

## Simulated Cyber Attack

The critical role of lawyers and governance in keeping a bad day from becoming a tragic year

May 22, 2024

**Jennifer Martin**

*Sr. Cybersecurity & Privacy Counsel, Postman*

**Michael Bahar**

*Global Co-Lead of Data Privacy, Security and Technology, Eversheds Sutherland (US)*



# **Cyber-Attack Scenario**

December 23-28, 2024

# Timeline 1

## Scenario

Friday, Dec 23  
12:00 pm

Saturday, Dec 24  
10:00 am

Tuesday, Dec 27  
9:00 am

- You're in-house at a public company. At noon on the Friday before the Christmas holidays you get a FaceTime call from your CEO: "One of our primary service providers has been hit with ransomware, and they have critical documents that cannot be released."
- The connection seems poor. The CEO says she is on a plane about to depart for Rome, but she directs you to "pay the attackers whatever they want now!" She then abruptly disconnects, before you have time to ask any questions.
- Moments later, you get an email saying: "we got your service provider, but we have your data. If you don't want it publicly released before the holiday, click [here](#); if you need more time, click [here](#)."
- You try to contact the CISO on his office line, but no one answers. Time goes by, and you try again, with no luck.
- A follow-up text to your cell reads: "This is your last chance, click to [pay](#) or click here for [more time](#)."
- You click for more time, download a .pdf of more information, and are relieved when a subsequent message thanks you for your responsiveness and indicates you now have 14 days before any impacts to your company's data.
- You decide not to bother people before the holidays.

# Timeline 1

## Group discussion

Friday, Dec 23  
12:00 pm

Saturday, Dec 24  
10:00 am

Tuesday, Dec 27  
9:00 am

### Discussion

#### Poll:

- 1) How many people think he should further engage the hackers to find out more about them and what they have?
- 2) How many people think he should consider their demands and start to figure out a way to pay the ransom?
- 3) How many people think he should reach out to the service provider to get more information about the attack and response?
- 4) How many people think he should call law enforcement immediately?
- 5) How many people think he should take off for the holidays, and deal with it in a week?
- 6) How many people think he should do something else?

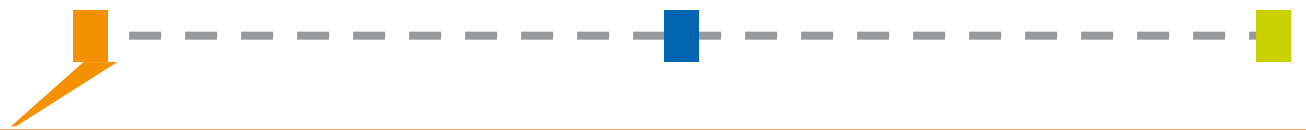
# Timeline 1

## Key Considerations

Friday, Dec 23  
12:00 pm

Saturday, Dec 24  
10:00 am

Tuesday, Dec 27  
9:00 am

- 
- Is there an Incident Response Plan? Does Security know?
  - Urgency + (click, download or wire) = bad idea
  - Take the time to look for things that may not make sense— is this really the CEO? Would she speak like this?
  - Do you have the ability to reach key people, even when you're not at your desk?
  - Bad news does not get better with age
  - Regulatory move towards personal liability
  - What would you do if this is a real service provider breach?

# Timeline 2

## Scenario

Friday, Dec 23  
12:00 pm

Saturday, Dec 24  
10:00 am

Tuesday, Dec 27  
9:00 am

- It's now Christmas day and you are awoken by multiple messages that systems are starting to lock up. You sign on and realize your system as well is showing a ransom message...
- Follow-up messages, apparently from the same attackers, now include a link to a schedule of internal documents, including employee data. The pre-selected data is set to "automatic leaks," and a timer counts down ominously unless 100 Bitcoin (~6.2m USD) is paid by Monday.
- The CFO convenes a core team remotely and says: "I know it's Christmas, but we have a real problem on our hands." You can hear him rapidly clicking in the background. "I am trying to find out what they have, but it's a lot and it's downloading slowly. I do know we can't let some of this become public. Our confidential merger documents are here!"
- Another executive jumps in: "Look, we need to pay and pay now! This is serious. It's not just the data they have, but we may not be able to service our customers!"
- Your mind is flooded. A wave of realization comes crashing down on you. You go to raise the possibility that you may have been tricked into clicking on a fraudulent link, but you decide there will be time for that later.
- The CFO says, "OK, I will try the CEO. If I can't reach her in the next 5 minutes, I will authorize the payment."
- He then adds: "Oh, I see they have also have a ton of data belonging to our overseas employees."

RECOVER: FILES.txt - Notepad  
File Edit Format View Help

>> what happened?

Important files on your network was ENCRYPTED and now they have "██████" extension.  
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.  
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:

- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

Samples are available on your personal web page linked below.

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.  
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.  
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> what should I do next?

1) Download and install Tor Browser from: <https://torproject.org/>  
2) Navigate to: <http://75gw6lqfesrhbitz2r4yihnrw4sknz3q2m5kf6ulpidt2wxuxs7zbaid.onion/?access-key=%2BkaNA1HqbuCu76V7kPCsT80ChQKdwOTmj%2BmgjjEGDQ4B1f31qzLuwtHbJSdoiPuuVeD7k2NzWfQV%2FBgRMq2LVNTw9880cB5UQ9B0JQCCuONtrzoYU2JC6wWwNkM48XphV4rSGc0roIjbfAs%2B42qYKF8dskmJu2U1XFvjyu1uTItfdH%2BeuwEhesrwr686MacfyAPyfw4WhVvtKdPed12k4HYAmbwFwN3Br26DXMLx0EQy56N34LJMZQLCOJE80i%2FJ3jwui1JanMYQ4TRPxvKSyRHdNrQf4dvh0Vrscy%2BstZdTdfGnJwaUwqCCmpnu%2FEDpyOrP1g5ZwQ%3D%3D>

## Timeline 2

### Group discussion

Friday, Dec 23  
12:00 pm



Saturday, Dec 24  
10:00 am



Tuesday, Dec 27  
9:00 am



### Discussion

*Spot the Legal Issues*: Read the next slide, and list in the meeting chat at least 3 legal issues you would consider your top priority to run down.



# Timeline 2

## Key Considerations

Friday, Dec 23  
12:00 pm



Saturday, Dec 24  
10:00 am



Tuesday, Dec 27  
9:00 am



**Legal Issues** - Paying ransoms is fraught with difficulty and it is not necessarily the “easy button”

- ATTORNEY-CLIENT PRIVILEGE
- Sanctions rules: Check the OFAC list!
- Data Breach (global)
- SEC Disclosure requirements
- Potential Insider Trading
- Theft of Trade Secrets
- Anti-money laundering legislation
- Tax and Financial implications
- Corporate social responsibility policies

### **Other Issues**

- Who is authorized in your plan to make ransom decisions if the CEO isn't?
- What are the mechanics of negotiating/paying ransoms?

***Let the experts handle the investigation! Downloading data, negotiating yourself, or making decisions without expertise can make the incident worse!***

# Timeline 3

## Scenario

**Friday, Dec 23**  
**12:00 pm**

**Saturday, Dec 24**  
**10:00 am**

**Tuesday, Dec 27**  
**9:00 am**

- The CEO is now firmly in control of the situation. She directs that no ransom be paid “until we get to the bottom of this.”
- The CISO retains their cyber forensic company, Cypfer, who dials in from California. You record the call so nothing missed and engage an AI-powered transcription and summary function. Cypfer is working before and during the call to scope the problem as per their retainer. They outline what they know about the attackers: “low-medium confidence they are state-backed.”
- The CIO states: “We have the best in the business, and Cypfer has drawn its people from NSA and GCHQ, can’t we go in and stop them ourselves?!”
- They also reveal more details about the documents, having downloaded them on a stand-alone “clean machine.” Some include complete personnel files for current and former California-based, UK, German and Japanese employees, while others include highly confidential strategic documents. Some files are encrypted.
- The room is abuzz with activity, as Comms quietly works in a corner typing out a press release, which includes an apology and assurances of a quick return to business as usual. Comms is also having to respond to reporter requests for comments based on an employee’s Facebook post about a “Cyber snowday! No work today!”
- Just then you overhear from the corner of the room: “May not be covered?! What do you mean?!” They must be talking about your cyber insurance.
- “One more thing,” Cypfer reluctantly adds, “within the exfiltrated files there are rather disturbing emails and documents from the CEO...”
- “What?!” the CEO interjects. “This is... what?! I never did this! These are completely made up!”

## Timeline 3

### Group discussion

Friday, Dec 23  
12:00 pm



Saturday, Dec 24  
10:00 am



Tuesday, Dec 27  
9:00 am



### Discussion

Poll: There are a lot of communications to consider. Choose which list represents the top three groups of people you need to communicate with first:

- 1) Board, largest enterprise customers (under contractual terms & before they hear it in the news), and EU regulators (per the GDPR)
- 2) Insurance Broker/Insurer, Public Statement (before news and rumors start), US regulators (SEC, state regulators, industry regulators)
- 3) Board, EU regulators, Law Enforcement
- 4) Insurance Broker/Insurer, Board, Largest enterprise customers
- 5) Insurance, Board, Public Statement

# Timeline 3

## Key considerations

Friday, Dec 23  
12:00 pm

Saturday, Dec 24  
10:00 am

Tuesday, Dec 27  
9:00 am

- If the attackers are state-backed, should that change how you respond? Does it create any legal obligations? Could it affect your cyber insurance coverage?
- Need to maximize legal privilege (three-way agreements signed in advance).
- Consider how different types of “sensitive” data, including personal data, must be treated. What type of data is most valuable? Security information?
- Consistent and Coordinated Communications to Media, Boards, and Regulators, and to do it all globally, especially challenging with varying triggers (eg risk of harm).
- Dangers of “hacking back.”
- Recording calls with individuals in California (and other jurisdictions) without consent can lead to liability; could “waive” work product privilege; ensure that you are complying with foreign law when handling multinational incidents.
- Data manipulation attacks
- How to deal with system impacts
- Need to review social media policies
- What’s the succession plan if key leaders can’t participate?
- Even encrypted data may soon be reportable (eg in Japan), especially in light of steal-now-decrypt-later attacks

## **Key takeaways**

# Key takeaways



- Hope is not a Plan. Instead, plan for the worst, hope for the best.
- Governance and lawyers make the difference between a bad day and a tragic year
- The global threat and regulatory environments are rapidly changing—and so must we
- Information Security isn't just about technology
- High tech problems can have low tech solutions
- Look out for single points of failure – including conflicts of interest, poor escalations paths, knee jerk reactions
- When a breach occurs, avoid “kid soccer”
- If you have to ask the question whether to notify, it is usually better to notify (or, “when in doubt, get it out”)
- You don't have to outrun the bear, only the slowest camper (in other words, it's about being reasonable and creating a favorable record of reasonableness)
- The plans may be useless, but the planning is essential