CRITICALEYE
The peer to peer Board Community

Where Next for Cyber Security?

James Mullock, Partner at international law firm Bird & Bird, tells **Dawn Murden** what leaders should do to prepare for the eventuality of a cyber security breach

Cyber crime is now a major risk for boards to manage. The cost of intellectual property theft, industrial espionage and data breaches to UK businesses alone is estimated to be around £27 billion per annum.

Such attacks can have momentous reputational and legal consequences. **James Mullock**, Partner at international law firm Bird & Bird, discusses the current cyber security landscape and how companies can create robust layers of defence:

'Are we prepared to deal with a breach?' That's the question board members are asking colleagues and advisors in the face of well-publicised attacks, such as the TalkTalk breach last year.

Most companies have various flavours of a continuity or disaster recovery plan for different scenarios relating to risk, but they lack one for a major cyber security breach or it's not up to scratch.

Often companies need help creating a resilient response plan in line with key legislation and regulation, while ensuring processes, procedures and training are all up to standard. We are entering a period of substantial regulatory change with new data protection and cyber law imminent, so there is a lot to be done.

One particular blind spot we've noticed is in supply chains. Quite often businesses have allowed access to their infrastructure or data without paying attention to the approaches that their suppliers take; that's often the biggest area of weakness. >

TalkTalk's cyber security incident reported on its website in October provided an interesting snapshot of the regulatory environment that all European businesses may face shortly. As a telecoms provider, TalkTalk is subject to breach notification rules – the obligation to proactively confess to regulatory authorities in the event of a serious data breach.

EU laws are set to change soon and may require all companies to disclose details of such breaches, potentially to both regulators and to affected individuals.

That will be quite a substantial departure from the current legal position. In the UK, breach notification requirements outside of regulated sectors, such as financial services and telecoms, are framed much more loosely.

This is coupled with significant increases to the maximum fines that can be imposed by data protection regulators (four per cent of worldwide turnover for breach of security notification laws) and increasing press interest in cyber breach stories. Businesses need to plan now how they will meet the new standards expected of them.

Businesses that are switched on when it comes to protecting their brand value are getting ready now for Europe's changing data protection landscape. Brands that are not prepared will be caught out by regulators and the general public.

Central to that preparation is having a well thought through cyber incident, response plan that deals with issues such as how you define and categorise incidents, escalation paths for different types of incident and the seniority and job title of those who should consider them. Additionally, the process for deciding whether breaches should be notified to regulators, affected individuals, the police and/or insurers.

> *"We will see more consumer and shareholder action against companies and their boards"*

A board should be asking its legal and technical teams if they identify an issue whether they have planned for it and how they would assess what to do next. In particular, who they have to tell and what they have to tell them. In-house lawyers and compliance teams need to structure incident response plans in a way that makes the best use of concepts like legal privilege, so they can investigate what has happened without creating a pool of evidence that can be used against them.

A Global Issue

The laws I've been talking about are European, but there are different legal environments around the world that need to be taken into account.

Quite often, clients think that data protection laws are predominantly European. In fact, there are over 100 countries that have data protection laws now and just 28 of those are in Europe.

For example, the US is looking very closely at its cyber regulation and has actually led the way on breach notification laws. Many other parts of the world have tough data protection laws, such as Latin America, Singapore, Hong Kong, Japan, Australia and New Zealand.

The introduction of new regulation is one area to be aware of, but I also expect there to be more data and cyber litigation – even if a regulator isn't interested in relation to an incident, the courts are likely to be.

I also think we will see more consumer and shareholder action against companies and their boards. For example, if a share price is affected by lack of preparation, that is a governance issue. And while consumers may understand that breaches can happen, they won't forgive a well-run company that hasn't planned for that eventuality. The best question that a board can ask of its IT, legal and compliance teams now is: 'Do we have a cyber incident response plan and what's our procedure plan for testing it?' ■

James Mullock
Partner
Bird & Bird

James is a partner in Bird & Bird's international data protection and India strategy groups, based in the London office. He advises on information law issues, including in the fields of data privacy, cyber risk and freedom of information and also handles complex technology, communications and outsourcing transactions for both customers and suppliers.

Contact James through:
www.criticaleye.com