
# Insuring the uninsurable:
## Is cyber insurance really worth its salt?

**Authors**
Michael Payne, MSc (Royal Holloway, 2016)
Peter Komisarczuk, ISG, Royal Holloway

**Abstract**

Cyber insurance is one of the fastest growing areas of risk cover in the insurance industry as businesses increasingly turn to specialist insurance in an attempt to cover a portion of their enterprise risk. Cyber risk is notoriously difficult to quantify and businesses face an arduous choice in deciding which risks to manage themselves and which risks to transfer to the insurance market. This article dips a toe into this emerging risk area and outlines some steps which businesses can take in order to make better informed risk mitigation decisions.[a]

[a]This article is published online by Computer Weekly as part of the 2017 Royal Holloway information security thesis series `http://www.computerweekly.com/ehandbook/Insuring-the-uninsurable-Is-cyber-insurance-worth-its-salt`. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at `https://www.royalholloway.ac.uk/isg/`.

## Introduction

Taking out an insurance policy is sometimes likened to having a parachute: if you don't have it the first time, the chances are you won't need it again. But in practice, insurance is not a zero-sum game and not all insurance cover is created equally. Insurance as we know it today evolved from early guilds to its modern-day form by allowing individuals and companies to take risks and trade with each other. As such, it has been called rather loftily the 'DNA of capitalism'.

The saying goes that 'hacks love a hack' and media coverage of cyber breaches is now almost a daily occurrence. So it is no surprise that with the insurance industry facing slow or stagnant growth across most segments, the fastest growing area of risk cover is cyber insurance. In what may seem like a beacon of hope in a sea of regulatory and compliance costs, low interest rates and low returns, and a glut of capital pushing down rates, this emerging and evolving risk coverage offers high returns, yet is not without its risks.

The London insurance market, of which the Lloyd's market plays a significant part, saw a 50% growth in cyber premiums in 2016. Lloyd's, which represents approximately 25% of the global cyber insurance market, introduced 15 new cyber products in the past year alone to meet rising demand. Global written cyber premiums are currently estimated by Allianz to be approximately USD 2.5 billion. Premiums are forecast to accelerate to USD 20 billion by 2025.

The insurance gold rush has led to a market of a few well-established and respected players over the past decade who have built up cyber underwriting expertise backed by valuable claims history. It has also seen partnerships forged by insurers with security vendors, legal, PR and communications firms in order to provide insured clients turn-key solutions to deal with the aftermath of a cyber breach. Even re-insurers and insurers have joined forces in some cases. For example, Munich Re and Beazley recently partnered to combine their respective strengths in data breach response and industrial and operational risk cover.

Yet the inherent complexity of defining and underwriting cyber risk has resulted in little standardisation of cyber insurance policies among insurers. Policies have been likened to 'Swiss cheese' in their exclusions of cover so it may seem like a Herculean task to any firm looking to transfer some of its enterprise risk into a cyber insurance policy.

## A brief history of cyber insurance

Some form of cyber insurance has been around since at least the early 1990s. The first cyber policies (or 'hacker policies' as they were known) were designed to cover third party liability for the effects of malware. It was only once the State of California enacted the first of the US state data breach laws in 2003 that cyber cover evolved to provide cover for the unauthorised disclosure of personal information. But insurance demand really took off once the Office for Civil Rights (OCR) was given the power to fine companies under the Health Insurance Portability and Accountability Act (HIPAA) for the unauthorised disclosure of Protected Health Information (PHI). Today this form of cyber cover dominates the US market and the US market represents 90% of global written cyber premiums. In Europe, most cyber cover has to date focused on providing cover for business continuity risk although this is changing as experience learnt in the US market is starting to make an appearance in Europe. The timing is not coincidental. New European data protection regulation and reporting requirements (the General Data Protection Regulation, GDPR, and the Network and Information Security, NIS, Directive) will very likely boost demand for cyber insurance among corporates but it remains to be seen whether regulatory fines are insurable in some jurisdictions.

**Characteristics of cyber risk**

*Cyber risk can be interpreted in many ways.* It may be articulated and calculated very differently by security practitioners, risk managers, business heads, or underwriters. Bridging the gaps within the business to identify and quantify risks and subsequently transferring risk to an insurer is a difficult task.

*Cyber risk is dynamic and evolving.* Defenders and attackers are engaged in a perpetual arms race involving technical and human factors to keep up with new and evolving threats. These may even see old threats used in new and innovative ways.

*Cyber risk is a systemic risk.* A combination of computer monocultures, the interconnectedness of systems and devices, the growing reliance on cloud services and the technological convergence of business enterprise and manufacturing industrial control system environments, could create the conditions for a perfect storm. Here one cyber event could have unforeseen knock-on effects which traverse application, host, and business boundaries and geographies leading to a potential 'cyber catastrophe'. A recent example of this was demonstrated by the 2016 Mirai DDoS botnet attack which corralled vulnerable IoT devices against a DNS provider preventing public access to sites such as Twitter and Spotify for several hours.

## Why buy cyber insurance?

Many cyber insurance buyers fall into 2 camps:

1. Companies which have suffered a breach; and
2. Companies which are simply ahead of the curve in managing their enterprise risk.

Another category of firms, which we will call the 'phantom insured', believe they are covered for cyber through existing, traditional lines of insurance such as Commercial General Liability (CGL) or Property and Casualty (P&C). These firms may even have dedicated cyber insurance cover but policy exclusions or policy triggers may in practice exclude cover. In the UK, it is estimated that only 2% of large organisations and a negligible number of SMEs have so far purchased standalone cyber cover. Yet according to a 2015 HM Government/Marsh report amazingly over half of CEOs believe they have some form of cyber cover when the real number is closer to 10%.

A final category of the insured are those firms with 'silent cover' which may have all-risk insurance policies not specifically excluding cyber, or policies with explicit cyber exclusions yet permitting certain

named perils which could be caused by a cyber-attack (consequently triggering the policy). With 'silent cover' insurance firms could find themselves on the hook for losses which have not been priced into the policy. The UK regulator, the Prudential Regulation Authority, has taken a strong interest in this area where the solvency of insurers in extreme cases may be at stake. Lloyd's has also asked its members to conduct a thorough review of policies to reduce this area of long tail risk.

## The steps to take before taking out a policy

Security is all too often an afterthought or seen as a business blocker, yet a security-aware corporate culture should strike the right balance between control and effectiveness of corporate strategy. ICT systems, applications, and the data stored and processed by organisations are its lifeblood. A firm's external relationships with stakeholders including customers and suppliers (in many ways an extension of the organisation) are also critical. A 2016 Ponemon survey found the biggest financial impact of a breach was due to lost business. Reputation matters.

The decision to choose cyber insurance should really only be made once a firm has a handle on its enterprise risk. An understanding of risk appetite and risk tolerance, and conducting a risk assessment would seem like the logical place to start. Yet according to an Aon survey less than two thirds of firms do this and half of firms surveyed were unsure if they complied with best practice or standards. Of those companies purchasing a policy one of the principal reasons for seeking cover was to provide 'due diligence comfort for the board'. A comfort blanket won't be much help in the event of a hack and such a tick-box approach to obtaining cover is best avoided.

An organisation needs to understand which risks it accepts and treats through risk mitigation activities typically involving people, process, and technical controls. This could include adoption of cyber security frameworks such as ISO27001, NIST 800-53, or even the Cyber Essentials scheme which insurers may also view favourably when pricing cover. The organisation should then be in a better position to know which risks to transfer to an insurer. Risks which are high impact with low likelihood or new and emerging risks which are hard to quantify are the logical choice to insure.

The insurance market has seen demand for cover shift from data breach cover to include business interruption cover. This may signal either a maturing market as companies' requirements broaden or it could be as a result of new threats such as the rapid growth of ransomware which directly cause business interruption. Indeed, Allianz forecasts business interruption cover to emerge as a major risk area within the next 10 years.

## Types of cover

Cyber policies fall broadly into two areas: first party cover which covers a business' own assets and third party cover which protects the insured from the fallout affecting the assets of others as a result of a breach.

In 2016 the majority of cyber products designated with the Lloyds risk code of CY cover data privacy (82 out of 87). Areas of risk which are less likely to be covered are physical risks such as death and bodily injury or reputational loss, although this is changing. The insurance market is faced with increased competition so previously uninsurable areas may start to become insurable albeit with exclusions, high retentions, and high premiums. Insurers differentiate their product offerings in other ways by offering a suite of breach response services from incident response to legal and PR advice. Anecdotal evidence points to rising rates due to the high cost of providing such services.

**First party cover examples**

- Physical damage: people and physical assets.
- Damage to digital assets (software and data).
- Business interruption.
- Cyber extortion, ransomware.
- Customer care and notification expenses.
- Reputational loss.
- Theft: Intellectual property, commercially sensitive data, financial.
- Cyber-attack from a breach of a third-party system.
- Regulation defence and fines.
- Bodily injury and death.

**Third party cover examples**

- Privacy, confidentiality, and security liability.
- Multi-media liability.
- Cyber-attack on a third-party from breach of insured systems.
- Content injury.
- Loss of third-party data.
- Outsourcing: damages and defence costs.

Exclusions such as war and terrorism are common across all lines of insurance and cyber is no exception. Cyber-specific exclusions have been added to traditional lines of cover as cyber cover has grown. Cyber insurance as a standalone cover is sometimes referred to as gap insurance but in practice there still may be areas of cyber risk which are not covered. Firms looking for a comprehensive risk transfer solution may decide to add explicit cyber risks to existing insurance policies through the use of 'write-backs' in addition to taking out a standalone cyber insurance policy. An unforeseen consequence of exclusions is one where it may potentially invalidate a third party contract. A specific example is the cyber attack exclusion clause CL380 typically present in marine and energy policies. The presence of this exclusion could technically invalidate a firm's banking covenants which usually stipulate that borrowers take out insurance cover as a precondition to taking out a loan.

Attribution for cyber events is also critical and should be factored into any assessment of cover taken: one reason is that attribution affects policy triggers, so an attack, which is determined to be an act of terrorism, may not trigger a claim. The key to this process is having a thorough understanding of policy wordings in existing and new policies. It is not surprising that an Aon report found that clear policy wording was a top concern to organisations seeking insurance. Retaining the services of an experienced legal counsel and broker would typically be useful.

Cyber insurance cover for Small and Medium sized Enterprises (SMEs) has so far had little uptake despite the UK government launch of the Cyber Essentials scheme in 2014. CFC Underwriting recently partnered with the British Insurance Brokers Association to provide tailored cyber cover for SMEs. "*Cyber risk is the number one biggest exposure that any of our customers have right now . . . [and it] is horribly misunderstood and miss-sold by the insurance industry*", said CFC's Graeme Newman. SMEs are less likely to have sophisticated security, backups, contingency plans, or financing in place to deal with attacks impacting business continuity (such as the growing ransomware threat). Insurance which covers these risks would make a lot of sense to many SMEs.

## Conclusion

Although there are many types of cyber products available to organisations these are still heavily skewed towards data breach response. Traditional lines may offer limited, if any, cover for cyber-caused perils. Standalone cover, often referred to as gap cover, may not actually cover all cyber risks relevant for an organisation or it may not be clear from the policy language what is covered. The price of the premiums may also be unattractive. One area of change identified for policies is for actuarial models to reflect the self-protection activities firms take such as their investment in security controls. In other words self-protection should be reflected in the value of premiums.

It is uncertain at this point how the insurance market will evolve to meet the risk transfer needs of business but the consensus view among this report's interviewees was that the industry would eventually adopt cyber risk cover into traditional lines of cover. Rarely covered areas such as contingent business interruption or cover for cyber physical events will likely become more mainstream albeit with limits. Third-party risk is another area which may spur cover for cyber insurance particularly if companies require their suppliers to take out insurance cover as a condition for doing business together. New legislation and the threat of fines will also very likely contribute to the uptake of cover.

The key to successful risk management is knowing which risks to manage and treat and which risks to outsource. Cyber insurance should be viewed as just one of many tools in any risk management strategy. In its current state of maturity, perhaps cyber insurance could be considered as a reserve parachute: you don't necessarily want to use it but it's reassuring to know you have one.

**Biographies**

*Michael Payne* is a Manager in the EMEIA Advisory Centre for Cyber Security at EY. Michael joined EY in 2015 after 15 years working in corporate governance, merger and acquisitions advisory, and financial services in Europe and Asia Pacific. Michael decided to change career in 2013 after reading a book, Ghost in the Wires, by high profile US hacker, Kevin Mitnick. Michael graduated from Royal Holloway, University of London, in 2016 with a Master's degree in Information Security.

*Peter Komisarczuk* is a member of the Information Security Group at Royal Holloway, University of London, where he is Programme Director for the MSc Information Security (Distance Learning). He is a chartered engineer and has a PhD (Surrey), researches in networks and security and has worked in industry in various R&D roles at Ericsson, Fujitsu and Nortel Networks.