Sponsored by

Paragon

CIR
CONTINUITY INSURANCE & RISK
thinking resilience

A persistent threat *Traditional information security methods are no longer enough to protect against cyber risk. The extent of the threat has become so great that a multi-pronged approach to defence is vital in seeking to manage the risks. Deborah Ritchie reports*

The evolution of cyber risk and insurance *Paragon's William Wright follows the journey of cyber insurance as a risk transfer tool, from a fledgling line of cover some 15 years ago, to a multi-faceted solution of vital importance in today's complex risk landscape*

Cyber risk and insurance

Paragon

Sponsored by

A persistent threat

Traditional information security methods are no longer enough to protect against cyber risk. The extent of the threat has become so great that a multi-pronged approach to defence is vital in seeking to manage the risks. Deborah Ritchie reports

The widely reported ransomware attack that unfolded this month showed how a relatively simple cyber attack can impact an organisation's ability to function. Attacks like WannaCry have been growing in frequency in recent years, but have not been seen on such a large scale before. According to Kaspersky Lab, the key factor in the spread of WannaCry was the use of the EternalBlue exploit – that is that organisations and individuals hadn't updated their systems. Malware can also spread in other ways too – most notably by tricking people into installing code. Principal security researcher at the firm's global research and analysis team, David Emm, points out that patching systems is vital. "It's also essential to ensure that systems are protected using Internet security software," he says. "On top of this, education of staff is also vital. [And] good network management will help to reduce the scope of any attack."

Dr Alexeis Garcia-Perez, an expert on cyber security risk management from Coventry University's Centre for Business in Society, agrees that a large part of the problem when it comes to cyber security is people and skills.

"We're seeing a massive chink in the UK's preparedness for a cyber attack, but everyone is talking about IT infrastructure. That can be upgraded overnight with investment. People and skills are the problem," he explains. "There is simply too little awareness of cyber security risk at management and senior level in the UK. Cyber literacy in the NHS, in the wider public sector and in UK plc is going to be as important over the next decade as being able to read and write."

Experts widely concur, however, that while training employees is necessary, it is no longer sufficient protection on its own. Cyber security experts at law firm Mishcon de Reya say the cyber threat has become much more potent than many companies realise.

"Much of the blame for this week's specific problem has been laid on organisations using Windows XP, an operating system that is 16 years old and has not been supported by Microsoft for three years. Whilst people are strongly advised to move away from the platform, Windows XP is here to stay – it is embedded within many devices, from MRI machines in the health service to Point of Sale systems in large retailers which cannot be easily or cheaply upgraded," comments partner at the firm, Joe Hancock.

"The cyber threat has become more potent than most executive boards recognise. Companies do invest in security technology but discover all too soon that the technology is being persistently undermined by different attack methods."

There is a growing recognition that traditional information security methods are no longer enough to keep cyber criminals at bay. Security professionals at BDO say the severity, nature and extent of the threat has become so great that to be successfully managed, the risk must be addressed at board level, where a strategic cyber threat model can be agreed – one that is based on a defence doctrine that takes the traditional 'protect' model one step further.

The impact on the NHS of the recent ransomware attack underlines the degree to which the threat can damage certain critical services. Notes Shahryar Shaghaghi, head of international in the firm's cyber security division, "Ransomware presents a growing threat to every industry, but healthcare organisations are particularly vulnerable. Their digital transformation came late, and the simple reality is that many IT systems weren't installed with cyber security in mind. Because many hospitals rely on end-of-life technology and may prioritise immediate data access over data security, cyber criminals have found their systems relatively easy to penetrate."

Upskilling, patching and investment aside, this latest ransomware attack is likely to increase demand for cyber insurance protection – to create end-to-end risk mitigation. Insurers are playing an expanded role in countering the cyber threat using traditional expertise in risk management and claims services. They are also gaining more technical expertise in cyber threat testing and prevention and post-event resolution through acquisitions or alliances with cyber security vendors, according to analysts at Fitch. Cyber protection coverage, therefore, increasingly includes a service and advisory component, as well as insured loss limits.

The evolution of cyber risk and insurance

Paragon's William Wright follows the journey of cyber insurance as a risk transfer tool, from a fledgling line of cover some 15 years ago, to a multi-faceted solution of vital importance in today's complex risk landscape

This month the WannaCry worm ripped its way through 100 countries, attacking 200,000 individuals. The NHS was hacked. Fifty out of 248 NHS Trusts were impacted and, in some cases, operating theatres were closed for 48 hours. The government and the NHS Trusts themselves will likely incur millions of pounds of increased costs to recover their operations. In addition to significant financial loss, this latest high-profile ransomware attack had the potential to cause loss of life.

Cyber attacks and technology failures create a serious business risk. They have the potential to leave physical and non-physical systems redundant – impacting hardware, software, revenue generation and business continuity. This comes at a cost. Insurance may not often be the first thing on the agenda when discussing cyber risk but it represents a partial and important solution to risk transfer. Before it can be used to its greatest effect businesses must understand and actively manage their cyber risk exposures.

The backdrop

Privacy legislation and corporate obligations to notify affected individuals following a breach have existed in the US since 2002. On 1st July 2003 however, the Californian legislature enforced a law that changed the worlds' approach to data breach and consumer privacy governance, when it issued a state-wide privacy law mandating consumer notification following the loss of personally identifiably information (PII). Whilst there had been previous laws in the US that govern consumer privacy as early as 1996 through HIPAA (Health Insurance Portability and Accountability Act) and in 1999 through the Gramm Leach Bliley Act, the relevance of California's progressive approach in 2003 is hugely important when considering the challenges that US and European businesses face today in handling the confidentiality of their customer and corporate data and maintaining their operational integrity and functionality.

Perhaps California saw early signs that consumers would demand the privacy and integrity of their data assets, that international privacy enforcement agencies would become more ruthless and impose financial penalties for non-compliance, and that businesses would become more – and in some cases entirely – reliant on technology. Legislation was the natural place to start a governance process that would ultimately protect consumers but at the same time force businesses to accept and manage their new 'cyber' risks.

Fast forward 14 years, 48 US states now have mandatory breach notification laws, HIPPA enforced 13 fines totalling US$23.5m in 2016 alone, and the European Union has ratified the General Data Protection Regulation (GDPR) which, when called into effect on 25th May 2018, will impose a uniform privacy standard across Europe. This law will enable (maybe even encourage)

regulators to fine up to four per cent of global turnover for non-compliance. The hacks on Target and Home Depot in the US have now reportedly and collectively incurred nearly US$250m in consumer costs, system remediation, litigation fees and regulatory charges. TalkTalk has been hacked to the tune of 157,000 records, fined £400,000 by the ICO and suffered a profit drop of nearly £20m. In February 2017, HCA International was fined £200,000 by the ICO for a data breach – this being one of the most sophisticated and largest healthcare groups in the world. No corporate organisation is immune. To put the evolution of the cyber risk landscape in perspective, research group Opinium indicated that 2.9 million UK firms suffered cyber security breaches nationwide throughout 2016, at a cost of £29.1 billion.

The risks

Whilst the threat actors for cyber risk have probably remained consistent for the last 5 to 10 years (nation states, hacktivists, organised crime, script kiddies and insiders) the business impact potential has increased – largely due to the complexity, variety and interconnectivity of the threat vectors. PWC's 2016 'Global IT Security Survey' found that 48 per cent of businesses relied on IT services delivered via the cloud, whereas the computer infrastructures of a decade ago had limited interactivity with the cloud, networked devices and applications, and sat on relatively isolated operating systems. The increased usage of cloud SaaS and IaaS systems and increased connectivity and dependency on third party hosted platforms, add layers to risk complexity.

In their simplest form, cyber risks fall into the following categories:

- Regulatory
- Legal
- Financial loss – which may occur due to:

a. System and data restoration
b. Crisis management
c. Third Party Liability
d. Reputational damage
e. Extortion
f. Loss of income, extra expenses
g. Physical damage (straddling liability and physical restoration)

As highlighted in the outset of this article, the first two of these categories (regulatory and legal) are largely dictated by the legislative landscape. The US operates in a highly litigious environment which increases both the chances and cost of litigation; regardless, regulations are enforceable irrespective those costs. What the US has taught Europe, is that if a regulatory authority wants to set a 'standard' and a business environment which respects consumer privacy and data integrity – it needs to deploy a framework which holds businesses accountable to that standard. Cue GDPR.

GDPR will create a framework that puts a European microscope on data privacy and the integrity of businesses capturing and processing consumer data, which will come at a cost – either by making the necessary changes to ensure compliance, or by being fined for non-compliance. Whichever way you look at it, the EU is moving towards the standard set in California in 2003. We may be 15 years behind that pioneering state, but a number of the same challenges US businesses faced in 2003 will be faced in the

Threat Actors and Threat Vectors

Threat Actors	Objectives	Threat Vectors	Method of Attack
Nation States	To assert an economic, political or military advantage	• Web-facing networks • Corporate networks • Network enabled physical control units • Third party vendors • Networked devices • Applications	• Malware • Hacking • Extortion • Social Engineering • DDOS • Theft of data assets • Theft of financial assets • Advanced Persistent Threats (APTs) – usually a combination of the above
Hactivists	To enforce social/political change, or to cause financial harm		
Organised Crime	Financial gain		
Script Kiddies	Enjoyment, bragging rights, financial gain		
Insiders	• Malicious intent to harm employer or to gain financial benefit – could be rogue employee or ex-employee • Accidental error		

EU and Britain (post-Brexit) in 2018 and beyond.

To address this regulatory development and remain compliant, businesses will need to understand the potential threat vectors which impact their data security and integrity. Insurance represents a partial solution to risk transfer but first businesses must understand and manage their cyber risk exposures. The table above provides an overview of potential threats that need to be considered and managed from a data and IT security perspective.

Part of the solution: insurance

Whilst risk management departments will need to deploy human, technological and operational controls to manage their cyber risks effectively, they should also consider insurance as a risk transfer mechanism. A typical cyber insurance policy would cover the following losses resulting from a cyber event:

- Corporate legal expenses
- Regulatory investigation costs and settlements
- Breach response legal expenses (may involve privacy experts in addition to corporate legal expertise)
- Income loss
- Extra costs of working
- Consumer response services
  - Written or publically announced notification
  - Credit and ID theft monitoring (where legally required)
- Corporate response services
  - Public relations costs
  - Forensic investigation costs
  - Data reconstruction costs
  - Extortion response cost and demands

Insurance providers will work with a business' existing incident response vendors or introduce them to specialists (at discounted rates, more often than not) who can form part of a dedicated incident response unit in the event of a network event.

The insurance industry has responded well to the business exposures created by cyber risk. Cyber insurance can provide a direct and measurable crisis management contribution to a company in a time of crisis, as well as financial reimbursement.

The UK and Europe may not have the same privacy landscape as the US but it cannot be ignored that currently every business – wherever they are located – has an exposure to system integrity and a need to stay online and operational.

In 2018, the UK will be enforcing the GDPR standard, regardless of Brexit. Once GDPR has come into force, the focus on data privacy and consumer protection will make progress towards the US data privacy framework. The cyber risk landscape is already complex and perilous, and the WannaCry outbreak is a clear and stark reminder that any company – no matter how sophisticated – can be dangerously exposed to an array of cyber threats. Insurance provides risk transfer for the moment that a cyber incident like WannaCry becomes a reality.

William Wright is Partner and Joint Head of Privacy, Cyber and Technology at Paragon International Insurance Brokers Ltd

Paragon

Specialist Broking.
Claims Advocacy.
Risk Management Consulting.

PARAGON IS AN INDEPENDENT, GLOBAL INSURANCE BROKER BASED IN LONDON AND BERMUDA.

With market leading capabilities and experience in the financial and professional lines sectors, Paragon will partner with you to deliver risk transfer solutions, claims advocacy and risk management services with a bespoke, personalised approach that is unique in the industry.

Serving UK and International firms in the following specialist areas:

- **Privacy, Cyber and Technology Liability**
- **Professional Indemnity**
- **Employment Practices Liability**
- **Management Liability**
- **Mergers and Acquisitions / Transaction Liability Insurance**

For further information about Paragon and how we can assist your firm, please contact:

WILLIAM WRIGHT
Partner
E wwright@paragonbrokers.com
T +44 (0) 20 7280 8252
M +44 (0) 7900 968894

JASPER GORING
Vice President
E jgoring@paragonbrokers.com
T +44 (0) 20 7280 8282
M +44 (0) 7773 037261

Paragon International
Insurance Brokers Ltd

140 Leadenhall Street
London EC3V 4QT England

T +44 (0) 20 7280 8200
F +44 (0) 20 7280 8270

www.paragonbrokers.com

Authorised and regulated by the Financial Conduct Authority. Accredited Lloyd's Broker
Paragon Brokers (Bermuda) Ltd 27 Reid Street, Hamilton HM11, Bermuda. Registration No. 33838