HM Government

MARSH

MARCH 2015

UK CYBER SECURITY

THE ROLE OF INSURANCE IN MANAGING AND MITIGATING THE RISK

CONTENTS

ACKNOWLEDGMENTS

We would like to thank the following organisations for their involvement in the steering group, and for providing expert input into this publication:

- Association of British Insurers (ABI)
- ACE
- AEGIS
- AIG
- AIRMIC (UK association for risk and insurance management professionals)
- Allianz
- Aspen
- Barbican
- Beazley
- Brit insurance
- CFC underwriting
- Guy Carpenter
- Hiscox
- Lloyd's
- Tokio Marine Kiln
- XL
- Zurich

We would also like to acknowledge contribution from the following organisations:

- TheCityUK
- The Department for Business, Innovation & Skills (BIS)
- UK Trade & Investment (UKTI)

FOREWORD

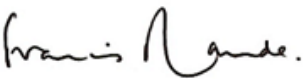
The cyber threat remains one of the most significant – and growing – risks facing UK business. 81% of large businesses and 60% of small businesses suffered a cyber security breach in the last year, and the average cost of breaches to business has nearly doubled since 2013[1]. Working in partnership, the Government and industry have done much to improve understanding of cyber attacks and how to reduce their impact, yet more needs to be done. As part of this Government's long-term economic plan, we want to make the UK one of the safest places in the world to do business online.

This report, the result of close working between the Government and the insurance sector, highlights the role insurers and insurance can play in reducing cyber risk. By asking the right questions in addressing cyber risks, insurers and insurance brokers can help promote the adoption of good practice, including the Government's Cyber Essentials scheme, which will reduce the frequency and cost of breaches.

The report includes some important messages for business. One is the need to value the risk of cyber attack properly. It also shows that many businesses are overestimating the extent to which their existing insurance provides cover for cyber risk. The report demonstrates how the insurance sector can help improve industry's understanding of cyber insurance.

Another clear conclusion is that some businesses still feel they do not fully understand cyber risk. This highlights the need for companies to have clear accountability structures for cyber risk and to put in place robust cyber security risk management arrangements. We have provided a range of advice and guidance to business, which it can draw on, and a set of basic criteria for all organisations through the Cyber Essentials Scheme.

Cyber security is not just a question of threats – it also represents an opportunity for the UK. The UK has world-leading cyber security expertise and cyber security services. The UK insurance sector is already a world-leader. With innovative ideas, like including Cyber Essentials certification as part of insurance cyber risk assessments for small to medium-sized enterprises (SMEs)[2], the sector is demonstrating that the UK is the natural home for a growing global cyber insurance market.



Rt Hon Francis Maude MP
Minister for the Cabinet Office
and Paymaster General

[1] *2014 Information Security Breaches Survey,* UK Department for Business Innovation & Skills, London, 2014.
[2] *Defined for the purposes of this publication as those businesses employing fewer than 250 staff.*

1 INTRODUCTION

Cyber attacks against UK companies present a daily threat to normal UK business operations and are increasing in severity. This report focuses on how insurance can help make UK companies more resilient to the cyber threat, and is the result of four months of co-operation between representatives of the UK Government and the insurance industry, led by the Cabinet Office and Marsh. Its formulation involved interviews with senior management in some of the UK's largest firms, expert input from 13 London market insurers, and the analysis of data emerging from surveys, insurance policies, and other sources. It has messages for businesses, insurers, and policy-makers.

While insurance may seem a narrow and non-technical way to approach such a complex and far-reaching threat, it adds a valuable perspective to cyber risk for three reasons:

1. Insurance places a cost on firms' cyber risk through the premium they pay, and the prospect of a reduced premium then encourages firms to take steps to mitigate the risk. For an emerging risk such as cyber, this should be an important spur to action ahead of losses becoming a problem.

2. Insurance goes arm-in-arm with loss prevention. Insurers will help firms reduce their losses by providing insight from claims and near misses across their client base. That information asset is of particular value for cyber risk, because cyber is a new risk and incidents often go unreported.

3. Insurers bring their knowledge and experience of more established risks that can be applied to cyber. There is a tendency to think of cyber as a new and hence unique threat. In fact many aspects of it – the risk of business interruption, the potential for large and public impact, and the need for rapid response post-event – are common to other tail risks (low frequency, high impact events), such as natural catastrophe and terrorism.

At present, within the insurance sector, the cyber threat is not well defined, with confusion surrounding definitions based on different causes and consequences. Insurers tend to conflate cyber with data breach given the well-developed demand for that cover driven by US regulation; however, UK firms have broader concerns about possible damage from cyber risk, including business interruption, damage to property, and theft of intellectual property. This report therefore focuses on the cause of cyber risk regardless of the consequence, and specifically on cyber attacks – that is, deliberate attempts to cause harm via digital channels. We focus on attacks because while more than 60% of incidents reported to insurers are the result of accident, the majority of the high-severity losses stem from actions designed to cause harm.

2 SUMMARY

Cyber attacks have entered mainstream consciousness on the back of a wave of well-reported incidents affecting individuals, firms, and governments, and today most large businesses[3] have cyber on their risk registers and have assigned accountability and actions to improve their cyber security.

Nevertheless, there is still a significant degree of discomfort at board level given the newness of the risk and its potential for costly and public disruption. Similarly, the cyber insurance market is still in its infancy, with around half the business leaders we talked to not aware that insurance covers cyber risk, and just 2% of large firms having explicit cyber cover, a figure that drops to close to zero for smaller firms[4].

This report addresses three themes:

1. Helping firms get to grips with cyber risk.

2. Helping the insurance industry to establish cyber insurance as part of firms' cyber tool-kits.

3. Helping London to be a global centre for cyber risk management.

There is a growing concern with the physical damage impacts of cyber attacks (whether indirectly or directly), given the increasing connectedness of assets to the internet.

[3] *Defined for the purposes of this publication as those businesses employing more than 250 staff.*
[4] *Estimate based on policies placed/written by insurers who participated with this project.*

1. HELPING FIRMS GET TO GRIPS WITH CYBER RISK

- Many firms place cyber among their leading risks in terms of the likelihood and severity of impact[5]. Consequences that cause the greatest concern include data loss, business interruption, and theft of intellectual property, with the impact being dependent upon the industry, risk profile, and size of a particular firm. There is a growing concern with the physical damage impacts of cyber attacks (whether indirectly or directly), given the increasing connectedness of assets to the internet. Cyber is rightly considered by firms to be a dynamic risk which pits them in an "arms race" against those seeking to cause harm. This is likely to keep cyber risk as a standing item on their agenda.

- Large firms have done a lot to make themselves cyber secure, yet significant risks remain including through their exposure from third parties, whether service providers, product suppliers, customers or in the case of banks, their borrowers. Businesses need therefore to improve supply-chain resilience to cyber attack, particularly in cases where they have smaller business partners, who are typically less well protected. Recent Government research[6] found that 22% of small businesses admit they "don't know where to start" with cyber security, demonstrating the importance of the Government's recently-launched Cyber Essentials, which guides businesses in protecting themselves against cyber threats by setting out the basic technical controls that all organisations should have in place. As an encouragement to adopt the scheme, insurers will now look to include Cyber Essentials certification as part of their small and medium-sized enterprise (SME) cyber risk assessment. As a further step, Marsh has arranged for a type of cyber insurance cover for SMEs that pays for the cost of Cyber Essentials certification to reflect the risk reduction that accreditation represents. This should help lead to large firms and banks expecting Cyber Essentials from the SMEs they deal with.

- Cyber attacks can be rapid, highly damaging, and public, potentially leading to a vicious cycle of declining investor and customer confidence and therefore cash availability. Banks, utilities, and other critical infrastructure firms are used to this kind of tail risk and are often regulated and run with it in mind. Most firms are not, however, and their risk management practices are geared around lower-level, slower moving risks, which can be managed within the business and with their impact smoothed by insurance. Firms starting from this position will need a substantial upgrade in risk management to cope, including having an independent board-sponsored risk function, introducing disciplines such as stress-testing, and creating a joined-up recovery plan that brings together financial, operational, and reputational responses. This final point invokes the need to move away from treating cyber primarily as a technology or security issue, to one that is owned collectively as a key risk to firm viability and that permeates the way the business is run.

- A specific aspect of risk governance is the quantification of the risk, particularly in light of listed firms' need to report a viability statement under the revised UK Corporate Governance Code. A paucity of data makes attempts to model cyber exposure difficult. Not only do traditional impact tests such as "value at risk" suffer through a lack of data, they also focus on solvency (size of loss) rather than liquidity, which is the more likely cause of failure from a cyber event. As an alternative, firms can start with the more manageable question of what size of financial shock they are able to withstand in terms of cash-flow, given how funding sources such as bank lines of credit and insurance will behave under stress, and then consider what scenarios – cyber or otherwise – would be required to exceed this amount. This cash measure of "event-absorbing capacity" and the decision on how far risk appetite can approach it can then be the bedrock for board-level assessment of risk and reporting requirements, such as viability statements. The elements of this approach are outlined in the report.

---

[5] *Global Risks 2015 (10th Ed.)*, World Economic Forum, Geneva, 2015.

[6] *Cyber security "myths" putting a third of SME revenue at risk available at https://www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk, accessed 4 March 2014.*

2. HELPING THE INSURANCE INDUSTRY TO ESTABLISH CYBER INSURANCE AS PART OF FIRMS' CYBER TOOL-KITS

- Insurance is not currently seen as relevant to cyber resilience. Indicatively, half of firm leaders we spoke to do not realise that cyber risks can even be insured. In fact, insurance solutions for cyber do exist and can cover a broad range of cyber consequences. As a first step to increasing business awareness, Lloyd's, the Association of British Insurers (ABI), and the Government have agreed to develop a guide on cyber insurance and to host it on their websites.

- Business leaders who are aware of insurance solutions for cyber tend to overestimate the extent to which they are covered. Surveys show that 52% of CEOs believe that they have cover[7], whereas in fact less than 10% do[8]. This picture is likely a result of the complexity of insurance policies with respect to cyber, with cyber sometimes included, sometimes excluded, and sometimes covered as part of an add-on policy. Insurers can help businesses by treating cyber risk more consistently. While this will likely happen over time as the risk matures, a more immediate solution is for brokers to provide a formal statement of cyber assurance, giving the board comfort on the completeness of their cyber cover versus their risk appetite.

52% of CEOs believe that they have cover, whereas in fact less than 10% do.

- The cost of cyber insurance relative to the limit purchased is typically three times the cost of cover for more established general liability risks, reflecting the possible exposure that insurers are taking on with cyber. Cyber insurance also has a much lower degree of price differentiation across individual firms, which suggests that pricing also reflects the lack of data needed to underwrite accurately. This is concerning because it undermines the value of insurance in encouraging risk reduction by firms, since they will not see a corresponding reduction in their insurance costs. One solution is for data pooling to help underwriters understand individual and aggregate exposure better, leading to cheaper pricing for the more resilient firms and a rise in the amount of available capacity for cyber cover. At the same time, government agencies have different sources of information. Much of this has been made available via data feeds, such as the Cyber Security Information Sharing Partnership (CiSP). The Government and insurers will continue to collaborate to make this, and other information and data sources, more accessible and usable for insurers. To aid this, the Government will work with the insurance industry, including the Association of British Insurers (ABI) and Lloyd's, to establish a forum for data and insight exchange. The forum will be designed to capture emerging threats and trends while protecting individual insurer and insured data confidentiality. It will also allow continued collaboration on wider Government and industry cyber security policy and initiatives.

- Businesses and insurers should be concerned by risk aggregation, given the possibility of single attacks leading to losses across a large number of firms, which can create counter-party risk for the insured and potential failure for the insurer. At the moment, such an event has not materialised, but that does not mean that the risk is not present (at the time of writing, details of an attempted fraud across 100 banks are being reported). The total realistic possible maximum loss for cyber globally is currently around £20 billion. By comparison, that amount is within the reinsurance capacity for single-event risk (£65 billion), but well above that for nuclear (£3 billion). With cyber set to grow, it suggests an urgent need to address the size of aggregate risk being built up, and how to handle it. While some market participants have suggested that a possible Government backstop may be necessary, there is no conclusive evidence of the need for such a solution at present. One of the roles for the data pooling forum described above will be to improve insights on aggregation risk and cyber disaster scenarios. The insurance sector will continue industry discussion on market capacity and the cyber risk pool.

[7] *2014 Information Security Breaches Survey.*
[8] *Marsh and Zurich cyber risk surveys.*

3. HELPING LONDON TO BE A GLOBAL CENTRE FOR CYBER RISK MANAGEMENT

- London is already a major centre for cyber insurance, with £160 million of cyber-specific premiums coming to London, largely in the form of US data protection coverage. London has a history of leading on large and complex risks that are challenging to underwrite locally. Cyber risk fits this description and should be a priority for London market participants as a common agenda. Outside of the US, cyber insurance has not been a significant focus as an export opportunity, but data protection regulation in Europe and elsewhere is likely to change this. Lloyd's and UK Trade & Investment (UKT&I) have agreed to co-operate to promote the cyber capabilities of the London insurance market to key countries around the world.

- Dealing with the cyber threat invokes a wider set of financial, advisory, and technical services that London is well positioned to provide. The market will naturally evolve to find combinations of these that work well for businesses and can be exported. At the same time, the speed of development and scale of opportunity make it worth looking at whether there are ways to accelerate that process of establishing connections. We recommend that a multi-disciplinary task force looks at ways that bring together London's assets to deliver a more joined-up cyber offer. TheCityUK has agreed to take this on, defining the terms of reference and composition of the task force, with input from the Cabinet Office.

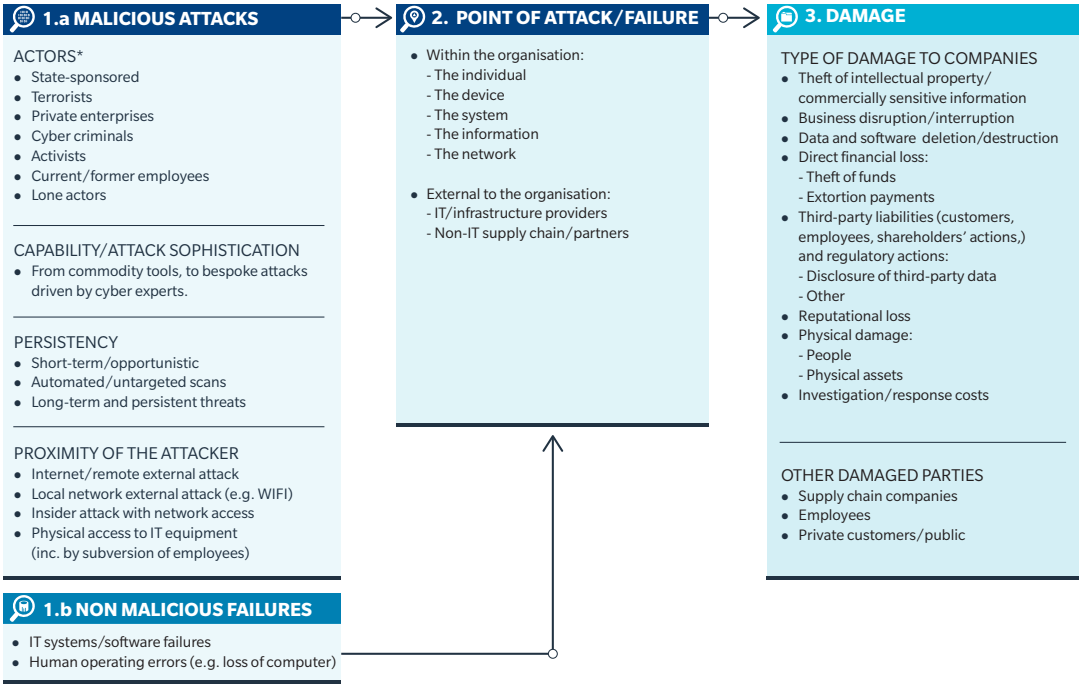
London has a history of leading on large and complex risks that are challenging to underwrite locally. Cyber risk fits this description and should be a priority for London market participants as a common agenda.

3 DEFINING CYBER RISK

In its broadest form, cyber risk is synonymous with IT risk – that is, "the business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise" (ISACA IT Risk Framework). Such a broad definition makes sense because similar outcomes may arise from an IT event, irrespective of whether its cause was malicious or not and whether it arrived via the internet or from internal systems.

In Figure 1 we provide a taxonomy of cyber risk that looks at the characteristics of the attack/failure, the points of attack/failure, and the types of damage that may arise. This structure is a basis for identifying different forms of threat and, consequently, the scenarios that need considering as part of cyber risk evaluation and stress-testing.

FIGURE 1: TAXONOMY OF CYBER RISK FOR CORPORATIONS



** Actors often correlated with MOTIVATION (1 Warfare/terrorism, 2 Propaganda , 3 Commercial gain/advantage, 4 Direct financial gain, 5 Protest, 6 Fun/demonstrate ability, 7 Revenge).*

The nature of the agent attacking the organisation will inform both their objective and the sophistication of their capabilities. This, in turn, will reflect the persistency of the attack (that is, the type of hacking tools deployed) and the determination over time of the attacker to compromise the organisation. A further characteristic of the attacker is their proximity, which recognises that the ability to defend against an attack and the scale of its eventual impact will depend upon whether the threat is external to the organisation's network or has come from within.

The point of attack outlines the vulnerability exploited by a malicious attacker or the point of failure for non-malicious events. In addition to exploiting vulnerabilities identified within the IT assets of an organisation, an individual may be the asset under attack through the use of various social engineering techniques (such as phishing) to gain system-access credentials. There is also a dependency on external networks such as cloud vendors and the public internet infrastructure, where an attack may result in the same loss outcomes as if the event occurred within an organisation's own self-operated network. This demonstrates the need for appropriate due diligence and assurance processes to apply to the IT supply chain, as was highlighted by Trustwave's 2014 Global Security Report, which found that 46% of breached organisations had outsourced IT functions.

Damage to an organisation resulting from a cyber attack can be categorised into 11 forms, indicating the extent to which cyber risk deserves to be afforded much greater consideration than the current focus on data breach. This categorisation also recognises that where a cyber attack is directed at an organisation that companies depend on as part of a supply chain, have system links with, or use to store data on corporate or personal customers, the impact of the attack may be felt well beyond the attacked organisation. As such, companies should consider the impact a cyber event at a supplier or other affiliate could have on their own business.

Damage to an organisation resulting from a cyber attack can be categorised into 11 forms, indicating the extent to which cyber risk deserves to be afforded much greater consideration than the current focus on data breach.

The focus of this report is malicious attacks, regardless of the point of failure they target or the damage they cause. This is because of the much higher severity of malicious attacks relative to non-malicious events, even though non-malicious events are the more frequent (data provided by Beazley shows that, in 2014, more than 60% of the reported cyber security breaches were due to non-malicious events). This picture is likely to get starker as technology and internal processes get better at eliminating accidental failures, while malicious attacks grow in ambition and impact.

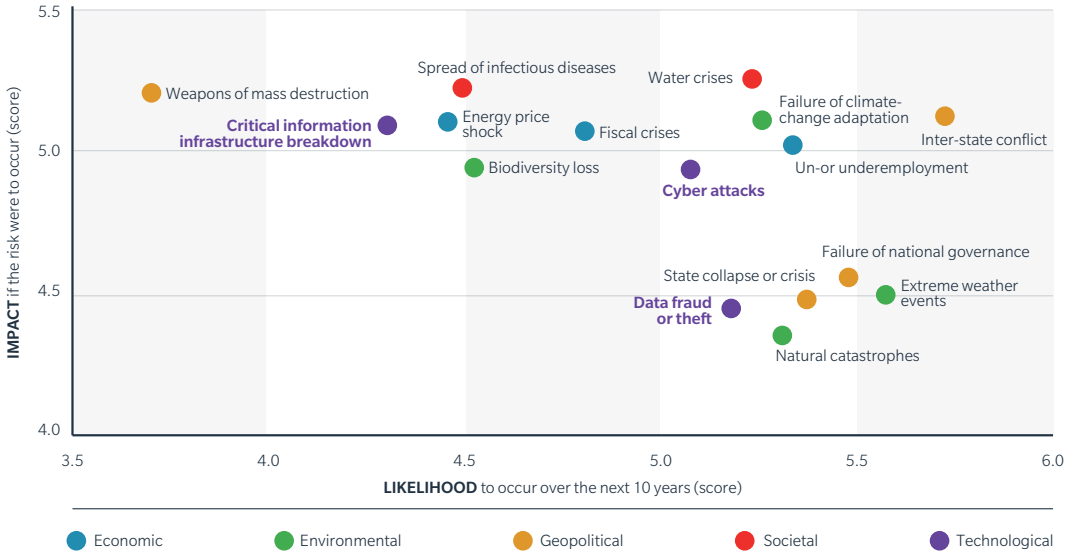
Cyber attacks represent a present and growing danger that threatens businesses, irrespective of size and sector. The UK Government's annual breach report shows that 81% of large businesses and 60% of small businesses suffered a security breach in 2014[9].

In addition, the UK Government has recognised cyber attacks to be one of the most significant risks facing the UK. The costs to businesses are rising as hackers become more focused and persistent in their attacks. Several attempts have been made to quantify the economic cost of cyber crime on UK businesses; while there are a wide range of estimates, figures consistently range in the billions of pounds. Such amounts tend to grab the headlines and provoke a debate over what is real versus scare-mongering, obscuring the fact that we can anticipate more frequent, larger, and even systemic attacks as an increasing number of devices go online.

[9] *2014 Information Security Breaches Survey.*

In the World Economic Forum's Global Risks 2015 report, cyber risk is firmly positioned as a major risk in terms of likelihood and impact: It is recognised as one of the top commercial risks along with geopolitics, the environment, and the economy.

FIGURE 2: TOP GLOBAL RISKS ACCORDING TO THE WORLD ECONOMIC FORUM



Note: Top 10 risks in terms of impact and the top 10 risks in terms of likelihood. Four Risks rank in the top 10 in terms of both impact as well as likelihood. Respondents were asked to rate each risk, based on its impact and likelihood, on a scale from 1 to 7.

Cyber risk is recognised as one of the top commercial risks along with geopolitics, the environment, and the economy.

Many commentators dubbed 2013 the year of the "mega-breach" following a spate of very public incidents. However, what at the time looked like a spike in activity appears to have continued into 2014. While the media will naturally focus on household names, data suggests there is a growing number of cases that remain out of the headlines. For example, the Information Commissioner's last annual report[10] showed a 28% year-on-year increase in data protection cases investigated, and, in April 2014, the Office for National Statistics revealed that fraud cases doubled across England and Wales in 2013 – and that around 70% of those cases had an element of cyber crime attached to them.

Businesses are taking action to respond to the threat: Large organisations have invested in IT security and made improvements in risk governance, as evidenced by the fact that 88% of FTSE 350 companies now include cyber risk within their strategic risk report, up from 58% in the previous year. This is proof of a heightened awareness of the threat at the highest levels of the UK's major firms.

[10] *Information Commissioner's Annual Report and Financial Statement 2013/14,* Information Commissioner's Office, London, 2014.

4 BUSINESSES AND THEIR EXPOSURES

RISK MAP FOR LARGE COMPANIES AND SMALL TO MEDIUM-SIZED ENTERPRISES (SMEs)

As referenced in the taxonomy provided in Figure 1, the potential losses deriving from cyber attacks or non-malicious IT failures fall into the following 11 categories.

FIGURE 3: LOSS CATEGORIES DERIVING FROM CYBER ATTACKS AND NON-MALICIOUS IT FAILURES

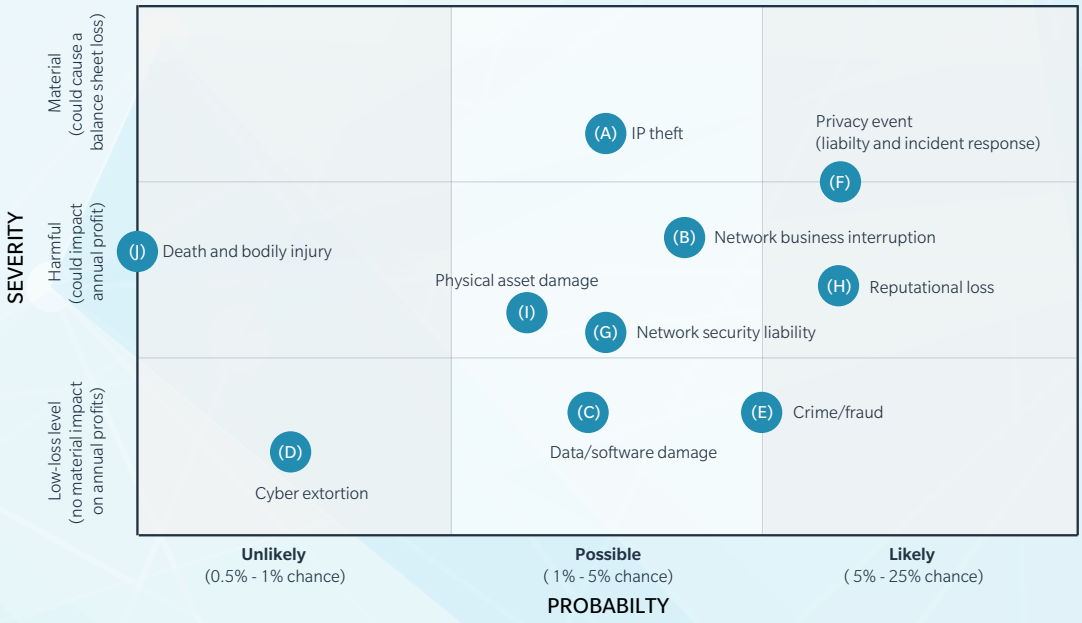
	LOSS CATEGORY	DESCRIPTION
A	Intellectual property (IP) theft	Loss of value of an IP asset, expressed in terms of loss of revenue as a result of reduced market share.
B	Business interruption	Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a result of cyber attacks or other non-malicious IT failures.
C	Data and software loss	The cost to reconstitute data or software that has been deleted or corrupted.
D	Cyber extortion	The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
E	Cyber crime/cyber fraud	The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities, or other property.
F	Breach of privacy event	The cost to investigate and respond to a privacy breach event, including IT forensics and notifying affected data subjects. Third-party liability claims arising from the same incident. Fines from regulators and industry associations.
G	Network failure liabilities	Third-party liabilities arising from certain security events occurring within the organisation's IT network or passing through it in order to attack a third party.
H	Impact on reputation	Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event.
I	Physical asset damage	First-party loss due to the destruction of physical property resulting from cyber attacks.
J	Death and bodily injury	Third-party liability for death and bodily injuries resulting from cyber attacks.
K	Incident investigation and response costs	Direct costs incurred to investigate and "close" the incident and minimise post-incident losses. Applies to all the other categories/events.

Source: Marsh

The insurance industry underwrites cyber risk by forming a view of the severity and frequency of cyber events. Figure 4 summarises that view for the different loss categories for large businesses, noting that one event can trigger more than one loss category. Furthermore, in almost all cyber events, the company incurs incident investigation and response costs, which can account for around 10% -20% of the cost of a cyber-security breach for a large business[11].

[11] *2014 Information Security Breaches Survey.*

FIGURE 4: RISK PROFILE FOR LARGE BUSINESSES



For large organisations, intellectual property (IP) theft is seen as the risk that could have the most severe impact. Quantifying the economic damage caused by the loss of IP or commercially sensitive data is challenging, however, because IP assets are difficult to value and the loss suffered by an organisation is dependent upon how the attacker uses the acquired information. In addition, not all industry sectors are affected in the same way, with IP-rich segments like aerospace and defence, chemicals and pharmaceuticals, and creative media among the most targeted in the UK[12]. There is also less information available for this type of event than for other types of loss, partly due to the fact that incidents are harder to detect and, if detected, more likely to be kept confidential by the victim.

Two other key risks identified by this analysis are the unauthorised disclosure of personal data and system outage events. In particular, losses deriving from the unauthorised disclosure of personal data have a higher severity and frequency than most other risks; a recent high-profile example of this type of loss is the case of a large US retailer that suffered a breach involving approximately 40 million payment card records and the personal data of around 70 million further individuals, following the infiltration of their corporate network via a link with a third-party contractor. The breach resulted in significant costs incurred to respond to the incident, in addition to defending liability claims. Disclosed costs currently stand at £160 million and continue to rise.

Network business interruption or system outage events also display relatively high frequency and severity. Recently, two major games console manufacturers, with a combined total of nearly 160 million subscribers, had their online services disrupted by massive distributed denial-of-service (DDoS) attacks, which took the companies' services offline for more than 24 hours.

Reputational damage is a relatively high-frequency event, as most cyber breaches can have a reputational impact if not handled adequately. Severity for this type of damage is difficult to quantify, but it is an area where proper incident response can limit the severity of loss. This is in line with the 2014 Information Security Breaches Survey, which estimates that reputational damage accounts for around 5%-20% of the cost of a cyber-security breach for large businesses.

[12] *Cyber-attacks: Effects on UK Companies*, Oxford Economics, Oxford, 2014.

Physical losses are a growing concern – both in terms of severity and frequency – given the interconnectedness of cyberspace and the physical world. One example of this new category of risk can be seen in the way that industrial control systems operate in the energy sector. Today, these new generation control systems are built on the concept of openness and interoperability, and this has exposed the sector to a host of cyber security risks that are only just beginning to be understood. A recent example of a physical loss resulting from a cyber attack occurred at a steel mill in Germany, after hackers managed to gain access to the control systems following a successful "spear phishing" attack, which targeted particular individuals for login details. Once access was secured, the hackers were able to cause the unscheduled shutdown of a blast furnace that resulted in "massive damage", according to the German Federal Office for Information Security.

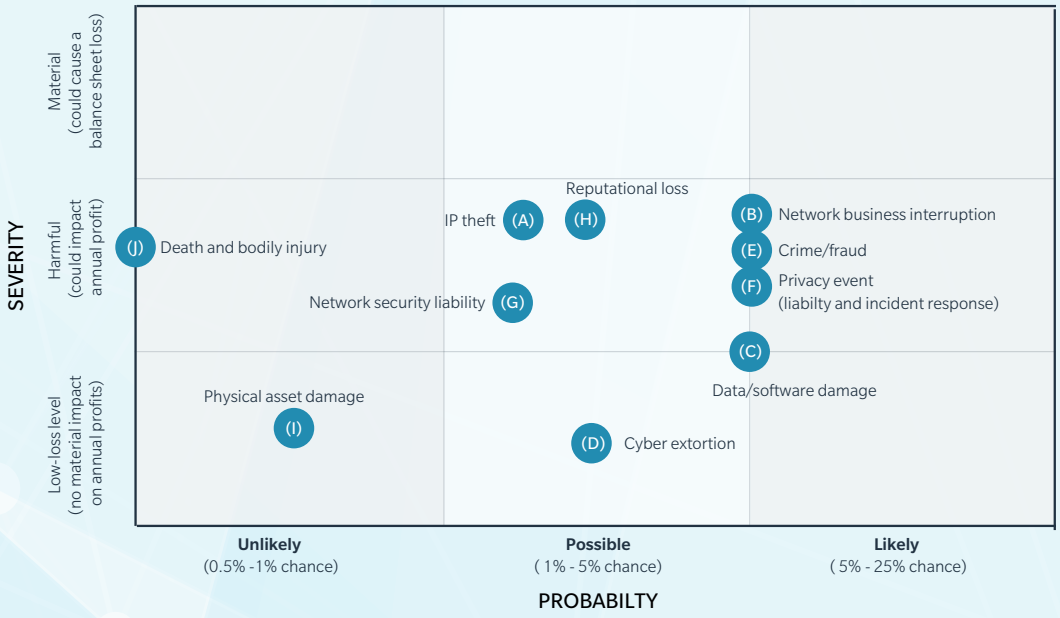
Physical losses are a growing concern – both in terms of severity and frequency – given the interconnectedness of cyberspace and the physical world.

For the time being, the probability of death and bodily injury resulting from a cyber attack is considered to be negligible. We should note, however, that in future, as more devices go online, cyber hacks and system malfunctions could pose a more material threat to human life.

The picture for SMEs (see Figure 5) is broadly consistent with that for larger firms, but for this segment of companies insurers see a higher incidence of cyber crime. For example, a small broker was targeted by a phishing scam, where an email containing a link to malicious software was sent to the financial controller within the business. The controller was tricked into installing the software onto their PC, and this software was used to steal banking credentials. The cyber criminals were subsequently able to complete electronic wire transfers to the total of £100,000 over the following 10 days.

SMEs are also considered to be at a greater risk of data/software damage. This reflects the belief that SMEs are more vulnerable to attack and lack the back-up disaster-recovery solutions of larger firms. On the other hand, with the exception of those working on innovative technologies, most SMEs are considered less likely to suffer from losses connected to damaged reputation or IP theft.

FIGURE 5: RISK PROFILE FOR SMES



RISK MITIGATION AND THE ROLE OF CYBER ESSENTIALS

In June 2014, the UK Government announced the launch of the Cyber Essentials scheme. This scheme was developed by the Government and the insurance industry to fulfil two functions: First, it provides a clear statement of the basic technical controls all organisations should implement to mitigate the risk from common internet-based threats; second, the assurance provides a qualification that allows firms to demonstrate to customers, creditors, insurers, and others that they have taken essential precautions against cyber risk.

As part of this project, insurers considered whether Cyber Essentials is meaningful in terms of risk reduction. The majority view was that Cyber Essentials would provide a valuable signal of reduced risk when underwriting cyber insurance for SMEs, allowing them to use a reduced question set and informing their decisions to underwrite. Accordingly, the participating insurers operating in the SME insurance sector have agreed to build reference to the Cyber Essentials standard into their cyber insurance applications, and will look to simplify the application where accreditation has been achieved by the applicant.

For larger organisations, Cyber Essentials can help make sure they have the basics in place; however, the level of underwriting due diligence is far more intensive. They need to demonstrate a level of IT security that goes beyond the implementation of basic controls and is commensurate with the scale and sophistication of the threat that these larger organisations face. To demonstrate the level of IT security practice required, insurers will look to benchmark against more comprehensive frameworks, such as the SANS Top 20 Security Controls or National Institute of Standards and Technology (NIST) Cyber Security Framework.

Cyber Essentials therefore lends itself to helping insurers differentiate risk in the mass SME market, where it might also be used by others with a stake in SMEs' resilience to cyber attacks, such as banks' lending to SMEs, or for supply-chain quality assurance.

The challenge is to promote Cyber Essentials quickly among SMEs, in line with the gathering pace of the cyber threat. In order to ensure that the cost of certification is not a barrier to adoption of the scheme, Marsh has constructed a cyber insurance product, named "Marsh CyberSmart", that is aimed at SMEs and which will fully absorb the cost of Cyber Essentials certification for the majority of firms. This is made possible by bulk purchasing of the accreditation work and by capturing for the insured the anticipated risk reduction of insurers resulting from Cyber Essentials. The product will be distributed directly and by partner banks and large firms with a relevant SME supplier or customer base. We expect this type of solution to be copied quickly by the insurance industry and to help fill the cyber assurance gap for SMEs. We hope others in the market will follow.

RISK GOVERNANCE AND RISK QUANTIFICATION

Cyber attacks have the potential to be crisis events given the scale of damage, speed of impact, and reputational damage that can follow. This can lead to a negative cycle of declining investor and customer confidence that squeezes cash availability and leads to a liquidity crisis akin to a run on a bank.

For some firms this is not a new situation, with financial institutions, utilities, and other critical infrastructure firms used to having to manage "tail risk" of this form. Most companies' typical risks involve low-level impacts that can be managed within the business, monitored via a risk register, and mitigated by insurance. That approach is likely to be inadequate for a tail risk like cyber, however, given the scale and pace with which it can threaten business viability. This becomes a reporting issue for listed firms under the viability statement now required by the UK Corporate Governance Code. More generally, it becomes a challenge for how risk governance operates.

There are several aspects of risk governance adopted by critical infrastructure providers that offer greater protection against cyber and other tail risks, and which are useful pointers for firms less used to dealing with these kind of risks. We highlight three in particular:

- A board risk committee, chief risk officer, and risk function that all operate independently of executive management.
- A recovery plan that brings together financial, operational, reputational, and other critical functions under a single structure.
- The use of risk scenarios and stress-testing of financial resilience against these.

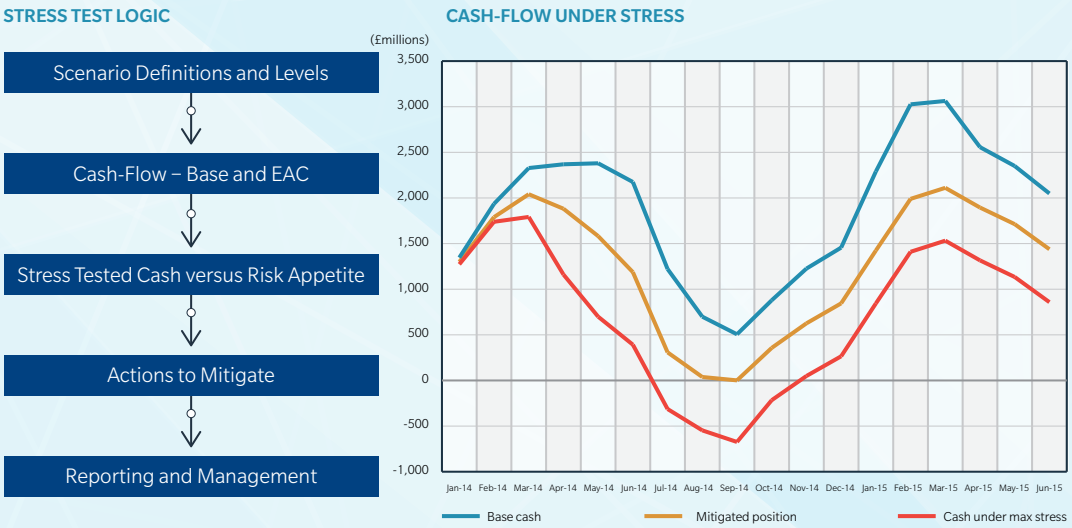
The ownership of risk and recovery planning is particularly relevant for cyber risk. Many firms house responsibility for cyber in technical or security teams. These have a lot to contribute to making the firm safe, but the risk and response plan needs oversight across functions. If an event happens, the firm needs to have considered its sources of cash, its message to stakeholders, alternative supply routes, and many other considerations that go well beyond the IT attack point. For example, some firms have adopted "operational ring-fencing" to ensure that certain assets can be disposed of readily in the event of a crisis occurring (noting that such an approach may reduce the synergies of common ownership).

In terms of stress-testing, the challenge is how to select scenarios and quantify their impact. We have earlier provided a taxonomy of cyber risk as a basis for flushing out scenarios a firm should consider (see Figure 1), noting that these will be different in type and potential severity for each firm. This makes it likely that there will be more than one form of business-critical cyber event to consider. To quantify losses, the traditional approach is to look at historic loss data as a basis for estimating the probability of an event exceeding a given size. However, such a "value at risk" measure is very difficult with a new risk such as cyber because data is so limited. It also focuses on an absolute loss, which may be relevant to the long-run capital position of the firm, but much less so to surviving a cash crisis.

If an event happens, the firm needs to have considered its sources of cash, its message to stakeholders, alternative supply routes, and many other considerations that go well beyond the IT attack point.

The focus for modelling needs to be on cash, not just solvency. Many forms of finance (such as bank lines of credit and insurance policies) come with covenants that mean they may not respond under stress, or at least may not respond at the speed that nervous investors and customers require. Accordingly, for tail risks, stress-testing needs to focus on cash availability, looking at the various sources of funding available and identifying how these will respond under stress. This gives an "event-absorbing capacity" (EAC), which is the scale of cash impact that a firm can reasonably absorb from one or more events occurring. Many businesses are seasonal, and such a measure will therefore vary over time and have a "pinch point", which should be taken as the maximum capacity given the risk that an event occurs through it. Quantification of risk scenarios can then be mapped against this to determine whether additional measures are required to increase EAC. For hard-to-quantify impacts, reverse stress-testing can be used – whereby you start with the more manageable question of how bad would an event need to be to breach the firm's risk appetite with respect to EAC.

FIGURE 6: ANALYSIS OF CASH-FLOW UNDER STRESS



Such a process should be central to tail-risk management, as it brings together risk appetite, scenario-setting, and stress-testing to give a basis for the board to hold management to account on risk-taking. Cyber is just one such scenario to run through this process, although for many firms it will be an increasingly important one.

In terms of mitigation, firms have many forms of actual and contingent capital they can draw on – cash being the obvious benchmark in terms of speed, cost, and certainty. Insurance can be configured to pay quickly, for example, through the up-front claims settlement of business interruption cover or through the use of parametric triggers (that is, linked to a pre-agreed objective metric). Similarly, firms may seek to reconfigure how they run things in the event of a crisis to increase working capital (held as an option in the recovery plan). Ultimately, insurance is another form of contingent capital that should be modelled as part of the resources available to provide financial capacity under stress, whether a result of cyber or some other event.

As a final note, our experience suggests that under this stress-test analysis, firms may choose to shift their insurance programmes from covering day-to-day losses, towards covering tail events. Reflecting firms' typical risk profiles, most claims are for a low level of value, making them relatively expensive to insure and of limited purpose beyond cash-flow smoothing. In contrast, because tail risks are unlikely they are relatively cheap to insure, and doing so may preserve firm viability in the event of a crisis occurring. Economic measures such as total cost of risk (TCOR) allow firms to make these trade-offs in an objective manner.

5 INSURANCE SOLUTIONS FOR CYBER RISKS

PENETRATION OF CYBER INSURANCE

Despite the existence of insurance solutions for most forms of cyber risk, our work suggests that business leaders are often unaware that cyber is an insurable risk. In addition, recent surveys show that those business leaders that are informed are too optimistic about the level of cover provided by the insurance they are currently buying. The majority (52%) of CEOs of large organisations that took part in a recent survey believe that they have cyber cover, whereas the reality is likely closer to 10% if we combine standalone cyber policies (at around 2% penetration) and cyber cover that is embedded in other policies. Differences may be, in part, as a result of selection bias, with those firms responding to cyber surveys more likely to be buyers of cyber cover. A similar gap applies with SMEs, where the penetration of standalone cyber cover is negligible.

FIGURE 7: DIFFERENT ESTIMATES OF CYBER INSURANCE PENETRATION

	SOURCE	VALUE
Percentage of CEOs or CIOs of large organisations who believe they have insurance that would cover them in the event of a breach.	BIS, Information Security Breaches Survey 2014	52%
Percentage of CROs or CFOs who state that their organisation has bought cyber insurance.	Marsh and Zurich cyber risk surveys	15%-20%
Percentage of firms with cyber cover, whether as stand-alone cover or implicit in other policies.	Marsh and Zurich cyber risk surveys	10%
Actual penetration of standalone cyber insurance products among UK large businesses.	Estimate based on policies placed/written by project participant	2%

This evidence suggests a failure by insurers to communicate their value to business leaders in coping with cyber risk. This may, in part, reflect the new and therefore uncertain nature of this risk, with boards more focused on security improvement and recovery planning than on risk transfer. It nevertheless risks leaving insurance marginalised from one of the key risks facing firms. As a first step to raising awareness, Lloyd's, the ABI, and the Government have agreed to develop a guide to cyber insurance and to host it on their websites.

CYBER GAPS IN TRADITIONAL INSURANCE PRODUCTS AND THE AVAILABILITY OF STANDALONE CYBER INSURANCE PRODUCTS

One likely source of the barrier for insurers is the complexity of their offerings. Traditional insurance products have not been designed to protect clients against cyber risks. In addition, underwriters of traditional insurance business lines have, in some cases, reacted to the emergence of this new class of risk by introducing cyber exclusions. The result for clients is a complex picture, with a mix of implicit and explicit cover as well as a number of exclusions to contend with. It makes it an exercise in and of itself to ascertain the true level of cover for any given cyber-risk scenario.

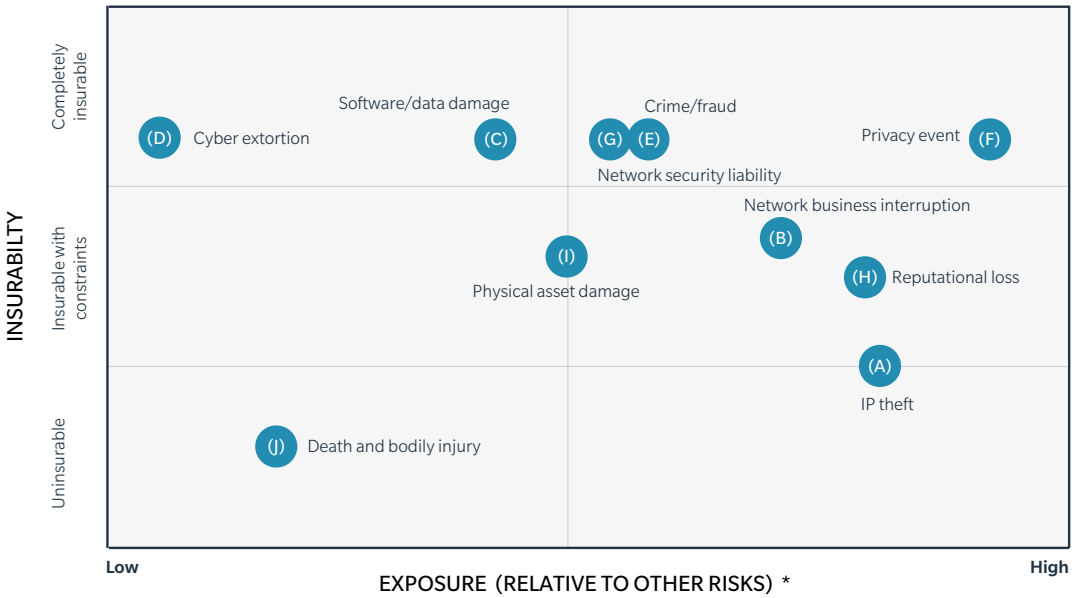
FIGURE 8: EXAMPLES OF TYPICAL CYBER EXCLUSIONS AND GAPS IN TRADITIONAL INSURANCE POLICIES

INSURANCE PRODUCT	MAIN TYPE OF LOSSES COVERED (PRIMARY OBJECTIVE OF THE COVER)	POTENTIAL GAP OF COVER FOR CYBER PERILS
Property	Physical asset damage (first-party).	• Exclusions removing cyber attacks and explicit coverage triggers for physical-asset damage. • Damage to software and data not covered (as deemed intangible form of property).
Business interruption	Lost revenues and additional cost incurred (first-party).	• Traditional policies are not triggered by cyber attacks that do not cause physical damage.
General liability	Third-party liabilities for physical property damage, bodily injury, and advertising injury (liability claims arising from published content, including violation of privacy).	• Exclusions of unauthorised disclosure of personal information.
Errors and omissions/ professional indemnity	Third-party liabilities arising from the performance of professional services.	• Cover may be restricted to liability claims from customers only, hence why claims for disclosure of employees' data are often not covered. • Several exclusions might apply (for example, computer virus transmission).

In order to respond to this gap, the insurance market has developed a dedicated product line that addresses many of the key risks faced by clients. Clients can purchase cyber-specific cover in the form of extensions to traditional policies, or as standalone cyber policies.

Figure 9 describes the level of insurability of different risks among the participating insurers. Insurability is then compared against the risk exposure deriving from the expected frequency and severity for each risk.

FIGURE 9: INSURABILITY AND EXPOSURE FOR DIFFERENT CYBER RISKS



** Combined score for frequency and severity (large organisations).*

The analysis shows that the cyber insurance market provides solutions for a broad range of cyber risks, most of which are rated as completely insurable or insurable with constraints:

- **Privacy events:** In this case, insurance cover can provide protection for both expenses that respond to a data breach (including notifying individuals, setting up call centres, investigating the incident) and for third-party liabilities.
- **Network security liability:** Insurance can provide cover for third-party liabilities arising from certain security events occurring within an organisation's IT network, and for attacks that utilise the organisation's IT assets as part of an attack or as a conduit to pass malicious code to a third party.
- **Data and software damage:** In the event that data or software is deleted or corrupted, insurance can provide indemnity for the costs of external experts to reconstitute that data or software.
- **Cyber crime:** The direct financial loss suffered by an organisation arising from the use of computers to commit fraud or theft of money, securities, or other property. (This would also usually be included as part of a comprehensive crime insurance.)
- **Cyber extortion:** Cover is provided for both the cost of external experts to handle the incident, including conducting the ransom negotiations, and for the payment of the ransom sum.
- **Network business interruption:** In case the company network is disabled for a few hours, a few days, or longer, a company can recover the actual harm it suffers from lost profits or extra expenses. This type of loss has been categorised as insurable with constraints, because insurers are concerned about the potential aggregate exposure deriving from insuring a large number of these risks which might be affected by a single cyber event. So far, the number of cyber insurance policies sold is low and insurers have declared that they have not yet refused to provide cover for this reason. However, as cyber insurance penetration grows, this might become a limiting factor.
- **Physical asset damage:** Several standard cyber exclusions may apply to certain types of property insurance, and, for the moment, there are a limited number of insurers providing standalone cyber cover for this category of risk.
- **Reputational damage:** Insurance products are available from certain insurers that cover business interruption losses arising from an increase in customer churn or reduced transactions that can be directly attributed to the publication of a defined security breach event. This risk is considered insurable with constrains because of the difficulty in establishing an explicit link between the cyber event and the loss.

There are some important risks, however, that are difficult to insure or completely uninsurable. The most important are **intellectual property theft** and **espionage**, for which insurers do not offer cover for direct losses (that is, compensation for the value of the IP asset compromised or the lost revenues as a result of diminished market share), as these types of losses are extremely difficult to prove and quantify. Some insurers do provide legal expenses cover for the pursuit of claims against third parties that are infringing the organisation's intellectual property.

Death and bodily injury risk is highlighted as uninsurable, only because standalone cyber insurance does not currently provide cover for this risk. It is, however, covered by general liability and employers liability products with the limited application of cyber exclusions outside specific industry segments. The lack of appetite within the standalone cyber market might become a concern in the event of the more frequent application of cyber exclusions in traditional general liability products to commercial businesses as a whole.

A MORE CONSISTENT APPROACH TO THE INSURANCE OF CYBER RISK

Cyber gaps and exclusions in traditional policies, together with the emergence of standalone cyber insurance solutions for new risks, often create a complex picture, where businesses struggle to fully understand the boundaries of their cover.

Insurers can help by treating cyber on a more consistent basis. It is foreseeable that there might be an increased use of exclusions in traditional policies, after which cyber exposures will be insured explicitly and priced separately via write-backs (that is, as an add-on to traditional policies) or corralled into standalone policies. Insurers will do this because they aim to have a comprehensive understanding of their exposures to cyber risk. Regulators, reinsurers, and industry associations may favour this move, but it will likely happen slowly as the risk matures and insurers develop a more robust loss experience to work with.

A more immediate solution is for brokers to provide businesses with a statement of cyber assurance, based on a review of exposure and cover versus risk appetite.

A more immediate solution is for brokers to provide businesses with a **statement of cyber assurance**, based on a review of exposure and cover versus risk appetite. The key elements of this approach are:

- **Identification of relevant cyber perils:** Based either on client scenarios generated in-house or pro-forma scenarios adapted to the client, which reflect those that are relevant for the firm's industry and profile.
- **Cyber gap analysis:** Determine the extent of cover provided in the event of a cyber incident, including traditional policies' response to a cyber event and the response of specific cyber cover that is in place.
- **Identification of solutions for uninsured risks:** Identify and arrange the appropriate cover to address uninsured risks where an insurance solution is available.
- **Cyber assurance:** Formal report, including assurance statement that cyber cover is in place to an agreed specification for those insurable risks that have been identified, and as appropriate to the firm's risk appetite.

For such assurance to be valuable, it should ideally form part of the wider risk assessment described earlier, including scenario identification and stress-testing. It can then form a fully integrated part of a firm's risk management and support viability statements and other signals of firm resilience.

PRICING AND DATA AVAILABILITY

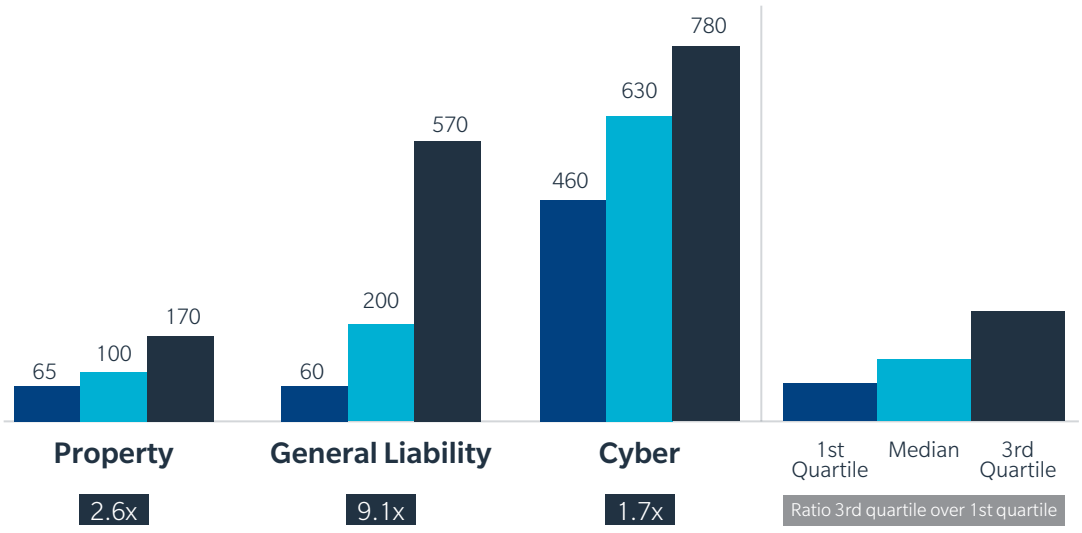
An analysis of the pricing for cyber insurance cover shows that the rate on line (premium divided by limit of indemnity purchased) for the primary layer (part of the policy that pays first in case of a loss) for this class of business is three times higher than for general liability cover and six times higher than for property.

There are several factors that influence the price of different insurance products. In the case of cyber insurance, the price may also be driven by uncertainty over the risk compared to more traditional covers. This seems to be the case, with much flatter pricing for cyber across firms than for other lines of insurance; the difference between third and first quartile pricing is 1.7x for cyber, 9.1x for general liability, and 2.6x for property. The combination of a higher absolute price and lower price differentiation suggests that cyber is early in its development and that underwriters are more conservative about the risk, creating a challenge to a core role of insurance – namely, that high pricing discourages take up, and flat pricing provides no incentive for firms to reduce their cyber risk and save on premiums.

FIGURE 10: PRICING ANALYSIS FOR CYBER, PROPERTY, AND GENERAL LIABILITY

Relative pricing index, property =100

Based on rate on line for primary layer for companies with turnover <US$1 billion



Insurers rate cyber risk based on industry segment and type of activity, hard metrics of risks (such as number of personal records, number of employees, and turnover), and an assessment of the IT maturity of the company. However, the limited amount of loss data due to low product penetration limits the ability of insurers to differentiate on price. In addition to reducing pricing differentiation, the scarcity of data forces insurers to use over-conservative assumptions. Any form of data pooling among underwriters would therefore benefit their customers.

Government agencies represent an additional source of information for insurers. It is worthwhile mentioning that in developing the privacy breach product for the US market, insurers benefited from the availability of a database that collated all personal data breaches known due to the near-universal and mandatory breach notification law in the country. In the UK, government agencies have different sources of information. Much of this has been made available via data feeds, such as the Cyber Security Information Sharing Partnership (CiSP). The Government and the insurance industry will build on this and the positive collaboration shown in this work to continue to share data and insights on the evolution of cyber risk. As part of this, they will explore how to make existing data more useable and accessible to the insurance industry, while protecting individual customer and insurer data confidentiality. The insurance industry and the Government will also maintain a dialogue on cyber security policy to help improve each other's understanding and awareness of how best to make the UK one of the safest places to do business in cyberspace.

The non-physical nature of cyber risk makes it possible for insurers to suffer losses from a vast number of clients spread across different geographies as a result of a single event.

Insurers and the Government will create a forum for policy discussion, data, and insight exchange. This needs to be done within the bounds of competition law and customer data protection. The Government will work together with the insurance industry, including the ABI and Lloyd's, to establish this forum.

AGGREGATION OF CYBER RISKS AND RISK POOLING SOLUTIONS

Cyber insurance is a global class of business. The non-physical nature of cyber risk makes it possible for insurers to suffer losses from a vast number of clients spread across different geographies as a result of a single event. That creates aggregation risk, for which an insurer or reinsurer could find itself burdened with catastrophic losses, and which might result in the non-payment of claims.

Four such scenarios were considered by the insurer expert panel as a basis for considering how to model and mitigate aggregation risk.

FIGURE 11: CYBER CATASTROPHE SCENARIOS DISCUSSED WITH THE EXPERT PANEL

1	Data breach	The world's largest provider of cloud data suffers a major breach of security.
2	Business interruption	The world's largest provider of cloud-based application hosting suffers a 24-hour outage.
3	Payment systems	Security breach at the largest provider of outsourced payment processing services; ecommerce payments not possible for 48 hours.
4	National electricity supply	Cyber attack results in shutdown of electricity transmission system for 48 hours.

Modelling the aggregation of physical risks is well established. For example, a large amount of historical data is used to build probabilistic models with regard to natural catastrophes. This data does not exist for cyber risk, which means that insurers have to rely on experts making educated assumptions when assessing the severity and frequency of possible cyber catastrophe scenarios. This has led to there being an extremely wide range of estimates for the likely cost of each of the scenarios listed above.

So too with the difficulty facing individual firms in quantifying their cyber risk, an alternative approach is to look at total exposure and capacity. We estimate that, in 2014, the global exposure of the insurance industry to cyber risk (as quantified by the total of standalone cyber indemnity limit sold) stood at around £100 billion. Assuming that the possible maximum loss (PML) follows the range for property risk (up to 20% of the total exposure), the insurance industry could face a cyber PML of up to £20 billion. If we consider that the cyber insurance market could treble in the next three to five years, the industry PML for cyber risks could easily exceed the global insurance/reinsurance capacity available for other aggregating events, such as nuclear disaster (£3 billion) or natural catastrophe (£65 billion).

FIGURE 12: COMPARISON OF CYBER INSURANCE EXPOSURE AGAINST GLOBAL INSURANCE AND REINSURANCE CAPACITY FOR OTHER INSURANCE CLASSES

Global exposure of the insurance industry to cyber risk total value.	£100 billion
Maximum global (re)insurance capacity any "one event" for natural catastrophe (Tokyo or Californian earthquakes).	£65 billion
Maximum global insurance/reinsurance capacity for a nuclear first-party loss (more comparable to cyber).	£3 billion
Range of possible maximum loss (PML)/total exposure ratios for property portfolios.	0.15% (for UK property) - 20% (PML for hurricane for small exposed Caribbean island)
PML for cyber (assume the same PML/total exposure ratio of selected property portfolios).	£150 million – £20 billion

Despite the lack of a clear consensus of the size of the possible maximum loss that the insurance industry could face, at the moment most insurers are comfortable with the size of their total exposure and the market does not face any supply constraints in the short term. Indeed, underwriters participating in this project have expressed a strong appetite to grow this line of business.

It is possible that aggregate exposure either does already or will soon become a problem for the market to absorb, since the fact that such a risk has not yet occurred is no doubt encouraging the market to continue to grow its exposure.

While some market participants have questioned whether a possible Government backstop may be necessary given the scale of possible exposure, there is no conclusive evidence of the need for such a solution at present. Other challenges in creating a pool in advance of systemic claims materialising involve the definition of what events and losses would be in scope (in particular, given the complexity referred to earlier of how cyber is treated in existing policies), the lack of data to model the level and price of risk to be transferred, and a lack of consensus among insurers about the need for recourse to Government support.

This position might change quickly in light of claims coming through. Rather than wait for that to happen, there are things that insurers can do now to prepare for such a situation. Specifically, we see the following steps as useful foundations for addressing possible deficiencies in market capacity and the need for a cyber risk pool:

- Improve the understanding of cyber interconnectedness and impact on different types of cover provided.
- Clarify what cyber exposures are included in the traditional insurance products.
- Increase consensus on the scale of possible losses and potential impact for the insurance industry.
- Propose a definition of systemic events that are either not insurable by the private sector, or where the global capacity available for such events is inadequate (in terms of trigger events and type of losses).

One of the tasks of the new forum will be to facilitate the sharing of insights on aggregation and cyber disaster scenarios, with a view to improving the ability to underwrite risks and the understanding of their aggregation.

6 CYBER AS AN EXPORT OPPORTUNITY FOR LONDON

SIZE OF THE CYBER INSURANCE SEGMENT AND ROLE OF THE LONDON MARKET

Cyber is a fast-growing sector within the insurance industry. We estimate that, in 2014, the global premium income for standalone cyber increased by 50% versus the previous year, and now totals around £1.5 billion-£2 billion, representing just 0.1% of the global property and casualty insurance premium pool.

The vast majority of the premium income derives from US-domiciled companies (approximately £1.5 billion), due to the fact the US has been the first market to adopt standalone cyber insurance products with solutions centred around data breaches. Insurers now expect increased interest from other countries as awareness and regulation drive demand. The premium income from UK companies is estimated at 1.5% of the global market (around £20 million-£25 million).

London is already a major centre for cyber insurance. Insurers write more than 10% of the global cyber insurance business from London, which represents around £160 million in premiums, with the majority of the flow into London coming from the US.

The London market is well positioned to compete for large and complex risks, and over time has provided innovative solutions for new threats. Cyber fits this description and, as such, should be a priority for the London market as it plays to its traditional strengths. With the expected growth of cyber insurance both inside and outside the US, it represents a significant export opportunity to:

- Increase the share of the existing US, data-breach-driven market.
- Widen the scope of cyber cover to other forms of loss from cyber attack.
- Widen the geographic scope. The European markets could grow strongly as a result of the expected approval of the General Data Protection Regulation from the European Commission. In the current version, the regulation introduces mandatory breach notice to affected data subjects and significantly increases the fines that can be imposed by national data protection regulators.

In order to capture this opportunity, Lloyd's and UK Trade & Investment (UKTI) will co-operate to promote the cyber insurance offering of the London market to key countries around the world.

FACILITATING THE EMERGENCE OF A MULTIDISCIPLINARY CYBER OFFER

In order to manage the cyber threat, businesses require a wide set of financial, advisory, and technical services, including those service-based industries in which the UK (and specifically London) excels, such as risk management, insurance, technical cyber security, and specialised incident response services.

We expect the natural evolution of the market will identify the combinations of these services that work well for global businesses and can be exported. In order to accelerate the process of establishing connections and creating a more joined-up cyber offer, we recommend a multidisciplinary task force. It should look to bring different disciplines together for creative discussion on how they might bring their capabilities and marketing together.

TheCityUK has agreed to take this on. The initial steps are the definition of the terms of reference and composition of the task force, with input from the Cabinet Office.

7 RECOMMENDATIONS

This report has analysed the role of insurance as a means to make UK companies more resilient to cyber attack, and as a possible way to export London's leadership in cyber insurance and related services. The following recommendations have been made as a result of the work:

1. HELPING FIRMS GET TO GRIPS WITH CYBER RISKS:

- The participating insurers will include the Cyber Essentials accreditations as part of their risk assessment for SMEs as a basis for encouraging Cyber Essentials adoption.
- Marsh will launch a cyber cover for SMEs that absorbs the cost of Cyber Essentials accreditation.
- Firms should review their management of cyber risk. This should include mechanisms such as the establishment of a board risk committee and chief risk officer, the development of a joined-up recovery plan, and the use of stress-testing to confirm financial resilience against different high-risk scenarios including cyber.

2. HELPING THE INSURANCE INDUSTRY TO ESTABLISH CYBER INSURANCE AS PART OF FIRMS' CYBER TOOL-KITS.

- Lloyd's, the ABI, and the Government will develop a guide to cyber insurance and host it on their websites.
- Brokers should provide firms with a cyber assurance statement, giving the board comfort on the completeness of their insurance with respect to cyber.
- The Government will work together with the insurance industry, including the ABI and Lloyd's, to establish a forum for data and insight exchange and for policy discussions. One of the main goals of the forum will be to improve the information available for underwriting and for determining aggregation risk.
- The insurance sector will continue industry discussion on market capacity and the need for a cyber-risk pool as information improves on which to judge aggregration risk.

3. HELPING LONDON TO BE A GLOBAL CENTRE FOR CYBER RISK MANAGEMENT:

- Lloyd's and UKTI will co-operate to promote the cyber capabilities of the London insurance market to key countries around the world.
- TheCityUK will look to set up a task-force aimed at coordinating different sectors in London with respect to their cyber offer.

APPENDIX: CYBER SECURITY GUIDANCE AND SUPPORT FOR BUSINESSES

CYBER ESSENTIALS

Cyber Essentials is a new Government-backed and industry-supported scheme to guide businesses in protecting themselves against cyber threats. Cyber Essentials is free to download. Any organisation can use the guidance to implement essential security controls.

The scheme provides businesses of all sizes with clarity on good basic cyber security practice. By focusing on basic cyber hygiene, organisations will be better protected from the most common cyber threats. Cyber Essentials is for all organisations, of all sizes, and in all sectors. It is not limited to companies in the private sector, but is also applicable to universities, charities, and public sector organisations.

Scheme website: www.cyberstreetwise.com/cyberessentials/

10 STEPS TO CYBER SECURITY (GUIDANCE FOR LARGE ORGANISATIONS)

The "10 Steps to Cyber Security" guidance for large businesses looks at how to safeguard a company's most valuable assets, such as personal data, online services, and intellectual property. The guide explains how cyber security is a strategic business risk which needs to be managed at board level.

10 Steps guidance: www.gov.uk/government/publications/

SMALL BUSINESSES: WHAT YOU NEED TO KNOW ABOUT CYBER SECURITY

This short booklet contains practical guidance for small businesses on how to put simple cyber security measures in place. It explains the cyber threat and how small businesses can ensure they are protected. By taking the advice in this guidance, small businesses protect their assets, customers, and their peace of mind.

Small business cyber guidance: www.gov.uk/government/publications/

ADVICE TO BUSINESS: REDUCING THE IMPACT OF COMMON CYBER ATTACKS

This advice from CESG, the Information Security arm of GCHQ, and CERT-UK, the UK National Computer Emergency Response Team, helps organisations understand what a common cyber attack looks like and explains why all organisations should establish basic security controls and processes, to protect themselves from such attacks.

Common attacks guidance: www.gov.uk/government/publications/

CYBER SECURITY INFORMATION SHARING PARTNERSHIP (CiSP)

The Cyber Security Information Sharing Partnership (CiSP) is a collaboration between industry and Government to share cyber threat and vulnerability information. This increases overall situational awareness of the cyber threat and helps reduce the impact on UK business. Any UK-registered company with an electronic communications network in the UK can apply for membership of the CiSP.

CiSP website: www.cisp.org.uk

FREE ONLINE INFORMATION SECURITY TRAINING COURSE FOR SMEs: "RESPONSIBLE FOR INFORMATION"

"Responsible for Information" is a free e-learning course for staff in micro, small and medium-sized enterprises (SMEs). It helps employees and business owners understand information security and associated risks, and provides good practice examples and an introduction to protection against fraud and cyber crime.

Free e-learning course for SMEs: www.nationalarchives.gov.uk/sme/

CYBER INCIDENT RESPONSE SERVICES

There are two schemes to help organisations deal with and clean up a cyber attack. They are led by CESG, the Information Security arm of GCHQ, and the Centre for the Protection of National Infrastructure (CPNI).

CESG website: www.cesg.gov.uk
CPNI website: www.cpni.gov.uk

CYBER SECURITY INNOVATION VOUCHERS

Innovation Vouchers provide funding of £5,000 for businesses to engage an external expert to gain new knowledge to help the business innovate, develop, and grow. SMEs can apply for Innovation Vouchers to help with advice towards protecting and growing their business by having effective cyber security. A specific cyber security Innovation Voucher theme is also under discussion. Further details to follow.

Apply for a voucher: https://vouchers.innovateuk.org/cyber-security