

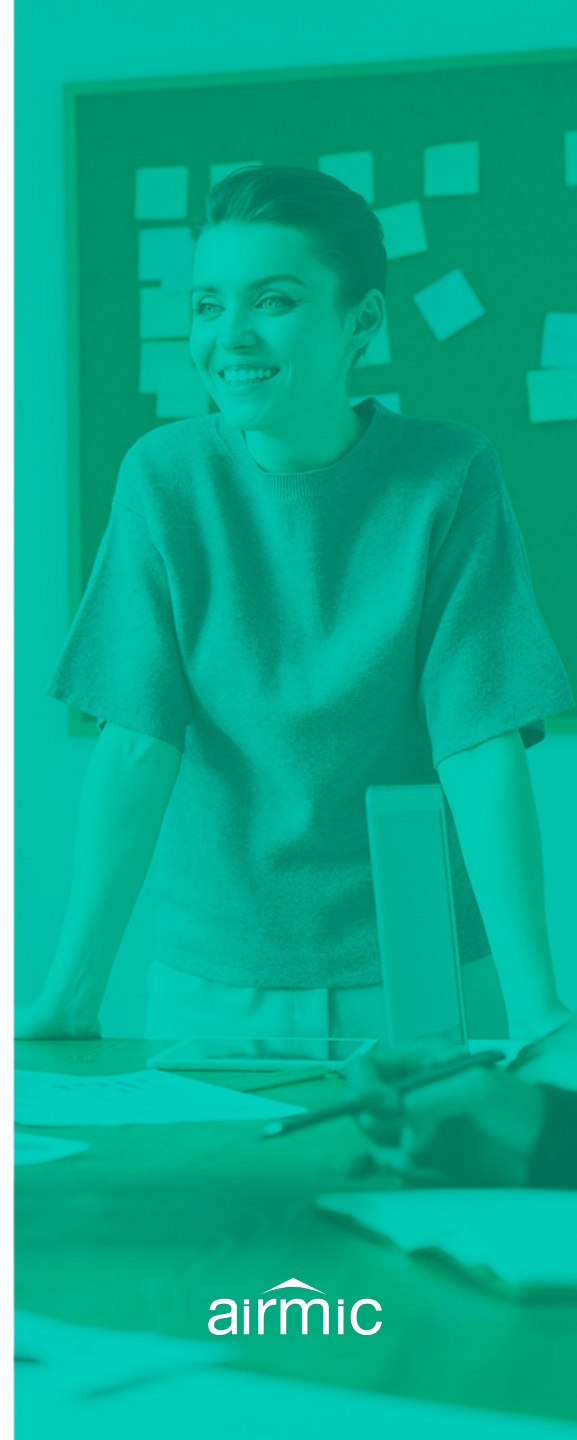
# Cyber Crisis Management

---

airmic academy session

# Introduction

- To understand:
  - the types of information needed to support a response
  - the roles of roles of external advisors (breach coach, digital forensics, crisis comms) and how they interact with the client team
  - the types of decisions faced by a company suffering a cyber incident and the time pressures when making them
  - the role of the regulator(s) and the potential need for regulatory notification not just to the regulators but to consumers as well





# Welcome to the board of ACME Corp

Specialists in the the provision of financial solutions



**Spoiler alert: it's not going to be the best day in the office...**

Please try to live through the experience of your client as we work through a typical incident in compressed time

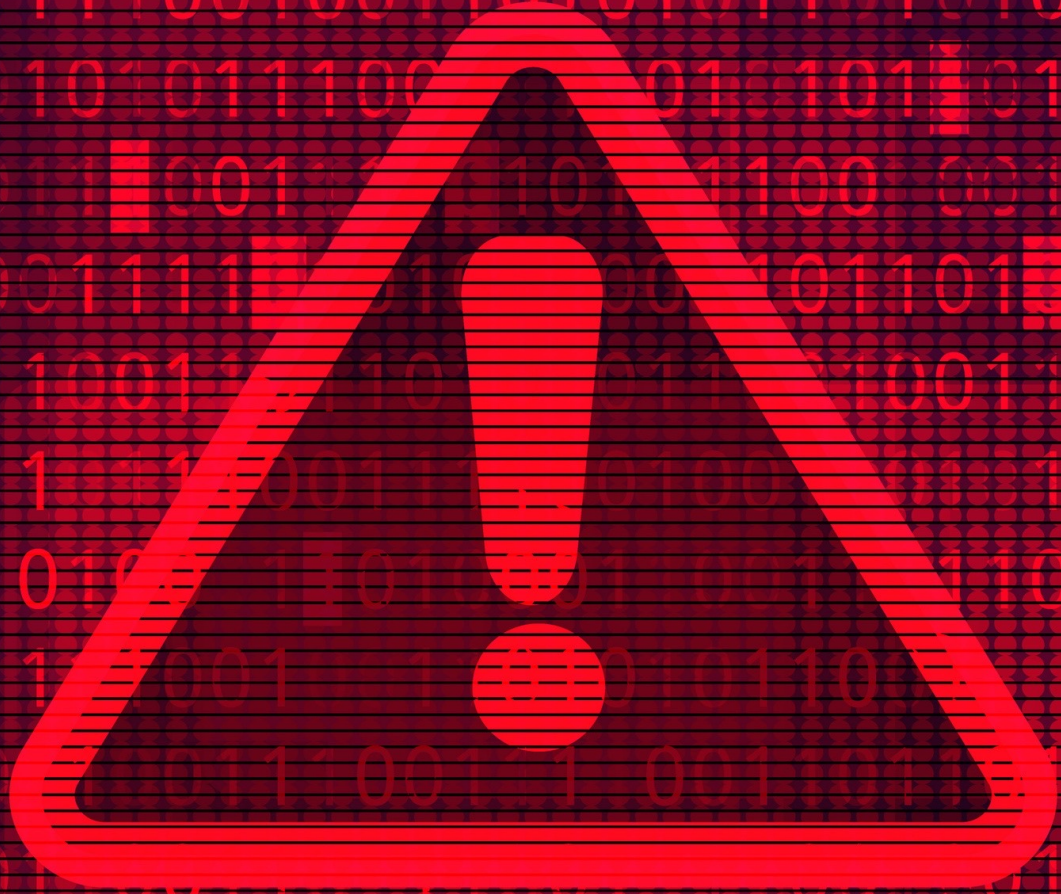
This is based on an amalgamation of the 2700+ incidents responded to annually



# 01

## Scenario

“How do you turn this thing on?!”







## Secure Connection Failed

The connection to the server was reset while the page was loading.

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

[Learn more...](#)

Try Again

☐

Report errors like this to help Mozilla identify and block malicious sites

## Sorry, something went wrong

The service worker navigation preload request failed with a network error.

TECHNICAL DETAILS







# 02

IT find a ransom note



# Friday 08:00 GMT

An update from IT...

Hello friend! Hope you are having a bad day. Ha ha.

\*\*\*\*\*

Attention! Your documents, photos databases, and other important files have been encrypted!

\*\*\*\*\*

Every byte on any types of your devices was encrypted... Don't try to use backups because it were incrypted too...

To get all your data back, contact us:.. SorosSoros@protonmail.com  
jojnBuns@onionmail.ru

Also be aware that we downloaded files from your servers and in case of non-payment we will be forced to upload them on our website, and if necessary we will sell them on the darknet.. Check out our cool website, we just posted there new updates for our special partners:

<http://gghoe5kd3o1g3.onion/>

FAQ

1. How do we trust you? You can send us 2 files for us to prove the decrypt works
2. Shall I contact the police? No! we will upload all your secrets at once!
3. Shall I recover? No. This will damage your data and then even we cannot help you my friend.





Friday 0915 GMT

## Emergency Board Meeting

IT confirms that systems are encrypting rapidly, help is needed to contain the threat. Laptops and servers are affected, though the extent is unknown.

The helpdesk is telling people to shut down their systems and leave them off.

Someone suggests that they've heard that paying the ransom is OK. It's got to be easier than restoring the company to operation, even if that's possible.

Is this really OK?





# Friday 1045 GMT

## Emergency Board Meeting Concludes

The Board decides to keep payment as an option of last resort.

- Insurers are called
- External counsel are appointed to provide a privilege wrapper and initial advice
- Insurers and the CISO recommend an Incident Response firm, who are appointed
- IT are instructed to explore all options to restore services and data. Expectations are set on weeks and months, not hours and days
- Internal comms starts communicating with internal staff on the situations and lines to take with clients. Press packs are prepared 'just in case'
- Insurers recommend a Crisis Communications Firm to help manage the message
- It generally feels like the company's been transported to the 1970's where paper, fax and phone are king





# 03

## Media Reports



**LIVE**

**ACME CORP**

**BREAKING NEWS**

# ACME CORP HACKED?

**13:55** Rumours grow that client data has been stolen



Friday 1430 GMT

## Emergency Board Meeting

Press reports are discussed in detail, although IT and Security note that they've been unable to find any traces of data exfiltration. Encryption is hampering the investigation

Incident responders are providing remote support whilst they travel to site

Internal communications are discussed

External Counsel attend and provide advice on regulatory impact

The board asks the DPO to update them on the impact





# Friday 1515 GMT

## Emergency Board Meeting Concludes

The Board decides to:

- Continue the investigation and prioritise finding out if there is a breach
- Ask the incident responders to see if there's any listing of the breached data on the dark web
- Re-enforce internal communications and remind all staff of the press policy
- Update the press packs
- Give the DPO all assistance to independently consider the risks and provide advice to the board
- Consider the financial regulatory impact






# 04

You have mail....





Saturday 01:10 GMT

Friend,

You have been quiet. Didn't you find our note? We know people are accessing our website and see that we have your data. Currently not many people have that link. But others will find it soon. And if not, we will show people where it is.

We have plenty more data of yours. And we can't wait to show it to:

- Your customers
- Journalists
- Your shareholders

Contact us before we contact them. ☺

[SorosSoros@protonmail.com](mailto:SorosSoros@protonmail.com)

[jojnBuns@onionmail.ru](mailto:jojnBuns@onionmail.ru)

<http://gghoe5kd3o1g3.onion/>



- Incident Responders have found that a sample of sensitive data has been leaked, with more threatened to be released
- Restoration and investigation efforts are underway
- So far, Incident Responders can only see that some data has left, but not what data has left.





# Saturday 0615 GMT

## Emergency Board Meeting

The breached data is the main discussion item. It's verified that the published data is from the company and long discussions continue to discuss what data could have left and review the associated impact

The board asks the DPO to update them on the impact. The Director of Compliance updates the Board on the Financial regulatory impact

Internal communications are discussed

External Counsel attend and provide advice in preparation of litigation.  
Takedown notices and injunctions against persons unknown are discussed





# Saturday 0717 GMT

## Emergency Board Meeting Concludes

The Board decides to:

- Continue to prioritise finding out what data has been exfiltrated
- To begin actively managing the external message in response to grave worries around reputational damage
- Notify regulatory authorities in the UK, EU and beyond through external Counsel
- Discuss paying the adversary to tell them what data has been taken. Specialist negotiator is instructed to contact the adversary
- Discuss the potential notification to individuals at a future date. Short term action taken to find out how to notify and discover any compensating services that could be provided



# Conclusion

- To understand:
  - the types of information needed to support a response
  - the roles of roles of external advisors (breach coach, digital forensics, crisis comms) and how they interact with the client team
  - the types of decisions faced by a company suffering a cyber incident and the time pressures when making them
  - the role of the regulator(s) and the potential need for regulatory notification not just to the regulators but to consumers as well



# Thank you!

For more information, please contact:

Andrew Beckett  
EMEA Regional Managing Director, Cyber Risk  
[andrew.beckett@kroll.com](mailto:andrew.beckett@kroll.com)

Ioan Peters  
EMEA Reactive Services Managing Director, Cyber Risk  
[ioan.peters@kroll.com](mailto:ioan.peters@kroll.com)



For 24x7 Cyber Incident Response, please call: +44 (0)808 101 2168