SPECIAL REPORT:

CYBER RISK

The existential threat of cyber risk

Cyber risk involves an entire company and lays a brand's reputation on the line. Rather than feel overwhelmed by addressing the threat, directors should seek to understand and manage it effectively or face the potential liability of a data breach causing reputational damage

IN YEARS TO COME, 2014 may be seen as the time everything changed for cyber risk.

Throughout this year and the last, several major breaches have affected the data security of ordinary customers at some of Europe's biggest brands.

In February, a major UK-based supermarket had to deactivate thousands of online customer accounts after login details, including passwords, were posted online, theoretically enabling access to online shopping accounts, personal details and even vouchers.

Between February and March, eBay was hacked and had to ask its users to change their passwords and login details as a result.

These are striking examples of what is at stake when a company suffers a major data breach and everything – brand, public trust, perhaps even the bottom line – can suddenly be affected.

"Cyber risk is growing and the rate of change is growing," says Peter Jopling, chief technology officer at IBM Security Software. "Hackers are adapting more and more – software can now be rented to attack companies and organised crime gangs are moving in because of the potential high gains for little investment.

"There are also ongoing state-sponsored attacks."

According to IBM figures, average organisations were the victims of about 91 million attacks in 2013 – any type of company, in every market, in all sectors, is at risk.

"There are ever increasingly sophisticated phishing scams, stenography," says Jopling. "In a nutshell, if a company has something people want, they will go for it; that is guaranteed."

Across the corporate world cyber is now seen for what it really is, namely a systemic threat, something that involves the entire company and a risk that has now moved beyond the level of accountability traditionally assigned to it.

However, a gap remains between this realisation and what is happening on the ground. Jopling says: "The challenge is that organisations are unable to see what is happening either because they don't have the right technology or the right processes to bring all the information together in a non-technical environment and fully appreciate the risk."

Attitudes have to change and risk managers should encourage this.

Take responsibility

"One of the key risks for businesses is that, until recently, directors were overly relying on IT, at times being afraid or overwhelmed by the risks," says Iain Ainslie, technology and cyber underwriter at ACE European Group. "If you asked a director what would happen in the event of a virus attack, they would likely refer you to their IT department. However, were you to ask them what would happen if your website were down for three days and the answer would probably be more direct. The question has to be asked in the right way, thus enabling risk managers to better understand the risks."

> *'When senior management ask me about [cyber] issues, I encourage them to think about the types of technology their company was using 10 years ago, and how much they relied on computers to run their business'*
>
> **Toby Merrill,** ACE Group

Already, attitudes are changing. "The financial effects are becoming more and more obvious, and so [cyber] becomes more of an issue for boards," says Wil Rockall, director, information protection, at KPMG. "[Cyber risk] is no longer seen as a mere technical problem with a technical solution; it is an organisational risk, a people risk and a structural risk.

"The biggest change of the past five years is that 'cyber' has become a much more widely used term. Five years ago, only financial services firms were concerned. However, there has been a significant upswing in carefully targeted attacks," he says. Hackers have moved on from untargeted attacks that would have raised their profile "in front of their online friends. Individual firms and even M&As are [now] being targeted."

Although the chief executive does not have to know the detail, they do need to understand the bigger picture and who is responsible. In the end, directors are responsible for the risks to their businesses, including cyber: see box overleaf.

Toby Merrill, division senior vice-president of ACE Group's global cyber risk practice, says: "When senior management ask me about [cyber] issues, I encourage them to think about the types of technology their company was using 10 years ago, and how much they relied on computers to run their business. Then, I ask them to look at how much they are relying on technology today. All industry sectors now run on technology.

"The scary concept for senior management is to think about the technology they will be utilising in 10 years' time, how much this will increase and how the benefits of increased technology come with increased risks. Companies need to understand that equation."

'About 35%-40% of breaches arise from staff losing data. This percentage tends to be at the higher end at smaller firms because there isn't as much investment in training; staff simply do not understand the downside of failing to handle data correctly'

Iain Ainslie, ACE European Group

Success involves understanding the new normal.

A total solution

Each company has unique needs and vulnerabilities that need to be specifically addressed. According to Jopling, the key is moving from a reactive to a proactive approach that involves the entire company.

Kyle Bryant, ACE Group regional manager, cyber liability, Continental Europe, agrees: "Risk transfer is only part of a successful response to cyber risk. A comprehensive risk management risk solution also needs to include loss and breach prevention and a crisis response.

"The primary job of a risk manager approaching the [cyber] issue is to build a culture of primary risk management. They need to clarify how this risk is managed contractually and whether: proper due diligence is being performed regarding vendors; clear staff policies have been developed and are being enforced; internal teams are in place to manage the risk; there is an internal council, be that legal or PR, who is ready to manage any exposure; and the business is ready for the additional exposure it will experience when transferring data overseas."

In all too many companies staff are still incentivised to do things quickly and cheaply. "That isn't the most secure approach," says Rockall. "This situation will change only from the top, when leaders start saying that this level of risk is not acceptable."

Above all, any approach needs to be thoughtful. Bryant says: "What works in Finland may not work in France because regulators there are different and have a different attitudes towards how companies should be managing [cyber] risk, and that feeds into day-to-day risk management."

The situation is always evolving and security should therefore also be dynamic.

"Get the basics right," advises Jopling. "Don't click on links you don't trust; make sure your stuff is patched. The risk of advanced persistent threat will always remain. If someone wants something from you, they will spend a lot of effort to get it and spend months or even years looking for a weakness. But a lot can be achieved with

'Experience is key. Cyber products cannot be looked at on premium alone'
Kyle Bryant, ACE Group

good housekeeping and being aware, staying well informed, making use of the available intelligence and having the right governance.

"It is important to know how to react quickly to minimise the risk to the business. The game has high odds: a business has to be right 100% of the time, whereas a hacker has to be right only once."

Start with the staff

Understanding vulnerabilities is key. To be successful the right people, processes and technology are required, as well as a strong appreciation of the risk across the organisation.

"About 35%-40% of breaches arise from staff losing data," says Ainslie. "This percentage tends to be at the higher end of the scales at smaller firms because there isn't as much investment in training; staff simply do not understand the downside of failing to handle data correctly.

"However, it doesn't have to be like this. Just look at the progress made with other risks. For example, staff are trained to evacuate a building in the event of fire; everyone understands it. That's the position we need to reach with data security.

"Cyber risk worries and scares many people, including risk managers. However, a lot can be achieved through simple staff training and procedures, by giving people clear guidelines. Encryption should be used and a safe internet usage policy should be in place. It's an easy win."

Organisations with a more highly tuned sense of risk are already ahead of the game and those that already have an ERM function seem to have grasped the cyber issue well.

"Having an appropriate ERM function within an organisation enables companies to look at cyber risk as another form of risk to performing their business," says Merrill.

"They can assess the risk, look at their controls and put it all into terms that directors can understand. When they do, it quickly becomes obvious that [dealing with cyber risk] involves more than firewalls and encryption; it's about culture and behaviour. Companies that have this process are moving forward, but those that don't are still trying to understand what they have."

Risk transfer

Good insurance cover has a critical role to play, but before an organisation can transfer risk, it first should understand that risk. However, many companies are struggling to assess their cyber exposure, which is why choosing the right insurer in a crowded marketplace is critical.

"A major part of the insurance industry's role is to provide the tools and information to help companies put numbers against their risk," says Ainslie.

"ACE can also help with mitigation. That's an added benefit. At the end of the day, an insurance company has to be comfortable with [a client's] ability to manage a risk, otherwise, it will not provide cover. Risk management is an integral part of risk transfer."

Bryant says: "ACE offers a reflective, thoughtful insurance backstop. We provide access to the people who can coach clients along the way, help them make the best decisions and help them obtain the best reputational management advice; and it works."

All too often, middle-market companies, in particular, do not have the scale to leverage their relationships with other providers and build effective internet response teams, and this is where insurance can help.

"[Insurers] can help make [clients'] money go further," says Bryant. "Middle-sized companies also struggle to maintain a global view, and this is where ACE can help: we have a worldwide footprint and we understand that data is borderless. A breach could occur in Egypt or the US and we can help clients deal with that.

"Experience is key. Cyber products cannot be looked at on premium alone. The primary exposure here is reputational, and that requires real experience.

"No two breaches are alike, and insurers need the breach experience and range to be able to address clients' specific circumstances with confidence."

Expect the worst

The most important element to remember is that cyber is not a problem that can be solved, but a threat to be managed. The truth is that, although the effects of a cyber attack are now greater and more public than ever before, attacks are also more likely.

All the high-profile victims of recent months had large, well-funded security apparatus, and yet, these failed when attacked.

This makes day-to-day risk management more crucial than ever. It means that organisations have to develop a greater understanding of the risk at every level and a greater preparedness across the board. Companies need to protect, be prepared – and partner well – so that they are ready when the worst happens.

"This is an emerging world where surprising things happen all the time, and it's hard to be current all the time," says Merrill. "However, it is vital to try." SR

Understand the risk – or face the consequences

If directors fail to take cyber risk seriously, they may face a risk to their jobs and their reputations. "All too often directors fail to fully understand the risk until it hits them," says Toby Merrill, division senior vice-president of ACE Group's global cyber risk practice. "Cyber is only a natural extension of the other risks that a company is exposed to and directors need to be able to understand it, otherwise they are potentially violating their obligation as directors of the company," he adds. "That could have serious consequences."

If the company's bottom line is adversely affected following a severe reputational damage from a cyber breach, shareholders can react aggressively and, in the US, derivative shareholder lawsuits have already demonstrated board-level exposure.

These cases raise first-party and third-party issues, and directors' and officers' insurance was not designed to address this.

"ACE's experience suggests that companies cannot rely on traditional insurance policies for cyber risk coverage today," says Ainslie. "We encourage our broker partners to re-examine and interrogate their complete risk transfer programme."