contact?

Day 1 (24 hours) Scenario

- **IT Update**
  - The forensic team reports they believe the threat actor gained access thorough a **compromised remote access device** then used **social engineering** to get a user to open a malicious file. All systems are still **down and encrypted**. **Backups** are **compromised**.

- **Breach Coach Update**
  - Threat actor has sent several files showing **proof of exfiltration.** Files contain client data including PII and intellectual property. Threat actor demands $4 million within 24 hours.

Day 1 (24 Hours) Questions

- **Human Resources**
  - What, if anything, are you **communicating** to employees and staff?
- **Marketing Communications**
  - What is your update **message** to vendors, clients and adversaries?
  - What, if anything, is being posted to your social media/website?
- **Executive Committee**
  - Are you paying the **ransom**? (Yes or No and why)

- **Legal/Risk**
  - Who are you **notifying** now that you are 24 hours into this incident?

Day 2 (48 Hours) Scenario- Bank Refused to Pay Ransom

- Threat actor has **sent demands** to **each senior executive** to their personal email accounts with sample client files and demanded they get the firm to pay, or the data would be released.

- Threat actor has contacted the **Executives** with **deep fake videos** and images of their family members and threatens to post these to their **social media accounts.**

- **Demand** has **increased** to **$8 million** since first deadline was missed.

Day 2 Scenario- Bank Paid Ransom

- Your bank elected to **pay the ransom**. You received a **decryption key**, but the IT team is struggling to get it to work on all servers and the order of restoration with integrated systems is proving to be a **challenge**. In other words, your **systems are not fully back online.**

- **Client data** is being **leaked** on the **dark web** with your Bank name.

Day 2 (48 Hours) Questions

- **Human Resources**
  - What are you communicating to **employees and staff**?

- **Marketing Communications**
  - What is your update **message** to **vendors, clients and adversaries**?
  - What, if anything, is being posted to your **social media/website**?

- **Executive Committee**
  - What is your **messaging** to **partners**?
  - If you didn't pay, are you reconsidering your approach?

- **Legal/Risk**
  - Who are you **notifying** now?

Day 3 (72 Hours) Scenario

- **IT Update-** Some **limited systems** are up and running. Users can get access to some applications but not others.

- **Forensic Update-** Team reports it is possible **all your data** was **exfiltrated** including employee data and client data. They have access to the firm's backups.

- **Clients** are calling concerned about the **release of confidential data** and are **expressing a loss of trust**.

Day 3 (72 Hours) Questions

- **Human Resources**
  - What, if anything, are you communicating to employees and staff?
- **Marketing Communications**
  - What is your update message to vendors, clients and adversaries?
  - What, if anything, is being posted to your social media/website?
- **Executive Committee**
  - What is your messaging to partners?
- **Legal/Risk**
  - Who are you **notifying** now?

Scenario Conclusion

- **Bank Paid-** The bank restored their data with a combination of backups and the decryption key. The systems were compromised for **16 days**, and **only small pieces of data** were found on the **dark web**. The first party claim totaled **$7m**

- **Bank Didn't Pay-** The bank restored their data with backups. The systems were compromised for **28 days**, and **client data was found** on the **dark web**. The first party claim totaled **$2.5m**

SHOULD YOU PAY THE RANSOM?

This is a business decision! Can you afford to be down? It depends on how prepared the organization was in the case of a ransomware attack.

Future Potential Fallout

- Repeat Cyber Attack
- Social Media Backlash
- Regulatory Inquiries/Investigations
  - Formal or informal
  - Multi-jurisdictional
- Third-Party Lawsuits/Class Actions
  - Clients
  - Employees
- Employee Mental Health Challenges
- Forensic Assurance Letters

What Did We Learn?

Tips & Takeaways

- Remain **calm** in the face of the crisis. Think **strategically**, don't be reactive.
- Establish **alternate communication** method
- Conduct **Holistic, Inter-departmental** Tabletop Exercises and training ***at least biannually***
- Create multiple different "**playbooks**" based on the threat environment at the time.
- Prepare crisis communication **messaging templates –** for both internal and external communications.
- Incorporate **insurance** into your incident response plan and your tabletop exercises.
- Have the conversation about whether, and under what circumstances, your firm would **pay a ransom, *frequently*.**