IT'S WHEN. NOT IF. BE READY.

SLAUGHTER AND MAY/

10 CYBER CRISIS QUESTIONS GCS NEED TO ANSWER

Informed decision making is critical during a cyber crisis. With the answers to these questions and the support of legal counsel, GCs and 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. Do we need to make market announcements?
5. We're being advised to shut down the systems, but that will cripple our business – should we?
6. We're trying to keep the incident response "Gold Team" small - does the legal function need to be represented in that forum?
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 who, 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.

The Slaughter and May Cyber Hub is often asked how to respond to these questions. We work with clients to understand their cyber risk appetite as part of preparedness activity which ultimately minimises the risk of reputational damage, hefty fines and provides a clear roadmap to navigate a cyber attack, if the event does occur. Arming Boards and GCs with the answers to the 10 Cyber Crisis Questions puts companies ahead in a cyber crisis.

HOW WE SUPPORT CLIENTS IN A CYBER CRISIS

We help clients over all three phases of cyber activity.

1

Preparedness activities as part of cyber contingency planning and audits

a. ensuring your cyber risk management frameworks and contingency plans enable you to act within your risk appetite.

b. supporting to ensure you have the appropriate third-party advisers onboarded and jointly trained with all your teams. Ensuring your primary legal advisers are specified on any cyber insurance policy.

c. helping collaborate and manage cyber risk within your general corporate governance risk framework.

2

Around the clock support in the aftermath of any attack

a. providing expertise, materials and advice to ensure the right decisions are made, in a timely manner, and reflecting your changing needs as the incident evolves. This will include advice on the legality of payment of any ransom, and support to senior stakeholders in their decision whether to pay.

b. coordinating comms strategies to ensure consistency of messaging, including with regulators, staff, key customers, suppliers, and (where relevant in light of ongoing disclosure obligations) shareholders, and to minimise exposure to potential liabilities.

c. ensuring co-ordination with internal and external technical advisors for your global response, including appointing a specialist third-party ransom negotiator, and providing an interface between you and that negotiator to coordinate flow of information and to assure privilege.

3

Longer term investigations and claims support following an incident

a. providing strategic advice and support on any regulatory investigation or enforcement.

b. advising (and acting) on claims and complaints (whether from or against third-parties).

c. coordinating and supporting internal investigation, remediation, and lessons learnt.

GET IN TOUCH

Cyber incidents rarely respect legal or operational borders. Our team of multidisciplinary experts enables us to advise on the full spectrum of issues, helping our clients globally and on all legal and operational issues.

To find out more, get in touch with a member of the Cyber Hub or your usual Slaughter and May contact.