AON

Welcome to the Law Firm CISO Forum #6

How can firms better prepare for and manage incidents covered by Cyber insurance?



Agenda

- 1. Introduction & brief update on cyber threat landscape for law firms
- 2. New Lloyd's guidance on ransomware claims
- 3. Law firms and ransomware claims a dialogue:

At the onset of ransomware attack – what are the major issues and priorities from a claims perspective?

What does good look like for a law firm managing a claim?

How is this different from general guidance for all organisations?

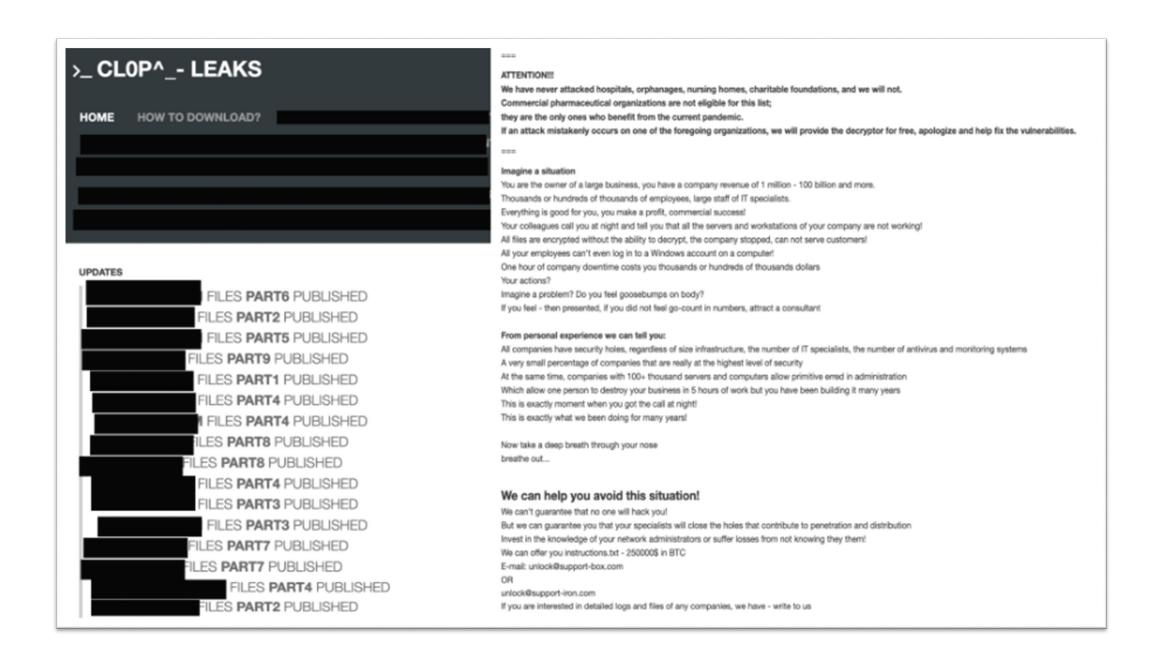
4. Q&A / Peer discussion





ICO fine notice for Tuckers Solicitors

First UK monetary penalty of victim of ransomware attack for GDPR violations



Sample CIOp ransomware notice

Key factors for penalty:

- 1. Lack of MFA
- 2. Took 5 months to patch a critical Citrix vulnerability that targeted remote workers in the pandemic
- **3. No encryption** of server holding archives of civil and criminal trial bundles, with **sensitive personal data** on clients and families
- 4. Keeping sensitive personal data past the firm's own 7-year retention policy

Bright side:

The strength of the victim's response (how they react, contain, and remediate the incident) can mitigate the penalties

https://ico.org.uk/media/action-weve-taken/mpns/4019746/tuckers-mpn-20220228.pdf



Lloyd's market guidance on ransomware claims

Insureds should align and updated their incident response plans

Guidance on due diligence:

Discovery and documentation of ransomware attack

Negotiations with threat actor

Ransom payments

Detailed screening and investigation requirements:

Blockchain analysis / Cryptowallet ID/address checks

Threat intelligence requirements (i.e. TTPs, IPs, domains against threat intel and regulatory databases; ransomware variant name, malware campaigns)

Other checks:

- Is it real person? Do they respond?
- Will they provide samples and allow testing of keys?
- Exfiltration analysis (have they taken copies?)
- Assess risk of re-extortion by same threat actor



https://assets.lloyds.com/media/152f8157-8c79-42b1-8a41-792b3dbc88dd/Y5359-Guidance-for-handling-a-ransomware-claim-incident.pdf



Case Study



A law firm is hit with Ransomware...

The CIO responds immediately and triggers the IT Department Incident Response Plan:

- 1. Assures the Executive Committee that they will work 24/7 until it's resolved
- 2. The firm engages the Managed Security Services Provider's Emergency Recovery Team
- 3. They establish that they have viable backups
- 4. They identify the exploit used by the threat actor and shut it down
- 5. They track down the backdoors left by the threat actor and delete them
- 6. They wipe all servers and start restoring from backup
- 7. The threat actor claims to have exfiltrated sensitive client data and provides file tree snapshots
- 8. The firm immediately authorises a payment of £10m, threat actor accepts and "deletes the data"
- 9. With systems back up and running, the GC reaches out to insurers to make a claim



What did they do wrong?

...almost everything

Assumed it to be a tech problem

No account of enterprise impact – internal & external communications

Disregards regulatory and law enforcement implications / requirements

No recognition of client contractual obligations

Breach of insurance notice requirements / obligations / consents

Engaged existing security service provider to investigate & remediate

Conflict of interests

No privilege / confidentiality protections

Not an insurer-approved vendor

Remediation work compromised forensic evidence



What else did they do wrong?

Did not immediately engage law enforcement

No due diligence around the Threat Actor for sanctions purposes

No preservation of forensic evidence

Missed valuable information on the Threat Actor's "TTP's"

Cyber policy requirement on law enforcement

Immediately agreed to Threat Actor demand

No attempt to verify exfiltration

No knowledge of threat actor behaviors

No negotiation of ransom

Failed to check for sanctions

No consent from cyber insurer



What else did they do wrong?

Only notified insurers once the event was resolved

Late notice compromised insurer's ability to manage the claim

No approved vendors involved

Failure to recognise regulatory implications exposed firm to investigation

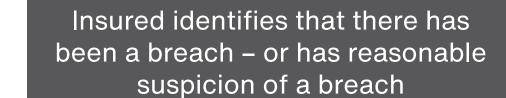
Failure to engage counsel compromised future litigation



Cyber Incident Flow Chart

Pre-Incident Protocol:

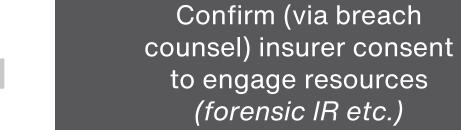
- 1. Identify Preferred Breach Counsel / Forensic Advisors
- 2. If a preferred vendor or breach counsel is not on insurer panel, seek insurer pre-approval through Aon



Contact and engage insurer-approved
Breach Counsel

Contact law enforcement

Engage resources (via breach counsel for attorney/client privilege protection)



Notify all Cyber Insurers - cc. Aon (breach counsel can draft / issue notice to insurers)

Notice Circumstance to Professional Liability insurer (review other policies for cover)



Track and earmark all expenditures and costs



Track and earmark all "business loss" (use "event code")

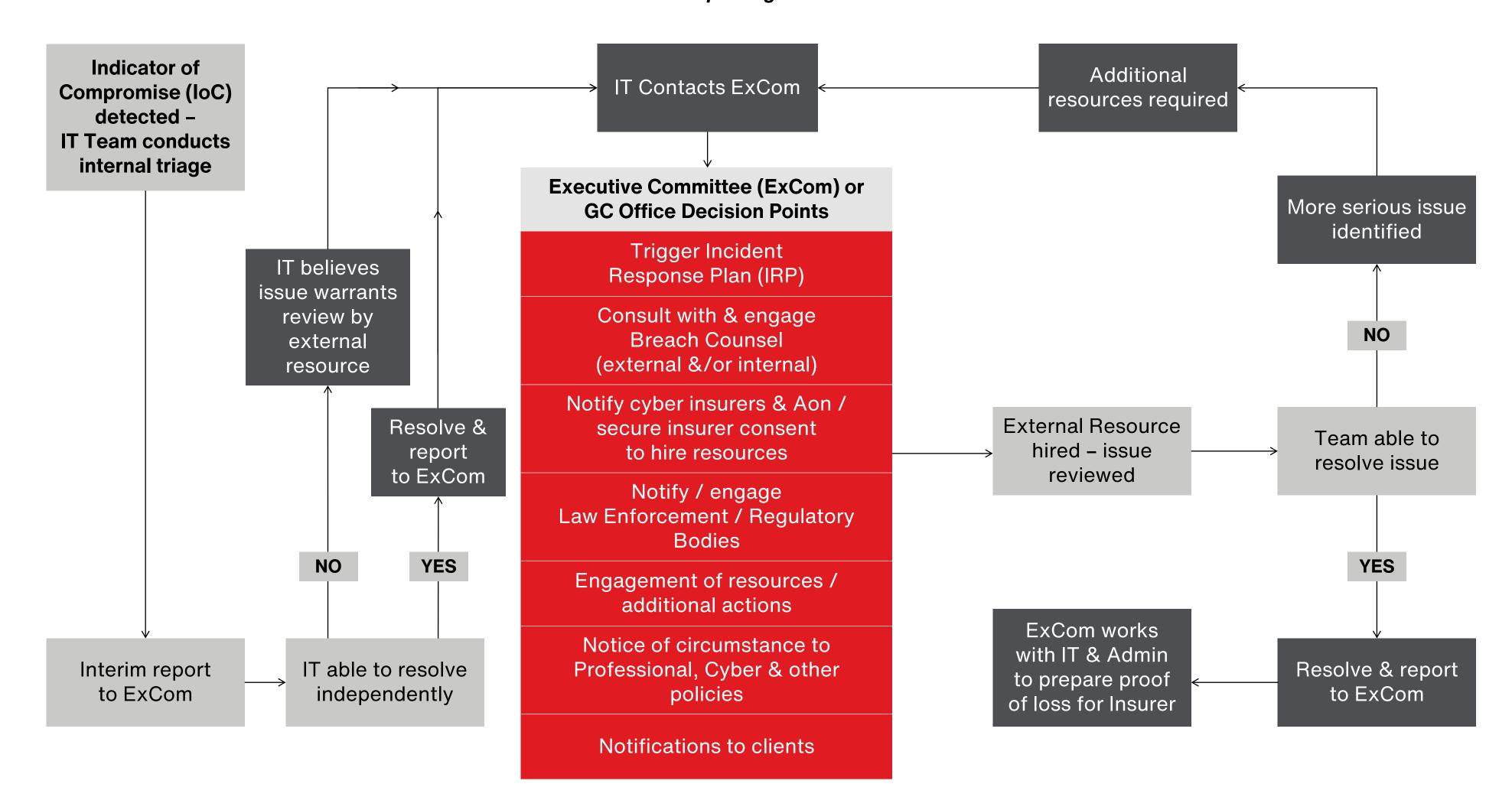


Monitor "Proof of Loss" period – extend as necessary



Claim Readiness Planning

This diagram illustrates how a cyber event response flow might work in a firm where it is coordinated through the Executive Committee or General Counsel's office. It can be modified to account for different internal reporting structures.





Thank You

About Aon:

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.

Follow Aon on <u>Twitter</u> and <u>LinkedIn</u>. Stay up-to-date by visiting the <u>Aon Newsroom</u> and sign up for News Alerts <u>here</u>.

Aon UK Limited is authorised and regulated by the Financial Conduct Authority. Aon UK Limited's FCA register number is 310451.

Registered in England and Wales. Registered number: 00210725. Registered Office: The Aon Centre, The Leadenhall Building, 122 Leadenhall Street, London EC3V 4AN. Tel: 020 7623 5500

