FT INNOVATIVE LAWYERS2020 EUROPE WINNER

Pinsent Masons

Ransomware

SCL Trainee Group

Stuart Davey
Alexandra Bertz
Patricia Oon

July 2021

Agenda for today

- Stuart sets the scene

- Alexandra covers practical response measures

- Patricia points out the legal technicalities
- Group exercise
- Reconvene to discuss the exercise

Pinsent Masons

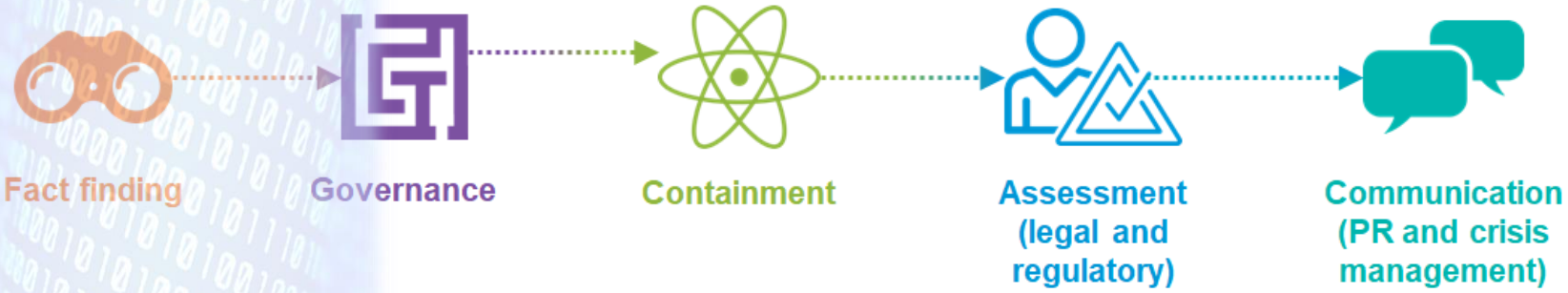
Scene setting

Then…

Now…

Pinsent Masons

How do we respond?



The Cyber Crisis Team

- C-Suite
- Legal
- IT Forensic
- PR/Comms

Pinsent Masons

Notification considerations

GDPR

Personal Data Breach

- a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

GDPR Article 33

- a controller must notify the DPA of a personal data breach without undue delay and where feasible within 72 hours of becoming aware of it. UNLESS it is unlikely to result in a risk to the rights and freedoms of individuals

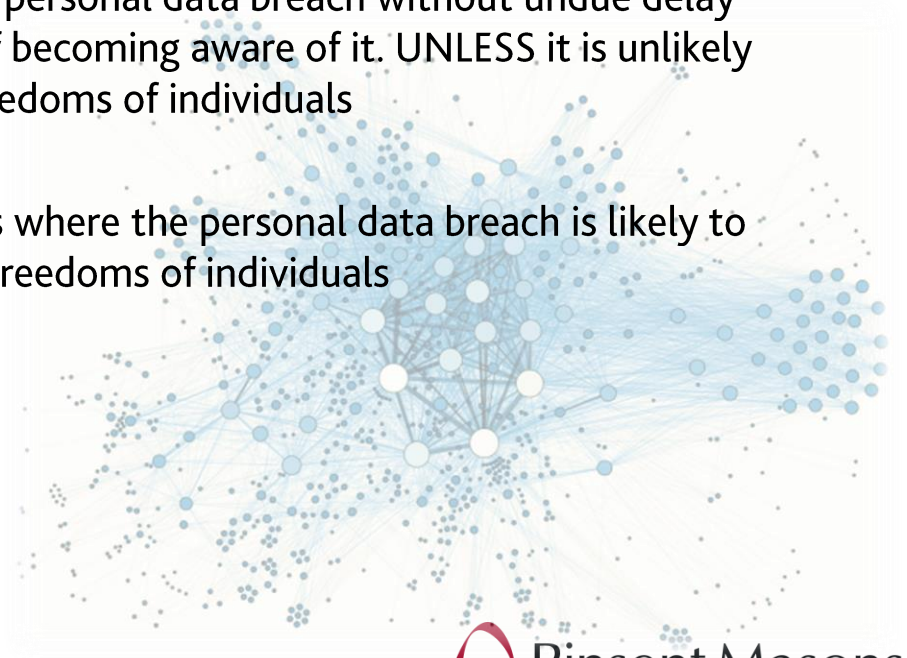
GDPR Article 34

- a controller must notify data subjects where the personal data breach is likely to result in a high risk to the rights and freedoms of individuals

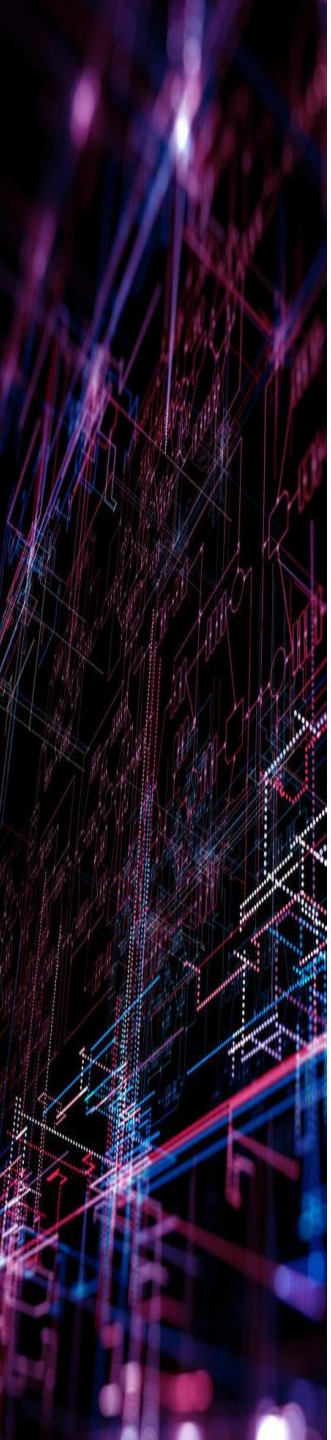
Other regulatory

Contractual

Law enforcement



Pinsent Masons



Group discussion

A ransom note is found….

Pinsent Masons

In your breakout rooms, you will discuss all four questions. Pick someone to represent your group.

RANSOMWARE MESSAGE

| What happened? |

Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED.

| What does it mean? |

It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.

| How it can be avoided? |

In order to avoid this issue, you are to COME IN TOUCH WITH US no later than within 7 DAYS and conclude the data recovery and breach fixing AGREEMENT.

| What if I do not contact you in 7 days? |

If you do not contact us in the next 7 DAYS we will begin DATA publication.

| You have convinced me! |

Then you need to CONTACT US, there is few ways to DO that.

I. Recommended (the most secure method)

Download a special TOR browser: https://www[.]to[redacted]
Open our website with LIVE CHAT in the [redacted] browser:
http:/[redacted]5jhonv.onion/[redacted]
Follow the instructions.

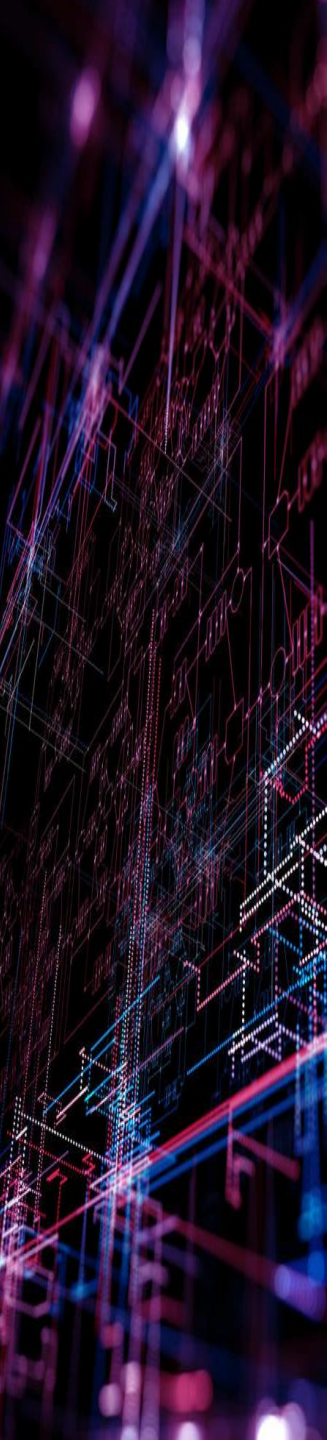
II. If the first method is not suitable for you

Open our website with LIVE CHAT: https://[redacted]support.com/7[redacted]
Follow the instructions.

Questions

1. Who do you reach out to in the first instance? What support do you need, internally and externally? What role will they provide?
2. Do you involve law enforcement?
3. Do you need to notify any regulators? What do you need to think about before telling any individuals affected, including your employees?
4. What are you going to do about the ransom? Will you engage with the threat actor? What do you need to consider before engaging with them?

Pinsent Masons



Any questions?

Pinsent Masons