Reach for the crisis plan

A data breach can significantly damage a company's reputation, which makes preparing for one all the more critical

DATA SECURITY IS NOT ONLY A legal issue. "It is a significant reputational issue that attracts media attention," says Arthur Artinian, partner in the London office of law firm K&L Gates and a member of its intellectual property group.

"A multi-stakeholder, enterprise-wide strategy is therefore essential. Every business should have in place some form of cross-functional cyber and data risk team that includes representatives from the IT, legal, operational, PR/corporate communications, risk management and senior management/board.

"That team should, if it hasn't already, develop a crisis plan for managing and responding to security incidents in the specific business context."

At an operational level, businesses should conduct a holistic audit and review of how they collect and use data, and test those findings against their legal and regulatory obligations.

"If third parties are involved in the use or collection of third-party data, contracts that are entered into with those parties should impose strict obligations to ensure that legal and regulatory obligations are complied with down the supply chain," says Artinian.

Of course, insurance also has an important role to play in the cyber risk management toolkit, because it facilitates the assessment and transfer of cyber risk.

Assessing coverage

Sarah Turpin, a partner in the litigation and dispute resolution and insurance coverage practice groups at K&L Gates' London office, says: "Some cover for cyber risk is likely to be provided by existing insurance policies, but such policies have not historically been designed to cover the risks arising from intangible assets and network-related risks.

"A careful assessment of the coverage provided by existing policies is essential, as there are likely to be potential gaps in cover, which can be filled either by enhancements to existing policies – where available – or through the new cyber insurance products being offered by insurers."

Although the cyber insurance market has developed rapidly in recent years, the scope of cover provided still varies

significantly. Some policies still impose very onerous terms and conditions that may enable the insurer to deny or limit the cover provided.

"A careful assessment of the policy terms, conditions and exclusions is essential to ensure that the policy is fit for purpose and there are no exclusions or limitations that could prevent payout in the event of a significant claim," says Turpin. "Some insurers are now providing access to their own panel law firms and cyber security specialists to assist insureds in the event of a cyber crime incident or data breach.

"This may prove beneficial in certain jurisdictions, but some insureds may prefer to use advisers they are already familiar with in what can be a crisis situation. Either way, it is worth considering these issues up front and attempting to reach agreement with insurers over who should be appointed.

"The purchase of insurance should be used as part of the risk management process and most insurers are likely to expect insureds to have appropriate incident response plans in place." **SR**

ALL AT SEA: TACKLING THE CYBER RISK TO SHIPPING

The sea has always been a dangerous place to do business and the shipping industry's increasing reliance on computerised systems in all areas of operations brings with it new vulnerabilities.

For example, in July 2013, researchers from the University of Texas demonstrated that hackers can change a vessel's direction by interfering with its GPS signal, which could cause the onboard navigation systems to pick up a false position and heading.

A hacker also forced a floating oil-platform off the coast of Africa to shut down by tilting it to one side, and evidence shows that Somali pirates have employed hackers to access shipping companies systems to identify vessels passing through the Gulf of Aden with cargoes and light security; something that led to the hijacking of at least one vessel.

Unfortunately, awareness of this threat is still too low. Marine operators need to improve their risk management by adopting the same rigorous systems and protocols as forward-thinking firms operating on land.

However, because shipping is, by nature, open and companies rely on interaction with a wide range of partner organisations, more needs to be done to establish global standards.

The International Chamber of Shipping, the Baltic and International Maritime Council, INTERTANKO, and INTERCARGO are developing guidelines and best practices, which it is hoped will be presented to the International Maritime Organization for approval in 2016.

In addition, underwriters need to look at the risks that they are writing, in particular, the way in which these can be aggregated on larger ships running more complex operations.

Everyone involved needs to read the weather well: a storm is brewing on the horizon and the time to start plotting a safe passage is now.