IT'S WHEN. NOT IF. BE READY.

SLAUGHTER AND MAY/

10 CYBER CRISIS QUESTIONS GCS NEED TO ANSWER

Recent ransomware headlines are a timely reminder that 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 these questions?

1. Can we pay the ransom? Do we have a duty to pay the ransom? Aren't there some new laws preventing payment?
2. Who will conduct the ransom negotiations with the cyber criminals?
3. Who do I want to (or have to) tell? The market? NCSC? Regulators? Customers? Employees? And what do I say?
4. We're being advised to shut down the systems, but that will cripple our business – should we? Can we?
5. We're a global business – how do I manage incident response if multiple jurisdictions are impacted?
6. We're trying to keep the incident response "Gold Team" small – do we need the GC on there? And what if we have an incident and can't get hold of the CEO?
7. I've got a complex supply chain – how do I manage its cyber risk, and what do I do if a key supplier is hacked?
8. How do I avoid (or reduce) any fines or claims?
9. This will all be covered by insurance, won't it?
10. How can I ensure the Board can take informed, risk-based decisions around cyber?

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 HANDLE 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) Helping identify and manage cyber risk within your general corporate governance risk framework and applicable legal landscape.

b) Ensuring your cyber contingency plans enable you (and key stakeholders) to act quickly, effectively and lawfully, in line with your risk appetite.

c) 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.

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 (and, if so, how) 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 claims and liabilities.

c) Ensuring coordination 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.

June 2025