EVERSHEDS SUTHERLAND

# Navigating a cyberattack – what do you need to know?

An interactive discussion and simulated case study

**September 2023**

Michael Bahar
*Partner, Eversheds Sutherland*

Rhys McWhirter
*Partner, Eversheds Sutherland*

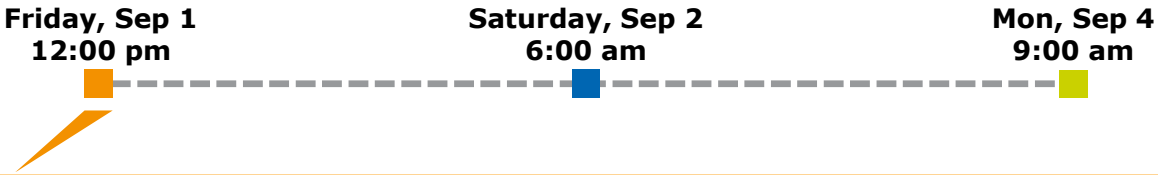
ACC Association of Corporate Counsel
SAN FRANCISCO BAY AREA

# Cyberattack scenario

September 1-4, 2023

# Timeline 1

Scenario




- It's Friday before Labor Day weekend, and you are the chief privacy officer of a global public tech company. The company provides data governance solutions for major companies (including financial institutions) around the world. The CEO's administrative assistant (AI) suddenly forwards you an email from a prominent US plaintiff's firm with a pdf. It contains a demand letter alleging unlawful and deceptive practices and wiretapping in your company's cookies opt-out practices.

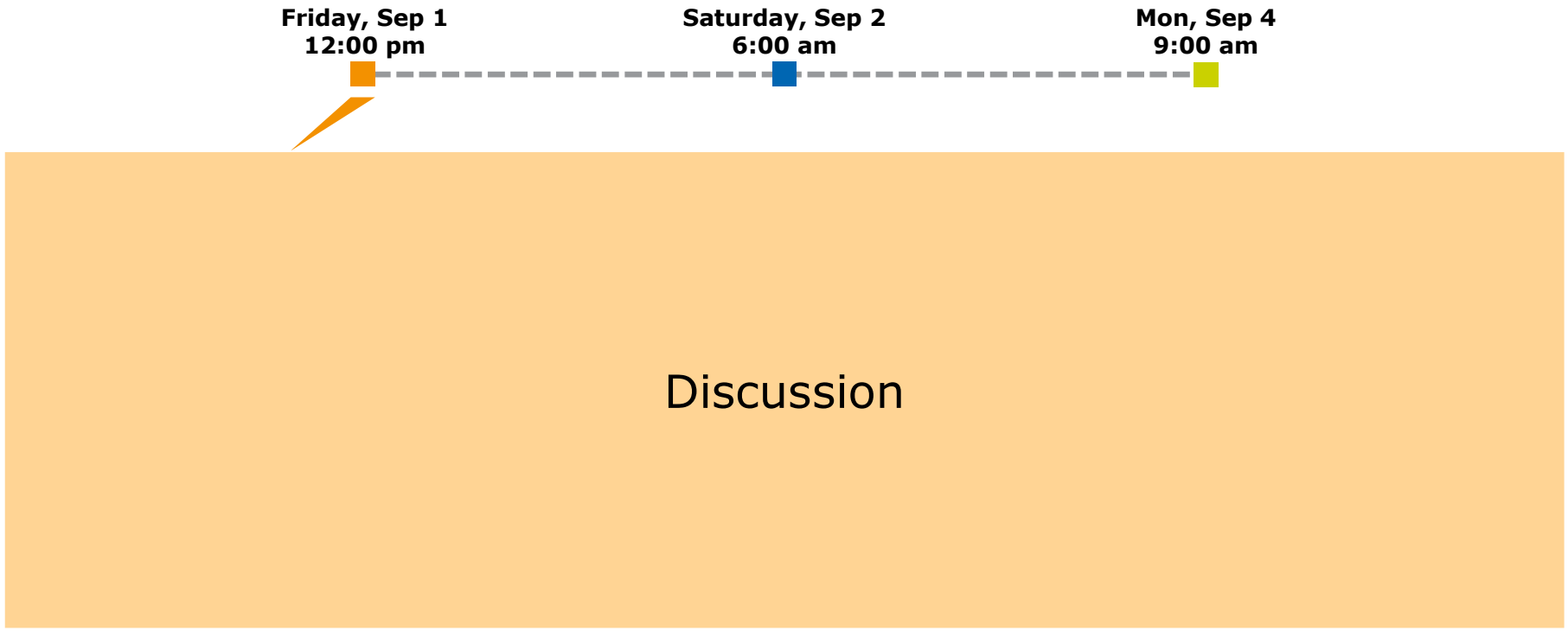
- The demand letter is far from a work of art, but it explains that based on automated tests they've run, your company is "failing to stop targeted advertisements even after individuals opt out." They provide a link to a forthcoming exposé from Consumer Reports and a zip file with more information. They assert that unless you respond by Monday with a class-wide settlement offer of $5.25 million, they will "file suit and inform relevant privacy commissioners."

- With your litigation colleagues already off, you call the number listed in the signature line, and while you're pleased the lawyer immediately answered, your initially polite (and very reasonable) requests for an extension are denied. You ask multiple times and in multiple ways, but the answer is always precisely the same (he seems both unmoved and nonplussed by your repeated and increasingly strident requests).

- Furious, you start reading the draft article and download the zip file of more information. You send a text to the GC who is on the beach but promises "all will be fine." She says she will contact the global head of litigation in London in the morning: "After all, they had their long weekend last weekend so they can take the lead!"

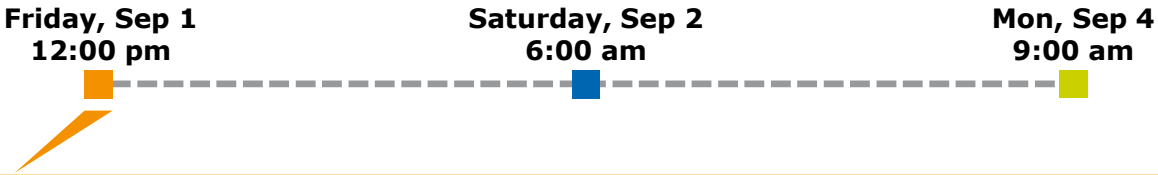
# Timeline 1

Group discussion



# Timeline 1

## Key considerations

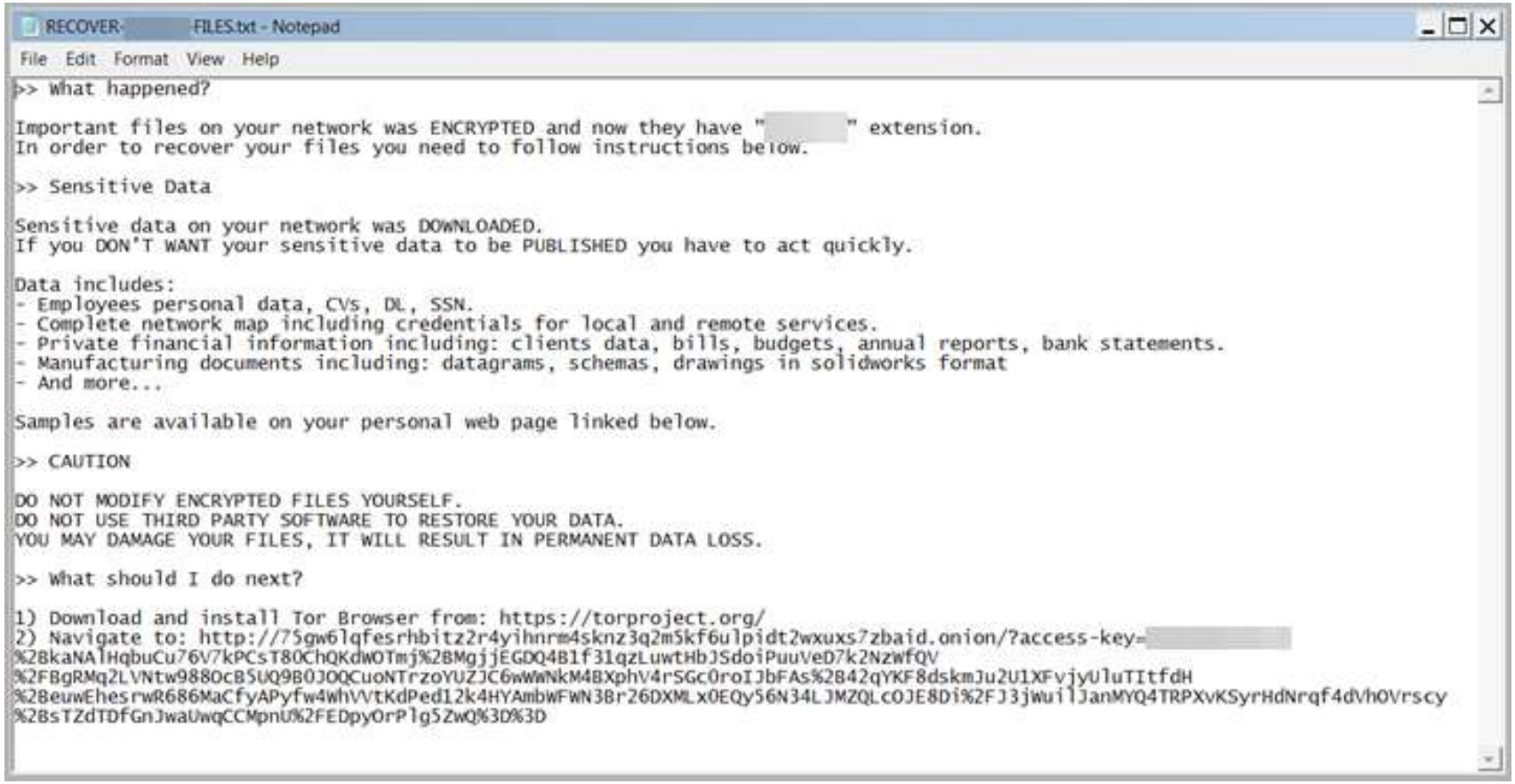



- The rise of turbo-charged AI threats, including even more realistic phishing and spear phishing, as well as spoofed audio and video (aka deepfakes)
- It's not perfect… yet
  - Normally, a US plaintiff's firm wouldn't expect a response that quickly
  - They wouldn't also threaten referring you to privacy commissioners as opposed to State AGs or the CPPA.
  - The "draft" Consumer Reports Article was also a clue.
- That said, the underlying issue of increased litigation and regulatory action around cookie practices – including from states without enhanced privacy laws – is real.
- And advanced technological game changers are not just AI – e.g., quantum computing

# Timeline 2

Scenario


- It's now Saturday morning and you are awoken by desperate messages from your colleagues in Asia and Europe that their systems are starting to lock up. You groggily sign on and realize that your system as well is showing a ransom message…
- Follow-up messages, apparently from the attackers, also include a link to a schedule of documents that contain personal data and crucial financial transaction data provided by the company's clients based in Mainland China, Hong Kong and Singapore which purport to have come from the company's local servers where the company's customers are based. The pre-selected data is set to "automatic leaks," and a timer counts down the remaining time unless 212.62 Bitcoin is payed by Monday.
- One executive tries to reach the CISO but he is traveling and is inaccessible for the next few hours. The executive cannot reach the general counsel either.
- She does manage to reach you. "I know it's the long weekend, but we have a real problem on our hands." You can hear her rapidly clicking in the background. "I'm trying to find out what they have, but it's a lot and it's downloading slowly. Let's get everyone together. If this is real, we need to pay and pay now."
- Your heart drops and goes to tell her that you may have clicked on the link that led to the ransomware attack; but you decide there will be time for all that later.
- Now what do you do?


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://75gw6lqfesrhbitz2r4yihnrm4sknz3q2m5kf6ulpidt2wxuxs7zbaid.onion/?access-key=
%2BkaNAlHqbuCu76V7kPCsT8OChQKdWOTmj%2BMgjjEGDQ4B1f31qzLuwtHbJSdoiPuuVeD7k2NzwfQV
%2FBgRMq2LVNtw988OcB5UQ9B0JOQCuoNTrzoYUZJC6wWWNkM4BXphV4rSGc0roIJbFAs%2B42qYKF8dskmJu2U1XFvjyUluTItfdH
%2BeuwEhesrwR686MaCfyAPyfw4WhVVtKdPed12k4HYAmbwFWN3Br26DXMLx0EQy56N34LJMZQLcOJE8Di%2FJ3jWuilJanMYQ4TRPXvKSyrHdNrqf4dVhOVrscy
%2BsTZdTDfGnJwaUwqCCMpnU%2FEDpyOrPlg5ZwQ%3D%3D
```

# Timeline 2

Group discussion

# Timeline 2

## Key considerations


- Know in advance whom to call – there should be multiple points of contact in case one or more people can't be reached. Make sure you have a way to contact them even after hours or if your systems are down.
- Take a breath – as fast as things seem to move, you have time. Attackers want you to make mistakes under pressure.
- But bad news does not get better with age!
- Let the experts handle the investigation. Downloading data from the attackers can make the incident worse!
- Consider the local law requirements in this incident.
- Paying ransoms is fraught with difficulty and it is not necessarily the "easy button"
  - No guarantees
  - Sanctions rules
  - Anti-money laundering legislation
  - Corporate social responsibility policies
  - Generally does not negate reporting responsibilities
  - Tax implications for global entities

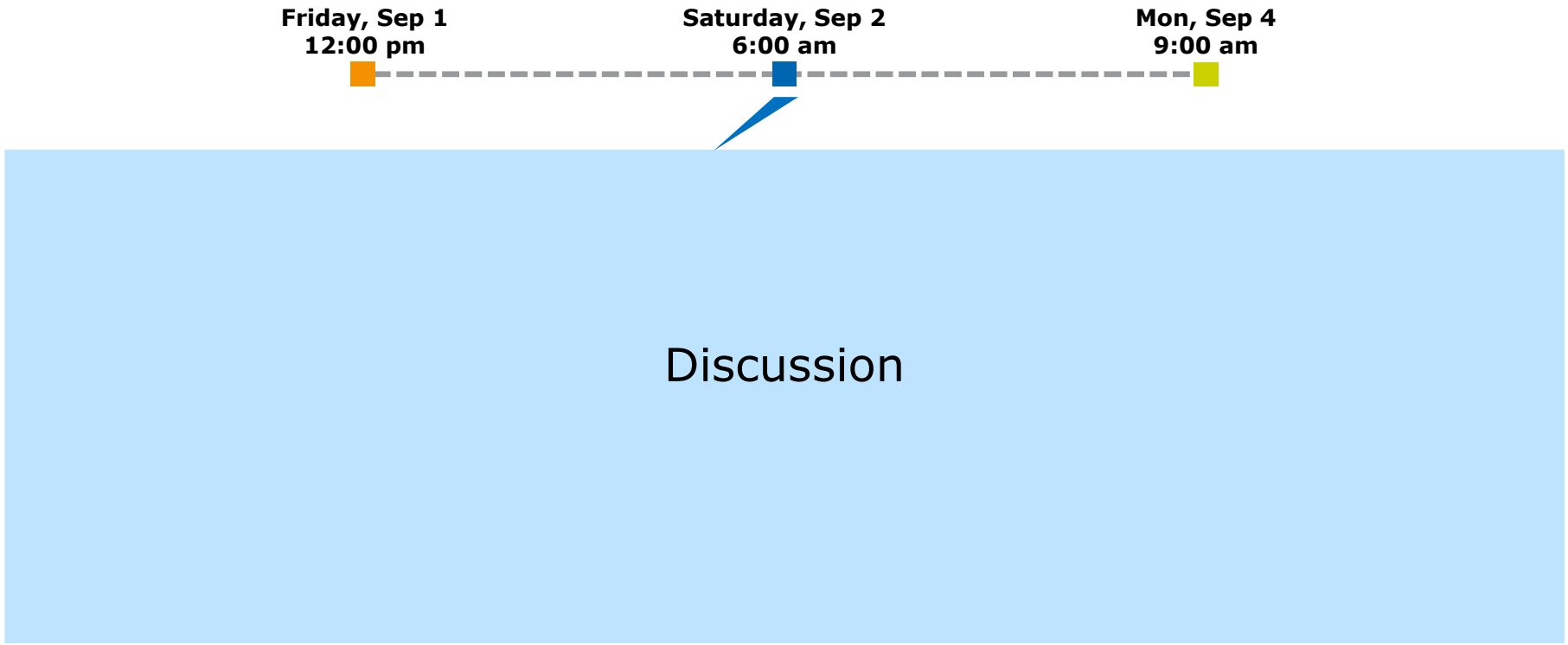
# Timeline 3

## Scenario


- The team convenes remotely via a link that the CEO's administrative assistant, named Al, sends around. Al, a married father of two, has recently been posting to social media about his wife's struggle with an illness, as well as his deep concerns about losing his job in light of what appears to be a global economic downturn, and his distrust of management.
- At the appointed time, the team convenes. At the direction of the CISO, Al also sends the invitation to Mandiant, and they dial in from Florida, Pennsylvania and their overseas offices (including Mainland China). Al records the discussion so that nothing gets missed.
- Mandiant 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."
- They also reveal what some of the documents are, having downloaded the documents on a stand-alone "clean machine." The documents set for release include highly sensitive corporate strategic documents, financial information and employee information from numerous corporate offices including Mainland China, Hong Kong, Japan and Singapore. HR files from the Japan operations were exfiltrated but remain encrypted. "At least some good news! No need to report."
- Just then you overhear from the corner of the room: "May not be covered?! What do you mean?!" They must be talking about their cyber insurance.
- "One more thing," Mandiant reluctantly adds, "within the exfiltrated files there is a surreptitious recording of the CEO…"
- "What?!" the CEO interrupts. "This is… what?! I never did this!"

# Timeline 3

Group discussion



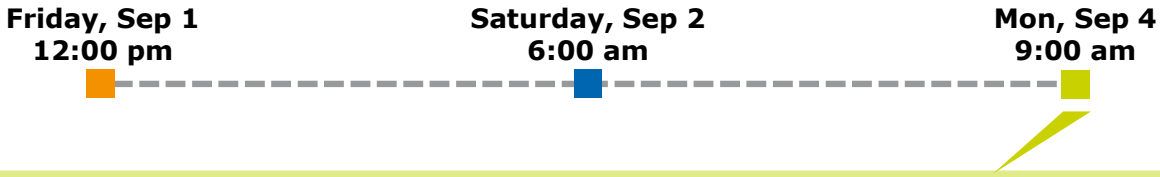
# Timeline 3

## Key considerations


- If the attackers are state-backed, should that change how you respond? Does it create any legal obligations? Could it affect whether your cyber insurance will cover the incident?
- Need to maximize legal privilege
- Consider how different types of "sensitive" data, including personal data, must be treated. What type of data is most valuable to your company? Intellectual property, upcoming deals, etc.?
  - Need for a coordinated approach to global notifications
  - Consistent and coordinated communications
- Recording calls with individuals in California (and other jurisdictions) without consent can lead to large liability; ensure that you are complying with foreign law when handling multinational incidents.
- Data manipulation attacks – another super-charged AI attack
  - Do you have a succession plan if key leaders can't participate?
- Even encrypted data may now be reportable, especially in light of steal-now-decrypt-later attacks

# Timeline 4

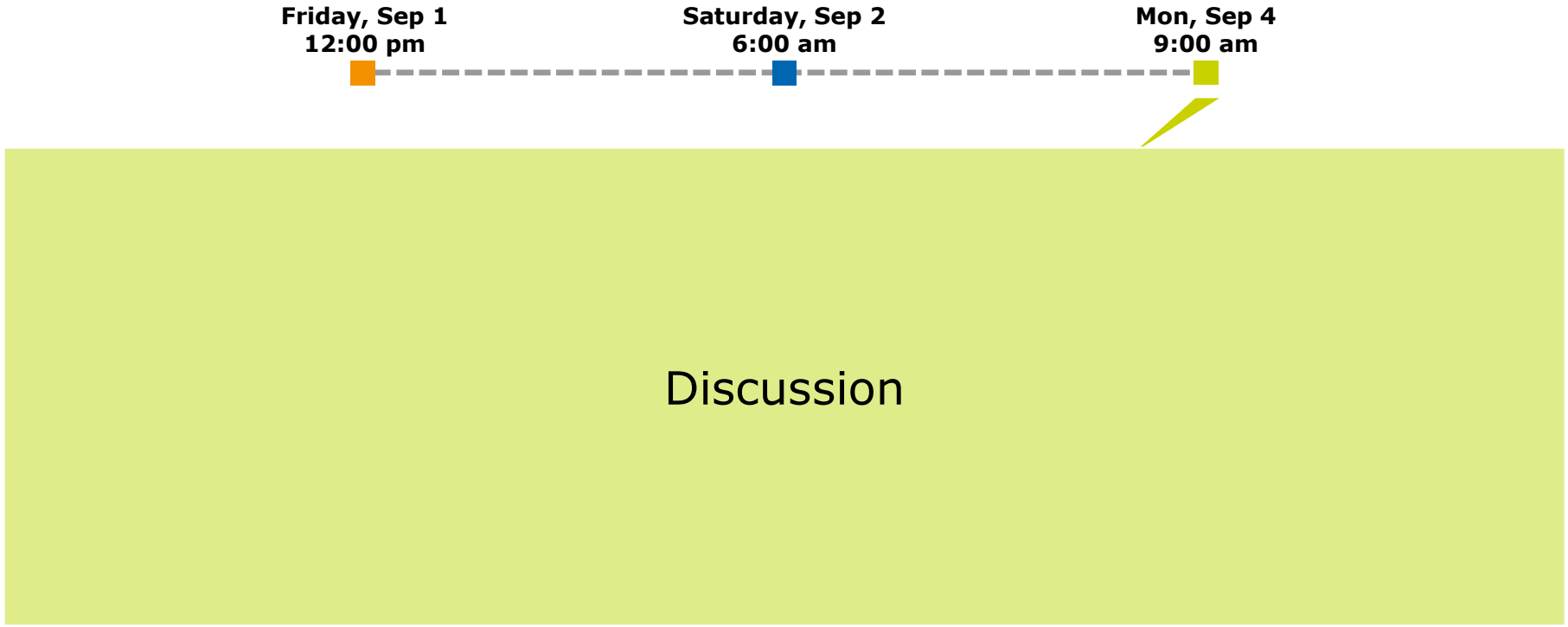
Scenario




- During a subsequent conference call the next day, the CEO informs the group that Al has been placed on leave. According to internal logs, Al has been keeping odd hours. He has also been downloading large amounts of data since the end of March 2020. That activity normalized for a time but then started up again.
- It also turns out that the attackers launched an initial phishing campaign targeting only a few employees on a Friday afternoon, asking them to confirm their health benefits status "by the end of the day" via a link to a fillable .pdf and a text message to their personal phones.
- The employees who received it were the ones who had been commenting on Al's social media page.
- Palo Alto Networks, now called in by OC "in anticipation of litigation," confirms that the source of the email was Al. "However," they add, "let's not rush to any conclusions."
- One executive exclaims: "Well, we have to rush. We are going to lose control of the situation by the end of the day! Fire Al, pay the money, issue a public apology, and let's all move on. If we manage to keep these documents from being released, we can all still have some semblance of a holiday!"
- Mandiant adds that some impacted employee documents are from the US, UK, Germany, Mainland China, Hong Kong, Singapore and Dubai. Some of the documents are in Chinese, so they have yet to translate them.
- An executive says: "OK, well, let's send a text message to our managers in those countries that we may need to speak to them, so they better be available. I got a message from our leadership in Hong Kong, and they rely on WhatsApp for their emergency communications and are demanding a WhatsApp update call ASAP."

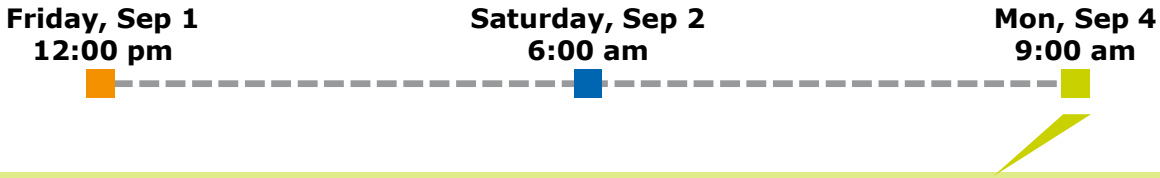
## Timeline 4

Group discussion



# Timeline 4

## Key considerations




- Haste makes waste. Don't make the situation worse by reacting too quickly.
- Consider how employment law could apply to Al's situation. Do we actually know whether he has done something wrong or illegal?
  - Is anomalous behavior the same after the pandemic?
- Beware of the apology – litigation and regulatory enforcement risks should inform your response, especially during external communications.
- What are the legal obligations during a breach in countries where employees may be impacted?
- Who within and outside of the company should be aware of the incident, and how should you handle those communications?
- Who should handle external communications? Is there a policy regarding what employees may post on social media or say to the media?
- Restrictions on communications (e.g., VPN restrictions)

# 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
- Time for a comprehensive digital strategy
- Look out for single points of failure
- When a breach occurs, avoid "kid football"
- If you have to ask the question whether to notify, it is usually better to notify
- 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

EVERSHEDS SUTHERLAND

**Michael Bahar**
Partner, Eversheds Sutherland
+1 202 383 0882
michaelbahar@eversheds-sutherland.com

**Rhys McWhirter**
Partner, Eversheds Sutherland
+852 2186 4969
rhysmcwhirter@eversheds-sutherland.com

**eversheds-sutherland.com**



ACC Association of Corporate Counsel
SAN FRANCISCO BAY AREA