

Sponsored by



► **A breach too far?** - The need to get hold of cyber risk is a fact of life for all. This means gaining a real understanding of the risk and putting in place the right processes to deal with it. David Adams asks just how much cyber risk management is enough risk management?

► **To err is human** - The growing trend to protect against cyber risk by investing excessively in technology and not in other influencing factors such as human behaviour is a common mistake made by companies today, says Xavier Marguinaud

## Cyber risk management



Sponsored by

In the short time between this article being written and its publication, more organisations will have been forced to announce that their systems have been compromised and data stolen. More people will have suffered fraud as a result of these breaches, and the media will have continued to report on allegations of state-sponsored cyber attacks on governments, global institutions and businesses.

For corporate victims, the potential impact of cyber risk is widely covered in these pages. The most recent spectacular story probably being the US\$350m discount that Verizon negotiated in the asking price for Yahoo!, after the latter disclosed the true extent of prior security breaches.

Wherever you look, cyber risks are a very real threat. The World Economic Forum 2017 Global Risks Report places data fraud or theft at number five in its top 10 global risks ranked according to likelihood – just ahead of cyber attacks at number six.

The positive news is that more organisations appear to be translating increased awareness at board level into action. Research from Deloitte suggests that 87 per cent of FTSE 100 company boards now identify cyber as a principal risk. In part this may be because investors have reached similar conclusions: almost three quarters (73 per cent) of investment professionals questioned for PwC's 2017 Global Investor Survey identified cyber threats as a concern.

Although organisations working within the most tightly regulated industries face the most exacting compliance requirements in relation to cyber risks, the scope of data protection regulation is increasing, with the European Network Information Security Directive (NIS) and General Data Protection

## A breach too far?

**▀ The need to get hold of cyber risk is a fact of life for all. This means gaining a real understanding of the risk and putting in place the right processes to deal with it. David Adams asks just how much cyber risk management is enough risk management?**



Regulation (GDPR) both due to come into effect in May 2018.

Yet while regulation is an important driver, experts stress the need for organisations to avoid treating cyber risk management as another compliance activity. The aim should instead be to attain a comprehensive understanding of these risks, to inform business decisions and strategy.

Risk managers across all sectors identified digital risks, including cyber attack and data privacy, as crucial issues when surveyed for the European Risk and Insurance Report 2016, published by the Federation of European Risk Management Associations (FERMA).

"There was a strong view from risk managers that the mitigation level for such risks needs strengthening," says FERMA President Jo Willaert. "We believe this requires an enterprise-wide approach led by the board."

Steve Williams, partner, technology regulation, at legal firm Moore Stephens, says he has seen

a general increase in awareness and understanding of these issues at board level. He says the calls he gets from organisations asking for help now tend to come from the FD or the COO, rather than the IT director, suggesting not just greater awareness but also a better level of understanding on the board. He believes that pressure from investors and other stakeholders, such as non-executive directors, may be a more important factor in driving progress than regulation, in the UK at least.

Others are more cautious. Richard Horne, cyber security partner, PwC, suggests that "a lot of boards realise they need to be giving this their attention, but don't really know what they should be doing". He suggests that while there are some companies performing well in this respect within every sector, many more still lag some distance behind.

Parts of the financial sector appear to be doing well. Ben de la Salle, chief information security officer at Old Mutual Wealth, says cyber risk is now

“a consistent focus” for the boards of the companies in the Old Mutual Group, thanks to increased media coverage, internal risk modelling and exercises and regulatory pressure.

“I do feel this is seen as much more than a regulatory requirement though,” he says. “It is seen as a core component of responsible business.” He says what is happening inside his company appears to match what other CISOs in the financial sector tell him is happening inside their organisations.

But companies operating in highly regulated sectors tend to benefit most from the work of risk management and IT security service providers. Paul Martin, now an adviser on risk to IT security firm Context Information Security and a former director of security at the UK Parliament, expresses concern about the standard of cyber risk management elsewhere; in local government, educational institutions, SMEs, and not for profit organisations, for example.

Any organisation seeking to improve cyber risk management can at least now find plentiful general advice about how to go about creating a cyber risk management strategy.

Horne has written a paper for PwC outlining seven principles that boards should use to improve governance of cyber security risks. These include gaining a real understanding of exposure; use of appropriate capabilities and resources; adoption of a holistic framework incorporating meaningful measurement of security controls and risk exposure; using independent reviews and testing; investing in sufficient incident preparedness (to identify, respond to and learn from incidents); developing a considered approach to legal and regulatory environments for cyber security; and making “an active community contribution” – in the

form of collaboration for information sharing with other businesses, law enforcement or intelligence agencies and even customers.

The WEF has also published a set of ten principles for boards to follow to advance cyber resilience, within a wider report on the subject. They include assigning responsibility for the oversight of cyber risk and resilience at board level; and nomination of a corporate officer who will be accountable for reporting on management and improvement of cyber resilience.

The WEF also stresses the need to integrate cyber risk assessment into overall business strategy and enterprise-wide risk management. Other principles relate to definition and regular review of the organisation’s risk appetite; to risk assessment and reporting, resilience planning and external collaboration. FERMA endorses the WEF principles and report.

Buy-in at the top of the organisation, defined responsibilities and accountability will help; but there must also be effective communication of risk information to decision makers. Horne emphasises the need to understand potential impacts; and has particular concerns about situations where organisations do not really understand risk exposures related to external factors, such as risks related to suppliers or service providers.

Andrew Johnson, a partner in the cyber risk services department at Deloitte, highlights the difficulties an organisation may have in establishing the actual extent and nature of its extended IT infrastructure, including all external IT services being used – and perhaps relied upon.

Even if an organisation does have a good understanding of technology risks and can create strong technical measures to mitigate them, there must

also be a focus on the human element in cyber risks, says Martin, including both accidental and malicious actions. A well-informed risk strategy must be complemented by an effort to create a more cyber security-aware culture – although the difficulties of doing that successfully are well-known.

As for collaboration with other organisations, progress is being made, but not in a consistent, coordinated way across industries or national borders. Willaert praises the work of some existing initiatives, including the Cyber Essentials programme in the UK; and information sharing in France involving insurers, the French risk management association AMRAE and the French cyber security agency ANSSI. FERMA is considering this issue in a joint working party with the European Confederation of Institutes of Internal Auditing (ECIIA) looking more broadly at governance process improvements to help organisations manage cyber risks. They will publish recommendations in June.

Old Mutual Wealth’s De la Salle hopes to see a standardised process for describing and analysing information shared in this way. “Greater guidance or the definition of standards on how metrics and information can be shared would be useful, but these standards should be adopted by all initiatives rather than each defining their own,” he says.

Yet while standardisation will help in some respects, principles such as those outlined by the WEF and Horne may be a better starting point, given that cyber risks continue to evolve rapidly and endlessly. This means that, above all, cyber risk management must be an ongoing process, of review and improvement. As Martin says, “You’re never going to reach a point where you don’t need to do any more.”

**H**aving carried out cyber risk assessment analysis for several industries globally, I am always surprised to find that many companies (from SMEs to large companies) follow the same trend. Board members, CEOs, risk managers and IT managers are, when considering solutions to mitigate cyber risks, focusing heavily on technology based solutions and technical tools; and failing to consider the human factor.

But why do we tend to react this way when discussing cyber risk? One explanation could be that in striving to understand how to manage this once emerging risk, we incorrectly assumed that we could develop technology to deal with the problem and allow us to forget it and get on with the business of business.

Another feasible explanation could be that investing in tangible and visible assets is more reassuring to the business executive or risk manager. The less tangible alternative of developing training programmes offers results and relevancy that are more difficult to measure and assess. It just doesn't seem as solid.

But executive directors, board members and risk managers are not alone in making this mistake. Advisors, insurers and other specialists fall into the same trap.

#### Prevailing human error

Even though never-before-seen cyber-attacks hit the headlines, the reality is completely different as a large number of incidents can be traced back to human error. Company networks are built, maintained and supervised by people... and people are fallible.

In 2015, the remarkable Baker Hostetler Data Security Incident Response Report identified human error as being the leading cause of cyber incidents. This year's report

## To err is human

**▀ The growing trend to protect against cyber risk by investing excessively in technology and not in other influencing factors such as human behaviour is a common mistake made by companies today, says Xavier Marguinaud**

says that human error continues to be a significant source, with phishing, hacking and malware taking the number one spot and accounting for about 31 per cent of incidents.

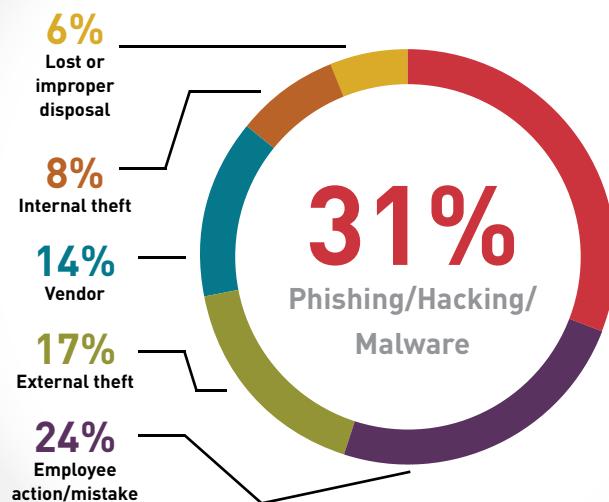
Interestingly, when focusing on the root cause of these incidents, the human factor is often the underlying cause: staff replying to a phishing email, a vendor sharing sensitive data on social networks or employees plugging an infected USB drive into the company system.

According to the authors of the Baker Hostetler report, we can

comfortably say that human error is still a predominant factor in cyber incidents "over half of the time". And attackers are clearly conscious of this weakness, taking advantage of the vulnerability by relying more and more on phishing emails to bypass security network perimeters.

Generally speaking, company network perimeters are improving. And this is just as well. Social engineering (spear phishing, baiting and tailgating) is, according to Security Through Education, a vector used in over 66 per cent of all attacks

Top causes behind cyber attacks in healthcare, retail and restaurants/ hospitality, and financial services



Source: Baker Hostetler 2016 Data Security Incident Response Report

conducted by hackers, hacktivists and nation-state attackers.

From my point of view these techniques, although highly time-consuming, have an unprecedented cost/effectiveness ratio. Most of the time, they successfully allow attackers (even unsophisticated ones) to get access to well-secured networks.

New societal and cultural behaviour, related to the use of LinkedIn, Facebook and Instagram, makes their job even easier. Social media represents a goldmine for individuals looking to identify and target employees. With this wealth of information at their fingertips they can tailor-make phishing emails.

Not many people can exploit zero-day vulnerability in software but a lot of us can trick an employee or a third party vendor to get his/her direct or remote access credentials or to upload some infected files.

It is also naïve to limit human factor causes to malicious targeted actions alone. Staff and vendors can also be their own worst enemies by failing to respect procedures such as patch management and information security protocol; loss of mobile devices, emails sent to unintended recipients, and improper disposal of documents can all figure in the list of causes.

#### **Best line of defence**

Given that employees are among the causes of a significant number of cyber incidents, what can companies do to mitigate this risk?

I believe companies should focus their efforts on reversing this trend and making staff their first line of defence against cyber attacks, alongside the appropriate technical and technological tools. To best position themselves and be cyber resilient, companies should look to:

- Set up clear expectations in

**terms of information security and procedures** This can be achieved by having an intelligible, factual and easy to understand policy, approach and strategy. These should be communicated not only to the entire organisation but also to third party organisations. It is also vital to keep all documentation, campaigns and programmes updated in order to address the constantly evolving threat landscape as well as organisational changes that impact data privacy and security.

- **Develop and run adapted awareness campaigns and training**

A good security culture can be emphasised by training and regularly updating all stakeholders via executive directors. As the National Cybersecurity Institute states: “Without training, workers will likely lack the skills and knowledge they need to adequately protect their companies’ networks from cyber attacks”.

- **Test employees on a regular basis**

With one of the most common attack routes being phishing emails, companies should develop specific testing campaigns and share useful feedback and tips with their employees. When you consider that the average company with 10,000 employees spends US\$3.7m a year dealing with phishing attacks (according to the Ponemon Institute) and that phishing attacks are successful mainly due to the untrained eye, in a test scenario one can quickly calculate the cost of not focusing on some specific details.

This kind of approach can help measure the existing baseline susceptibility of employees – identifying those who may need additional training, and measure the organisation’s progress towards reducing user click rates. Regulators across the globe are aware that

phishing attacks are the main cause of external data breaches, and organisations that have a mature anti-phishing approach ought to get some credit for this in the event of a breach.

- **Support security culture with comprehensive and effective technology and processes**

Some technologies and processes could have a significant impact on the likelihood and financial impact of a cyber incident. Data encryption, data loss prevention software and access management are just a few examples of what could be deployed alongside a healthy data security culture. A comprehensive risk management approach should also take into consideration human factors.

Well-informed people and well-designed processes also need to be taken into account. One should not lose sight of the fact that there are three pillars upon which companies are safeguarded: people, technology and processes. Being cyber resilient means a complete and collaborative approach that is driven by the board, involves everyone within the organisation and extends to the supply chain, partners and customers.

I believe that chief executives and risk managers should reconsider their current approach and reassess their investments in order to find a better balance between investments in technology and people, avoiding the common mistake of becoming over-reliant on technology.



**Xavier Marguinaud**  
**Underwriting**  
**Manager – Cyber**  
**Tokio Marine HCC**  
**T: +34 93 530 7439**

[xmarguinaud@tmhcc.com](mailto:xmarguinaud@tmhcc.com)



## Mind over risk:

The secret behind cyber resilient businesses  
and the people who insure them.



Companies are increasingly vulnerable to a widening range of cyber threats, including data breach, network interruptions, cyber extortion, as well as third party claims and regulatory penalties. Our experienced experts have in-depth knowledge about cyber risk insurance. This allows us to create tailored coverage that guarantees business continuity and bridges potential gaps between policies effectively. Wherever you are based, our dedicated team of internationally focused underwriters and claims specialists are ready to provide an intelligent approach as well as a fast and efficient service worldwide.

Tokio Marine HCC is a trading name of HCC Global Financial Products, S.L. (HCC Global), which is a member of the Tokio Marine HCC Group of Companies.

HCC Global-Sole Shareholder Company, ES B-61956629, registered with the Mercantile Registry of Barcelona, volume 31,639, sheet 159, page B-196767 is an exclusive insurance agency registered with the Spanish General Directorate of Insurance and Pension Funds (Dirección General de Seguros y Fondos de Pensiones) in their Special Register for Insurance Intermediaries, Reinsurance Brokers and their Senior Posts under the code E0191B61956629. It provides insurance mediation services on behalf of HCC International Insurance Company plc registered with Companies House of England and Wales No. 01575839 and with registered office at 1 Aldgate, London EC3N 1 RE, UK, operating through its Spanish branch domiciled at Torre Diagonal Mar, Josep Pla 2, planta 10, Barcelona, Spain.

Torre Diagonal Mar, Josep Pla 2, 10th Floor, 08019 Barcelona, Spain  
Tel: +34 93 530 7300 tmhcc.com