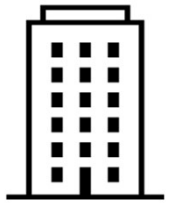
SLAUGHTER AND MAY/

CYBER PREPAREDNESS: THE FINANCIAL INSTITUTION PERSPECTIVE

Guy O'Keefe and David Shone
September 2024

What is cyber risk?

Not just a tech issue



Corporate governance risk

- Board level issue
- Incident impacts BAU, brand / reputation, share price etc.

Regulatory risk

- Key international regulatory focus
- Cross-cutting requirements
- Double jeopardy

Evolving risk

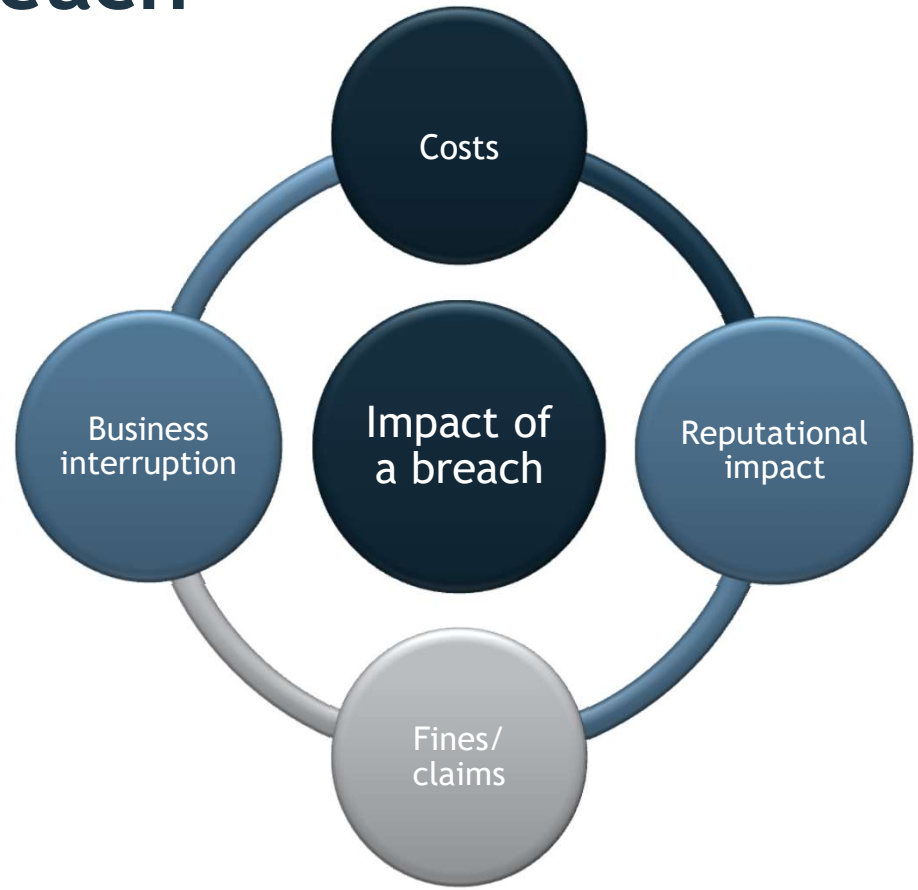
- Threat actors evolve (cyber supply chain)
- Geopolitical, technological and regulatory changes

People

- A very human tech problem
- Training / education
- Role for all employees

Impact of a breach

Why does it matter?



Cyber risk in a regulated environment

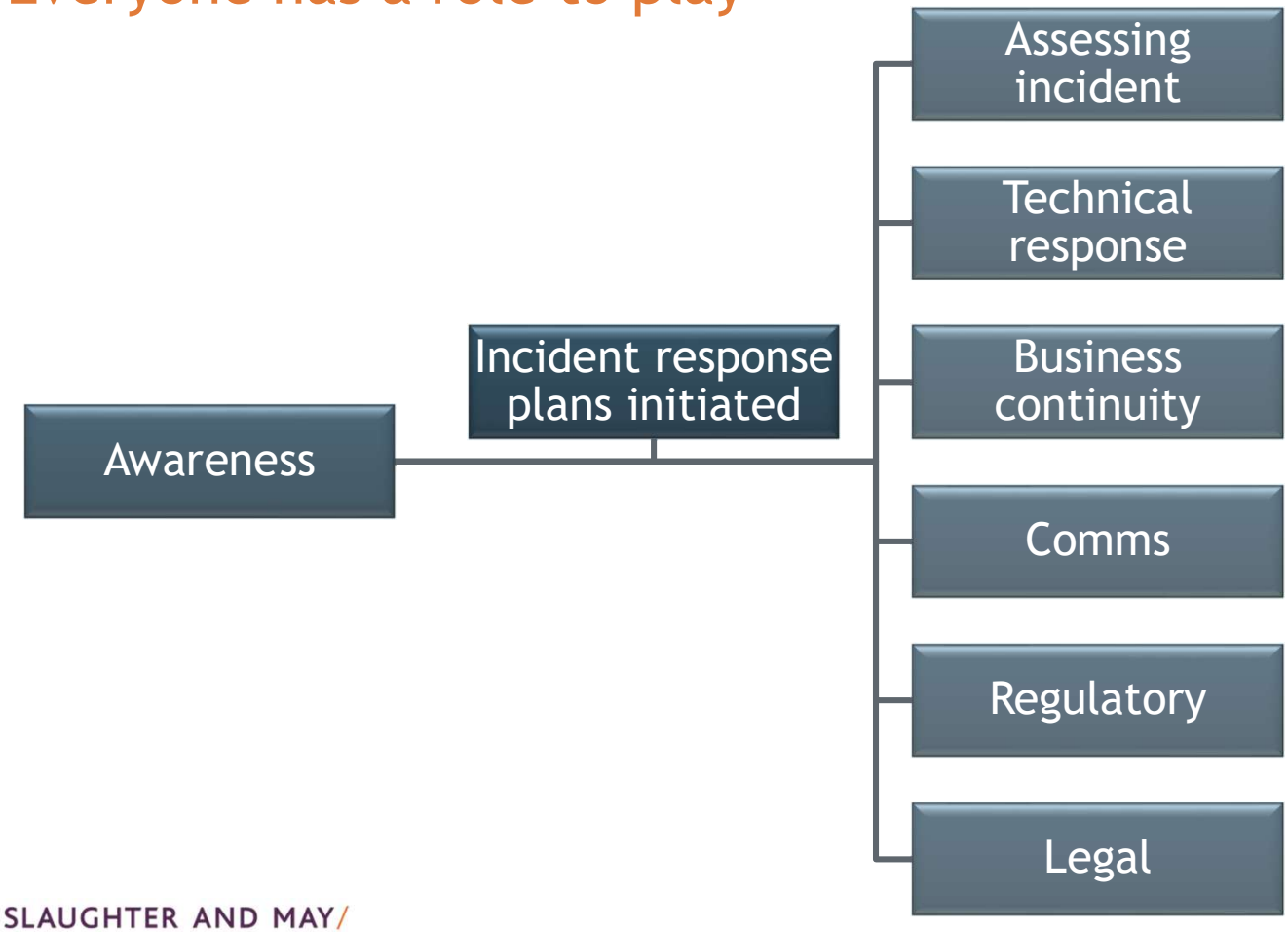
UK and EU regulatory approach

Cyber risk in a regulated environment

Other relevant UK and EU regimes

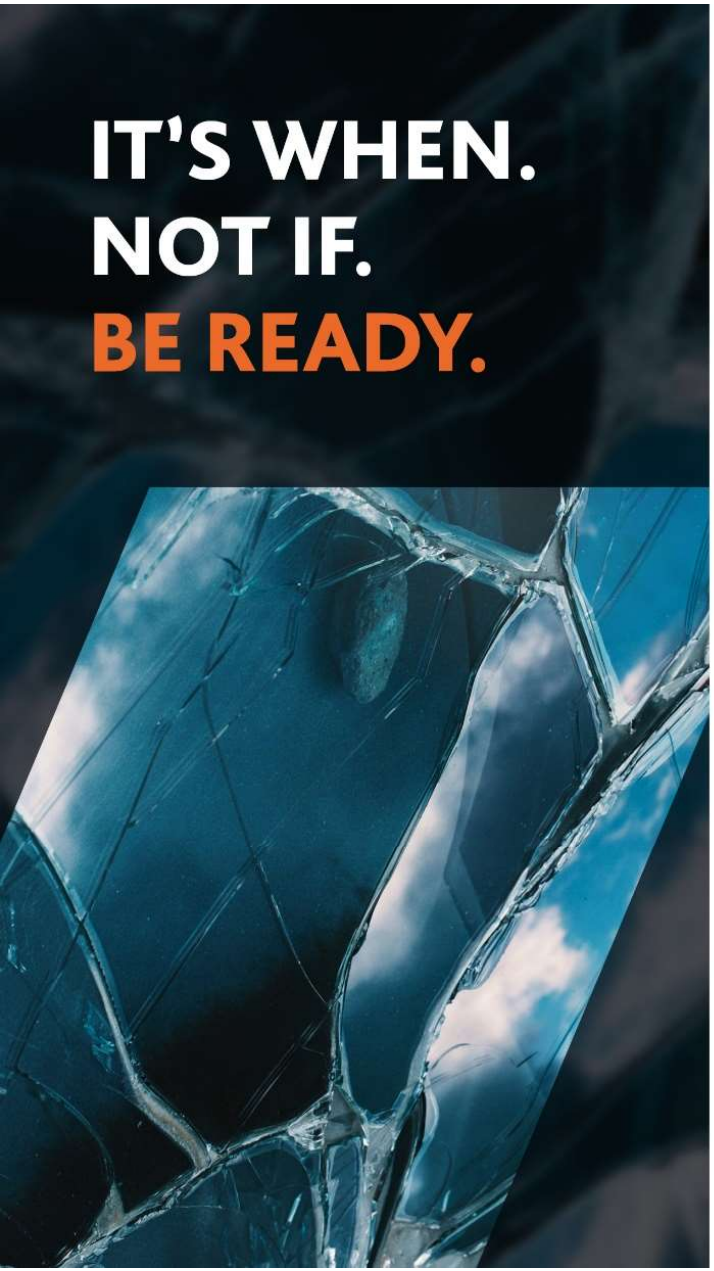
Anatomy of a response

Everyone has a role to play



Stages of a cyber response:

1. Immediate Response
2. Communications and Investigations
3. Longer Term Impacts



SLAUGHTER AND MAY/

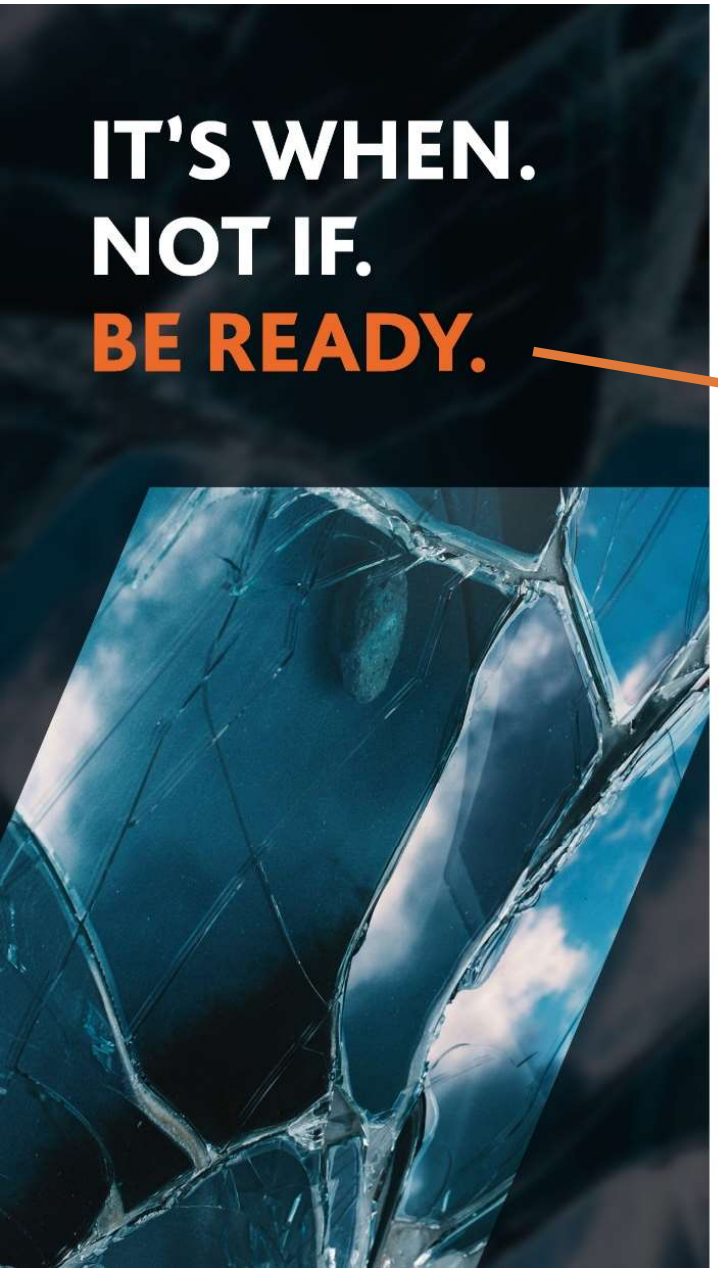
10 CYBER QUESTIONS YOU WILL NEED TO ANSWER

Informed decision making is critical during a cyber crisis. With the answers to these questions and the support of legal counsel, Boards will be well-equipped to navigate a cyber-attack calmly and effectively.

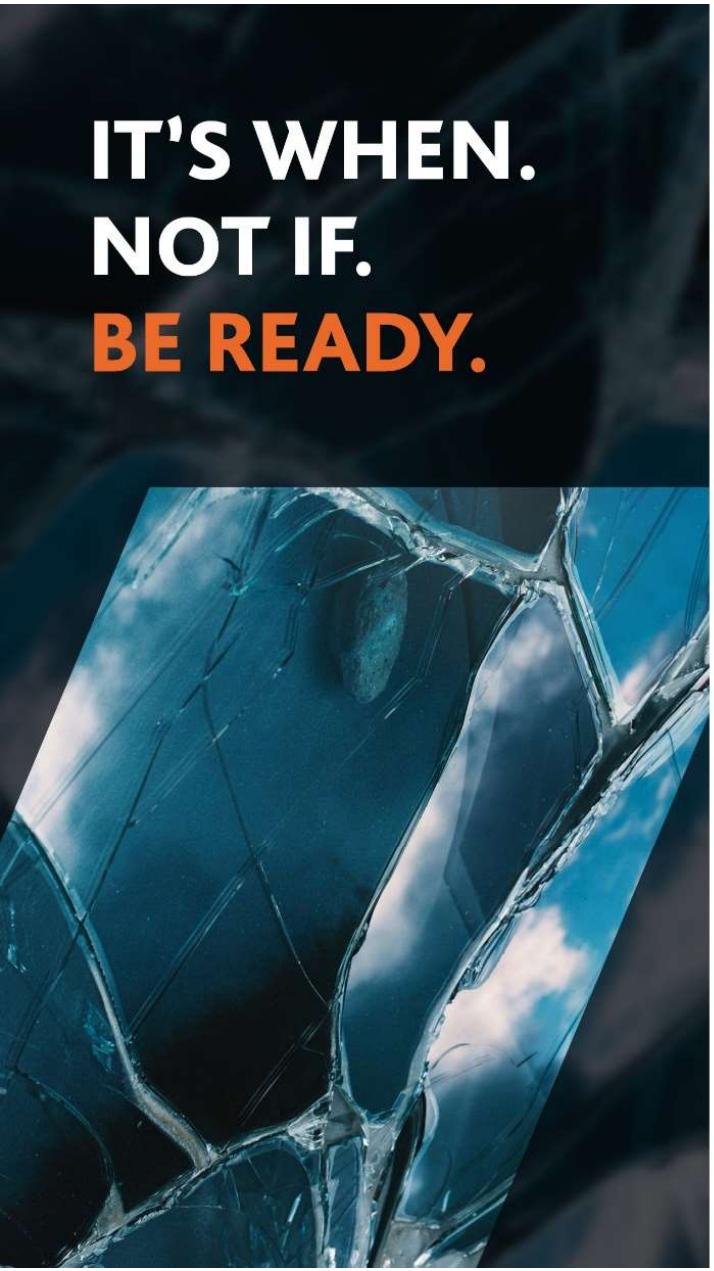
Would you know how to answer all 10 questions?

1. Can we pay the ransom? Do we have a duty to pay the ransom?
2. If we pay the ransom, must we declare this to our auditors, and will they disclose this?
3. Who will conduct the ransom negotiations with the cyber criminals?
4. We're trying to keep the incident response "Gold Team" small – does the legal function need to be represented in that forum?
5. We're being advised to shut down the systems, which will cripple our business – should we?
6. Do we need to make market announcements?
7. We need to communicate with our employees and our customers before this leaks out – can we? How?
8. Will we face a fine? From whom, and how much?
9. The breach has come in through our supplier, and we'd prefer them to deal with all of this – how do we make this happen?
10. This will all be covered by insurance, won't it?

Cyber preparedness is key.



- Preparedness is key.
- Regularly review, update and practice incident response plan.



SLAUGHTER AND MAY/

10 CYBER QUESTIONS YOU WILL NEED TO ANSWER

Informed decision making is critical during a cyber crisis. With the answers to these questions and the support of legal counsel, Boards will be well-equipped to navigate a cyber-attack calmly and effectively.

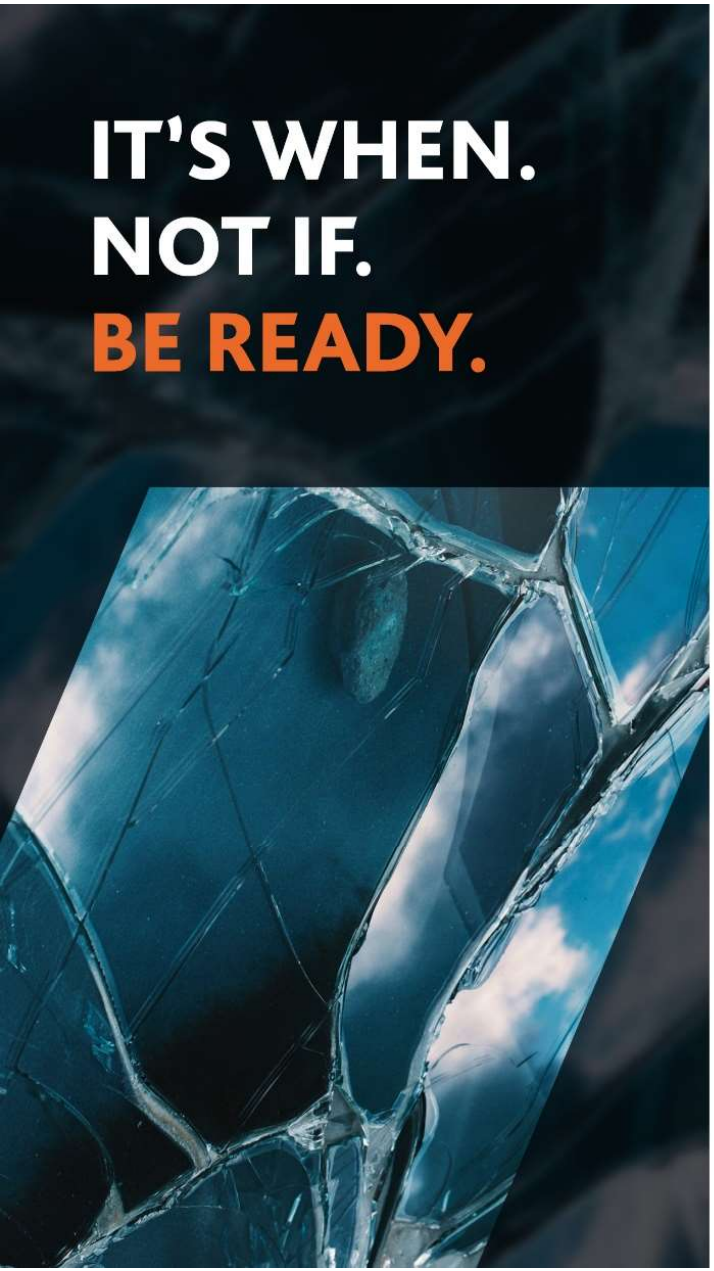
Would you know how to answer all 10 questions?

1. Can we pay the ransom? Do we have a duty to pay the ransom?
2. If we pay the ransom, must we declare this to our auditors, and will they disclose this?
3. Who will conduct the ransom negotiations with the cyber criminals?
4. We're trying to keep the incident response "Gold Team" small – does the legal function need to be represented in that forum?
5. We're being advised to shut down the systems, which will cripple our business – should we?
6. Do we need to make market announcements?
7. We need to communicate with our employees and our customers before this leaks out – can we? How?
8. Will we face a fine? From whom, and how much?
9. The breach has come in through our supplier, and we'd prefer them to deal with all of this – how do we make this happen?
10. This will all be covered by insurance, won't it?

Cyber preparedness is key.

1 Can we pay the ransom?

82% of UK victims pay ransoms v global average of 58% *(Proofpoint research reported in The Times)*



SLAUGHTER AND MAY/

10 CYBER QUESTIONS YOU WILL NEED TO ANSWER

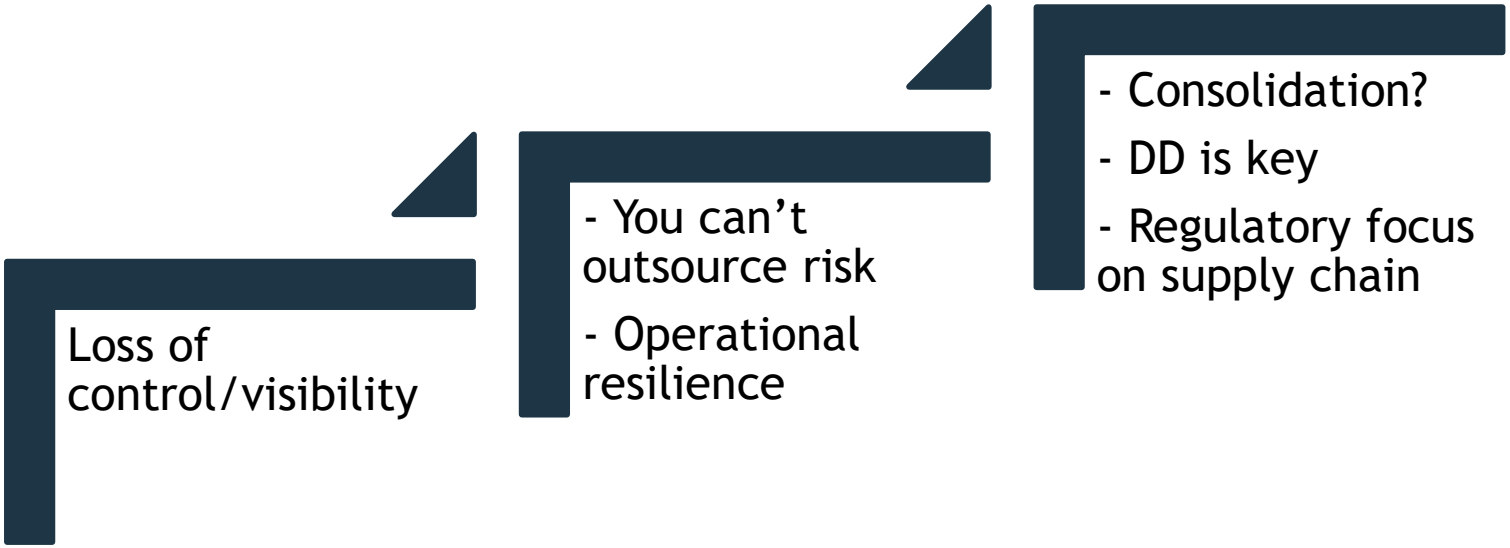
Informed decision making is critical during a cyber crisis. With the answers to these questions and the support of legal counsel, Boards will be well-equipped to navigate a cyber-attack calmly and effectively.

Would you know how to answer all 10 questions?

1. Can we pay the ransom? Do we have a duty to pay the ransom?
2. If we pay the ransom, must we declare this to our auditors, and will they disclose this?
3. Who will conduct the ransom negotiations with the cyber criminals?
4. We're trying to keep the incident response "Gold Team" small – does the legal function need to be represented in that forum?
5. We're being advised to shut down the systems, which will cripple our business – should we?
6. Do we need to make market announcements?
7. We need to communicate with our employees and our customers before this leaks out – can we? How?
8. Will we face a fine? From whom, and how much?
9. The breach has come in through our supplier, and we'd prefer them to deal with all of this – how do we make this happen?
10. This will all be covered by insurance, won't it?

Cyber preparedness is key.

9 Supply chain breach



Types of supply chain breach (examples):

- Smaller supplier = weak link
- Large managed service or cloud provider = attractive target
- New tech, different procurement approach? E.g. AI
- Hardware or software suppliers targeted

Takeaways . . .

- Cyber is a corporate governance risk and the risk landscape is changing
- Prepare for different scenarios (ransomware, supply chain etc.)
- Reflect lessons from drills and real-life incidents

Questions?

PowerPoint Presentation 587008502

SLAUGHTER AND MAY/