

# Global Cyber Market Overview

*Uncovering the Hidden Opportunities*

*June 2017*

# Table of Contents

- Introduction .....3
- Cyber insurance, a market still in its infancy .....4
- The US market.....5
- The upcoming European opportunity.....7
- A market with growing competition .....8
- Emerging needs and evolving products .....9
- A nascent reinsurance market .....11
- Opportunities beyond risk transfer solutions .....12
- Conclusion .....14
- Contacts .....15

# Introduction

Highly publicized attacks on blue chip companies, announcements of alliances formed between insurers, reports of partnerships established with cyber security firms and hiring of renowned experts have all contributed to making cyber one of the hottest topics in the insurance industry. However, behind the hype of the media and the marketing battles fought by insurers and brokers to position themselves as leaders in the market, there is the reality of a genuine opportunity. In this paper, we explore how the cyber insurance market has evolved in recent years to understand how:

- the drivers underpinning the growth in the US will contribute to the growth in other part of the world, with a focus on the upcoming European market,
- a few insurers have been able to build significant presence in the market but face imminent challenge as more and more insurers are now competing in this space,
- customer needs and covers are developing and the opportunities this is likely to bring,
- the reinsurance market is playing its part in supporting cyber insurers, and
- key players have looked beyond the insurance market to identify growth opportunities.

The preparation of this white paper has been made possible thanks to the insights provided by Aon's Cyber Solutions team, in particular Kevin Kalinich, Global Practice Leader, Cyber Insurance, and Luke Foord-Kelcey, Co-head, Global Cyber Practice, Aon Benfield. Last but not least a special word of thanks to Jeremy Maginot, Director, Consulting, Aon Inpoint, who has led the creation of this white paper with support from Aon Inpoint colleagues across the globe.

Sincerely,

**Michael R. Moran**  
Chief Executive Officer  
Aon Inpoint

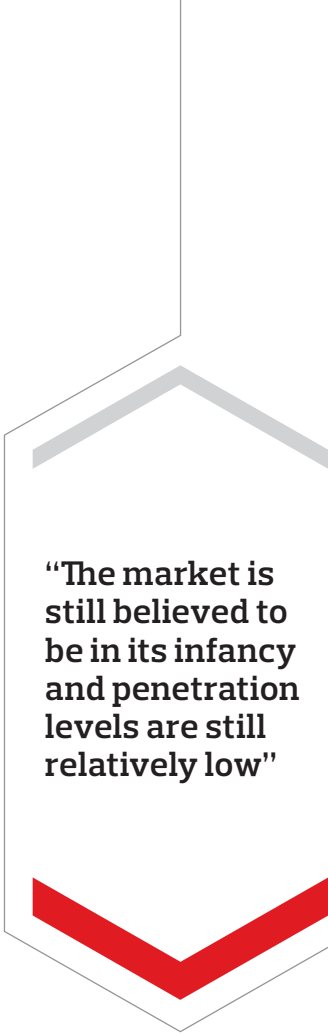
# Cyber insurance, a market still in its infancy

Cyber insurance products have been around since the late 90s. The demand originated from the technology, media and telecom (TMT) sector and professional services firms which needed covers to protect themselves against inadvertent transfer of malware (cyber liability cover) and loss of confidential client information (privacy breach cover). Initially developed as add-on covers or bundled into existing liability or professional indemnity policies, these early products were a first attempt by insurers to offer traditional risk transfer solutions to help their clients with an emerging risk. Elements of cyber coverage have also been found in property, general liability, crime, K&R, and other lines of insurance. However, in policies where cyber coverage intent was silent, some courts have ruled in favor and others have denied coverage. As a result, insurers have tightened up their policies to clarify intent of coverage. In most cases, this has meant introducing specific cyber exclusions but in some instances, insurers have added affirmative cyber coverage in property or liability policies. However, there remain significant elements of cyber coverage under other lines legacy policies.

With the global strengthening of regulations on loss of personally identifiable information (PII), the costs related to the handling of a breach increased: i.e. costs of reporting a breach to the regulator, customer notification, PR costs and legal expenses. Awareness of cyber threats also started to reach the boardroom. As a result, the demand for cyber insurance products grew beyond the TMT and professional services sectors to reach all industries handling confidential customer information: financial institutions, retailers, hospitalities and the healthcare sector. Along with the growing demand from a wider range of companies came the need for more sophisticated and specific covers which could not be addressed with endorsements or add-ons to traditional policies, leading the way to standalone cyber products.

A study conducted by Aon and Aon Inpoint estimated the 2015 global standalone cyber market to be worth \$1.7bn in annual gross written premium. While still cyber insurance has been around for over 25 years, the market has grown tremendously in recent years, achieving annual growth rates of c.30% between 2011 and 2015; levels not seen in traditional lines of business. With data pointing at higher growth rates in 2016, we estimate last year's global standalone cyber market to be c. \$2.3bn in premium.

However, the market is still believed to be in its infancy and penetration levels are still relatively low: <15% in the US but <1% in other regions of the world, leaving plenty of room for further growth. In particular, the percentage of US companies that purchase cyber insurance varies significantly by industry and company size segment. For instance, we estimate that over 75% of financial institutions, retail, healthcare and hospitality companies with revenue over \$1bn purchase some cyber insurance. On the other end, the level of penetration among small and medium businesses is estimated to be less than 5%.



**“The market is still believed to be in its infancy and penetration levels are still relatively low”**

# The US market

The US is the largest market and is estimated to account for c.\$1.5bn or c.90% of the 2015 global standalone cyber premium. It has been the main contributor behind the growth of cyber premiums.

The impressive growth rates observed in the US have been driven by several factors.

Data breach legislation was progressively enforced across the US and is now in effect in 47 of the 50 states. On March 15th, the New Mexico Senate passed the Data Breach Notification Act to become the 48th state with a data breach notification law once the bill is signed by the governor, leaving Alabama and South Dakota as the only states without such a statute.

Legislation started in California where The Mandatory Data Breach Disclosure Law was first signed in 2002 and effective from July 2003, making firms legally obliged to notify affected parties in the event of a data breach. Similar legislations were subsequently enforced in others states between 2005 and 2016.

Highly publicized data breach incidents involving large corporations targeted by hacking groups (e.g. Sony in 2011, Target in 2014, Ebay in 2014 and the 2013 and 2014 Yahoo breaches disclosed in 2016) have contributed to raising both public and C-suite Executive awareness of cyber threats. A survey conducted by Aon shows that cyber now appears on the boardroom agenda of a growing number of companies. This trend is likely to continue.

## Key growth drivers

<b>Legislation</b>	Data breach legislation has been enacted in 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands
<b>Awareness</b>	In 2015, US firms ranked cyber as their 5 <sup>th</sup> most important risk, compared to 18 <sup>th</sup> back in 2011
<b># of breaches</b>	More companies are uncovering data breaches and reported breaches in the US have risen by c.325% since 2006
<b>Higher cost</b>	On average, the cost of a data breach is 60% higher than it was in 2006

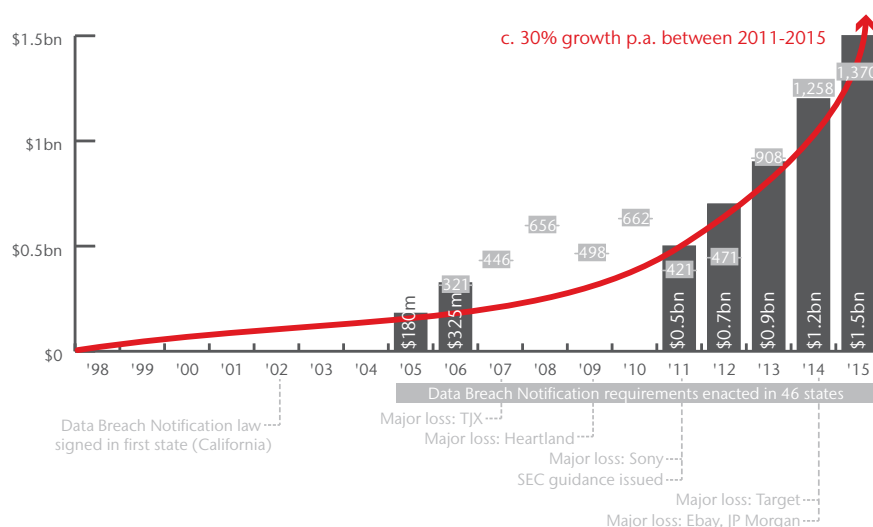
Furthermore, the effect of a data breach on a company's brand and customer loyalty can result in loss of future revenue. It can also impact potential merger and acquisition deals as recently illustrated with the disclosure of Yahoo data breaches shortly after Verizon announced its acquisition plan; Verizon subsequently requested more favorable deal terms.

While cyber insurance was initially purchased by TMT companies and professional services firms, in recent years demand has been predominately driven by large corporations storing personally identifiable information (PII) and processing vast amount of financial transactions, i.e. large retailers, heavily regulated financial institutions. These companies are currently estimated to account for nearly half of the US standalone cyber premium, 21% and 29% respectively. Healthcare is also a large and growing segment of the US cyber market. Estimated to represent 15% of the standalone premium, these companies are increasingly purchasing data breach cover to protect the sensitive patient information they hold. This is mainly driven by the HIPAA legislation, which provides data privacy and security provisions for safeguarding medical information, and now holds companies responsible in the event of a breach. Originally embedded in liability policies, data breach covers for healthcare companies are now offered by insurers on a standalone basis.

There is also growing concern about how hospitals and clinics are exposed to cyber-attacks which could, for example, impact the operation of networked life-support devices.

This in turn is driving demand for cover against third party bodily injury arising from a cyber event.

**Historical estimated standalone cyber market size in US** ■ US market size ■ No. of disclosed data breaches



Sources: Betterley Report, Advisen, PropertyCasualty360, Business Insider, Marsh, Aon, datalossdb.org, Identity Theft Resource Center, NCSL, Ponemon Institute, Aon Global Risk Survey, Aon Inpoint analysis

## Estimated breakdown of standalone cyber market in the US (2015)

Company type	Industry and revenue	SME	Mid-market	Large corporate	% of total
Companies storing personal data	Technology	\$39.0m	\$18.0m	\$14.0m	5%
	Telecoms and media	\$3.3m	\$8.0m	\$13.0m	2%
	Education	\$5.3m	\$46.0m	\$21.0m	5%
	Professional services	\$9.4m	\$43.0m	\$22.0m	5%
Financial transactions driven companies	Retail and wholesale	\$76.0m	\$141.0m	\$93.0m	21%
	Financial institutions	\$31.0m	\$180.0m	\$227.0m	29%
	Business services	\$6.7m	\$47.0m	\$33.0m	6%
	Hospitality	\$5.5m	\$22.0m	\$13.0m	3%
Companies exposed to operational risks	Manufacturing	\$56.0m	\$19.0m	\$16.0m	6%
	Utilities	\$1.3m	\$4.1m	\$15.0m	1%
	Energy (Oil and Gas)	\$1.2m	\$3.6m	\$9.0m	1%
Companies storing personal data & exposed to operational risks	Healthcare	\$3.4m	\$103.0m	\$81.0m	15%
	Transportation	\$13.0m	\$14.0m	\$10.0m	2%
<b>Total</b>		<b>\$282.0m</b>	<b>\$649.0m</b>	<b>\$567.0m</b>	<b>100%</b>
				<b>\$567.0m</b>	<b>101%</b>
					<b>\$1.5bn</b>

Notes: SME are defined as companies with sales/turnover below \$100m; Mid-market: \$100m to \$1bn; Large corporate: >\$1bn

Source: Advisen, Marsh, Bureau van Dijk, Aon placement data, Aon Inpoint analysis

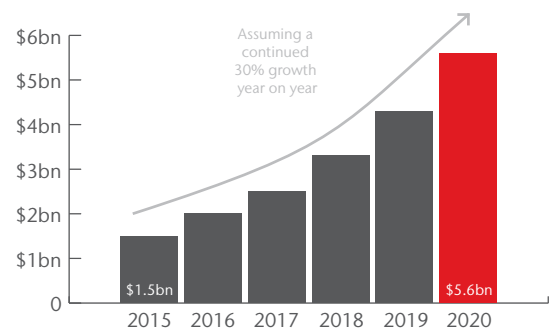
With higher penetration levels compared to the rest of the market, medium-size and large companies are the main buyers of cyber cover. We estimate these companies to represent 80% of the standalone cyber premium. Although further penetration in these segments is expected to drive future growth, demand is also expected to come from the smaller segments. These firms are increasingly assessing their cyber exposures and are concerned about the potential impact of a cyber incident.

There is also a lot of growth potential from non-PII industry segments (i.e.

manufacturing, energy, utilities) as they start to get a better understanding of their exposure to a cyber event and the impact it could have on their operations.

Assuming the US standalone cyber market experiences growth rates comparable to those witnessed in recent years, it could reach \$5.6bn in annual gross written premium by 2020.

## US standalone cyber market projection



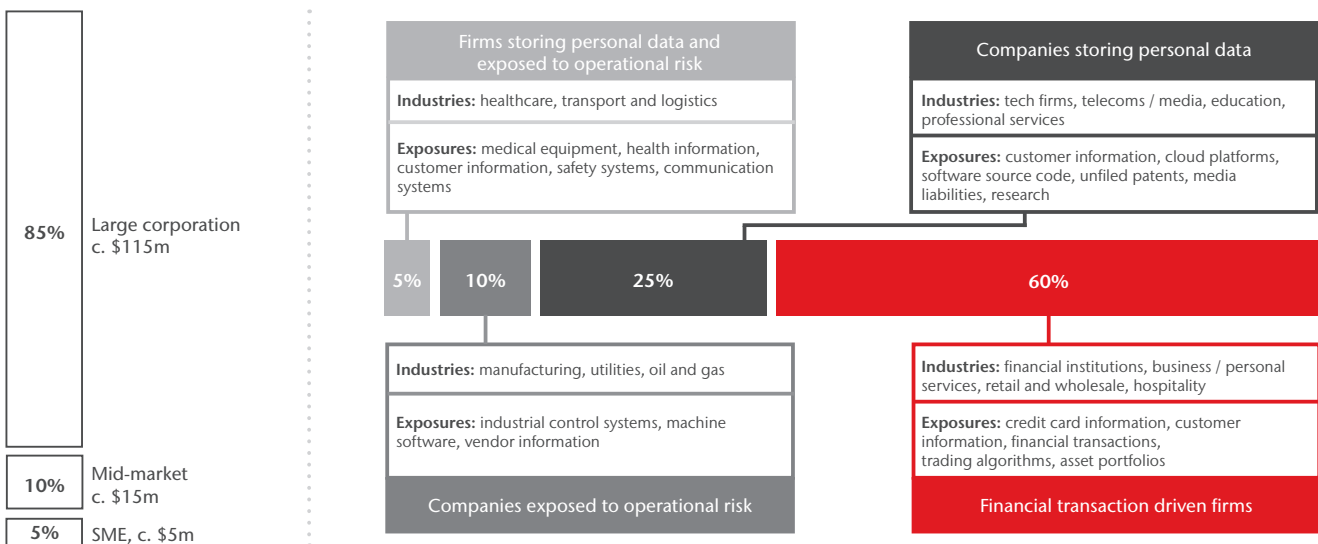
# The upcoming European opportunity

Until recently, most of the appetite for cyber protection in Europe was limited to large companies. However, in the last 18 months demand for cyber insurance products has come from a wider cross-section of the market. Like in the US, this is largely explained by insureds becoming more aware of their exposure to cyber perils coupled with rising concerns about the impact an event could have on their company's balance sheet.

Aon Inpoint estimates that the 2015 European standalone cyber market was worth \$135m in annual gross written premium.

Large companies with a turnover above \$1bn have contributed most of the demand and we estimate they represented over 85% of the standalone premium. Similar to the US market, financial institutions, large retailers and the hospitality sector are the main buyers of cyber insurance. The lack of a strict set of regulations across the region means that until now the demand was mainly focused on extortion and business interruption cover. However, this is expected to change with the European Global Data Protection Regulation (GDPR).

## 2015 breakdown of standalone cyber premium using Aon's portfolio



Source: Aon broker insights, Aon GRIP data, Aon Inpoint analysis

The upcoming GDPR, to be enforced in May 2018, is expected to be a catalyst for accelerated growth. All companies doing business with clients and prospects in the EU will need to comply with the new legislation. It will require companies to notify the regulator and individuals in the event of a breach of personally identifiable data. If companies do not comply with the new regulation, they could be fined up to 2% or 4% of their global revenue depending on the type of activity and subject to monetary caps. Companies will have a limited amount of time to ensure that they adhere to the new regulation.

The European market is trying to react to the anticipated uptick in take up rates. The main brokers are helping their clients prepare for the upcoming regulation changes, supporting them in evaluating their cyber exposure and the adequacy of existing covers. Brokers are also working closely with local insurers to help them tailor their products and ensure their offerings address the needs of their clients.

	Pre-GDPR	Post-GDPR
<b>Legislation</b> 	<ul style="list-style-type: none"> <li>No general legislation mandating notification following a breach</li> <li>Weak regulators with limited ability to sanction firms</li> <li>EU laws enforced with varying degrees of severity</li> </ul>	<ul style="list-style-type: none"> <li>Strict regulation with a general requirement to notify in the event of a breach</li> <li>GDPR regulations allow for a fine of up to 2% of global turnover</li> <li>EU wide enforcement of GDPR</li> </ul>
<b>Awareness</b> 	<ul style="list-style-type: none"> <li>Cyber already recognised as an emerging risk in Europe</li> <li>Aon clients currently view Cyber as 14<sup>th</sup> biggest risk</li> </ul>	<ul style="list-style-type: none"> <li>Increased awareness expected to be driven by GDPR with higher numbers of data breaches likely to be publicised</li> <li>Aon clients already expect Cyber to be their 8<sup>th</sup> biggest risk by 2018</li> </ul>
<b>Number of breaches</b> 	<ul style="list-style-type: none"> <li>European breach rates are already growing fast, 36% since 2011</li> </ul>	<ul style="list-style-type: none"> <li>Mandatory notification is likely to drive known breach numbers much higher</li> <li>In the US where similar legislation already exists there were 1.1k (c.85%) more publicised breaches compared to Europe in 2015</li> </ul>
<b>Cost</b> 	<ul style="list-style-type: none"> <li>The cost of data breaches in Europe currently lags that of the US by 35% on average</li> </ul>	<ul style="list-style-type: none"> <li>European firms are likely to suffer higher costs as a result of GDPR</li> <li>US firms have seen the cost of data breaches rise at a rate of 9% a year since 2012</li> </ul>

# A market with growing competition

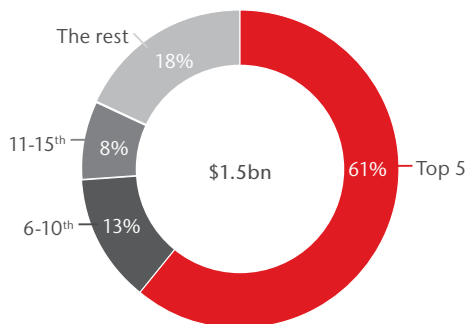
The increasing demand for cyber insurance and the growth potential of the market have attracted more and more carriers.

In a global P&C market where yearly growth levels have not exceeded the low single digits and where insurers have struggled to achieve organic growth, the emergence of a new product growing at 30% year on year has generated a lot of interest.

While in the early 2000s there were less than a dozen of insurers that were able to offer cyber covers, today, close to seventy are offering standalone cyber products, albeit with varying degrees of protection, risk mitigation and incident response service levels.

In the US, the five largest insurers (four domestic insurers and one Lloyd's insurer with local operations) have established a significant market leadership presence. We estimated them to write over 60% of the 2015 US standalone cyber premium. The three largest insurers have written cyber since the late 90s – early 2000s and have developed cyber products and incident response capabilities to establish themselves as recognized market leaders. Their longstanding position in an emerging market also means they have accumulated underwriting data which other insurers cannot access, further enhancing their dominant position. The proprietary information at their disposal coupled with their expertise in creating wordings to address regulatory changes and insureds' needs has allowed them to demonstrate a broad appetite and largely unrivalled flexibility levels. As a result, they have been seen as go-to insurers and have been able to participate on a broad range of programs.

## US total standalone cyber premium by carrier

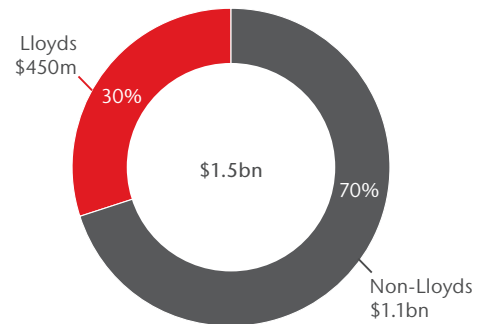


Source: Aon Inpoint analysis

About \$450m of the 2015 US standalone cyber premium was written in Lloyds. The London market is represented by a handful of long-established and committed cyber players which are actively growing their share and developing their underwriting and servicing capabilities. Other recent entrants and cautious players are still trying to define how they want to position themselves in the long run. They tend to limit themselves to providing small lines of follow capacity on excess layers and target small insureds by offering cyber covers as options or part of packages via

coverholders. Smaller risks are perceived to be easier to access and are also considered more attractive compared to large risks which could leave insurers exposed to more volatile results.

## US total standalone cyber premium

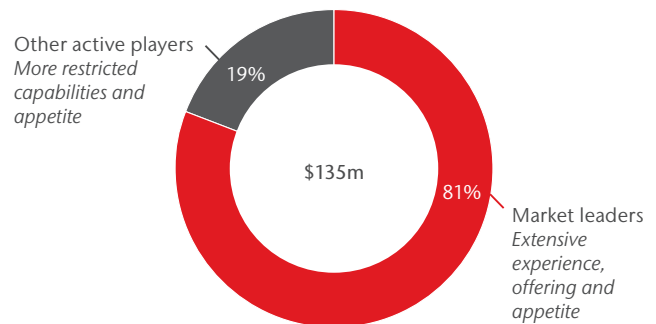


Source: Aon Inpoint analysis

In Europe, the same top three insurers have significant market presence in the market and are believed to write three quarters of the standalone premium. They have leveraged the expertise and capabilities developed in the US market and have pro-actively built upon their relationships with global brokers to position themselves on the European scene.

There is enough capacity to write the business domestically and unlike in the US market, only a limited amount of European cyber insurance business (complex deals or large excess layers) finds its way to the London market.

## European standalone cyber premium



Source: Aon GRIP data, Aon Inpoint analysis

However, the competition is growing to capture the cyber opportunity. London players are driving innovation to attract more cyber premium and more domestic insurers are developing their primary offerings in an attempt to become more relevant, disrupt current market leaders and write the business locally.



# Emerging needs and evolving products

The increasing awareness of exposure to cyber incidents and the potential impact onto a company's business has driven the demand for larger limit programs and broader coverage terms. 2016 saw dramatic changes in capacity for PII cyber programs. While two years ago, it was generally understood that the largest PII programs were approximately \$300m in total capacity, this increased in 2016 where a number of programs with \$500m in aggregate limit were built for financial institutions and FinTech companies.

Demand for cyber insurance products has also extended beyond data breach cover. While this has been a strong driver of the growth in the US as a result of increased regulation and litigation, there has recently been an increasing demand for products to cover financial losses and property damage resulting from a system failure or cyber incident. In Europe and in other parts of the world, where strict data regulations have yet to be enforced, cover for cyber liability, cyber extortion and business interruption account for most of the demand.

A closer look at recent cyber events clearly illustrates the range of losses that could be triggered as a result of a cyber incident. Companies operating critical infrastructures through complex industrial control systems run by software are increasingly vulnerable to malicious cyber-attacks. The energy, utilities and manufacturing sectors have grown increasingly worried about the impact a cyber event could have on their activity. This has been a prevalent trend in the energy industry where insurance policies have traditionally had cyber exclusion clauses.

Until recently, cyber insurance products covering business interruption losses and physical damage were only offered by a few insurers. They were mainly provided as "difference in

condition" products to fill in the gaps in cover offered by more traditional insurance policies. However, the emerging demand for first party business interruption and physical damage cyber covers caught the attention of a few market participants.

In 2014, Brit launched a new cyber product designed specifically to provide cyber insurance cover for large industrial companies. It includes all features of the oil and gas sector (from upstream to downstream activities), the utilities sectors and other heavy industry sectors. The launch of the product was supported by a consortium of syndicates led by Brit that could offer cover for first party losses up to \$250m.

In April 2016, Beazley and Munich Re partnered to offer an enterprise-wide cyber product, aimed at large corporate and industrial clients. The product provides up to \$100m of protection including data breach, denial of service, extortion, property damage and bodily injury exposure.

In September 2016, Aon announced an all-encompassing product of its own: Aon cyber Enterprise Solution. The "first-of-its-kind" property/casualty/internet of things insurance product offers comprehensive and integrated enterprise-wide coverage against cyber risk. It provides up to \$400m cover for cyber expense reimbursement, security/privacy liability, network business interruption and contingent business interruption, property damage, and product liability. Using an Aon form and supported by several strategic insurer partners, the product is aimed at large companies with first and third party cyber exposures (e.g. manufacturing, IT/technology, utilities) and can be tailored to specific client needs.

**"Until recently, cyber insurance products covering business interruption losses and physical damage were only offered by a few insurers."**

## Examples of cyber incidents

		First party loss recipient				Third party loss recipient	
Non-financial loss	Property damage	<b>Iranian government (2010):</b> The Iranian government's nuclear development programme was disrupted by a computer worm called Stuxnet, the virus caused <b>one fifth of the country's nuclear centrifuges to spin so fast that they tore themselves apart</b> causing severe first party property damage.				<b>Hunter Water (c.2000):</b> A disgruntled employee who had prior knowledge of the Supervisory Control and Data Acquisition (SCADA) system of a water services company hacked into the system and released <b>264,000 litres of raw sewage</b> at a variety of locations over the course of 3 months. The attack led to severe damage of the local environment including the loss of marine life.	
	Bodily injury	(covered by Workers' Compensation policies)				<b>Lodz City Tram System (2010):</b> The first cyber attack to directly cause injuries came after a Polish teenager rewired a television remote to interact with the wireless switch junctions of the trams. By overriding the control of a train it made it jump off the rails and hit another tram, <b>causing minor injuries to several passengers.</b>	
Financial loss	Business interruption	<b>Saudi Aramco (Aug 2012):</b> a state owned oil and gas supplier, Saudi Aramco, was targeted by hackers with the intent to cease the company's crude oil and gas supplies. The hard drives of <b>30,000 desktop computers and 2,000 servers</b> were destroyed, forcing IT systems to be disconnected from the internet for two weeks.				<b>Polish airline LOT (2015):</b> Polish airline LOT suffered a hack on the hardware that issues flight plans at Chopin Airport in Warsaw, grounding over 10 flights and thus affecting the travel plans of thousands of people.  <b>Los Angeles City Hall (2006):</b> was liable to business interruption of third parties after hackers got into the system and caused gridlock at 4 key intersections for several days.	
	Other financial loss	Company	Incident date	Industry	# records breached	Est. cost of incident	Details
		<b>Anthem</b>	<b>Feb 2015</b>	Healthcare	80m	\$100m	Hackers gained unauthorised access to Anthem's IT system and <b>obtained personal information for current and former members</b> (name, date of birth, social security number, street address, employment information including income data).
		<b>JP Morgan Chase</b>	<b>July 2014</b>	Financial Services (Banking)	76m	-	Hackers obtained the highest level of administrative privileges to a number of servers stealing names, addresses, phone numbers and email addresses. JPMorgan has said it plans to spend <b>\$250 million</b> on digital security annually.
		<b>Ebay</b>	<b>Mar 2014</b>	Retail (Online)	145m	\$200m	Hackers obtained login credentials from a small number of employees using them to access all user records and copy a large part of the credentials. Reports suggest that whilst 85% of eBay passwords have been reset the site is yet to return to the previous activity levels seen prior to the hack revelations. The hack has forced the company to <b>lower its annual sales targets by \$200m.</b>
		<b>Target</b>	<b>2014</b>	Retail	40m	\$162m	Malware stored on Target's checkout registers led to the theft of data from <b>40 million credit and debit card accounts</b> along with personal information from <b>70 million customers.</b>
		<b>Zappos</b>	<b>Jan 2012</b>	Retail (Online)	24m	\$500m	Hackers accessed customer names, email and postal address, phone numbers and encrypted passwords.
		<b>Heartland</b>	<b>2008-2009</b>	Financial Services (Payment processor)	136m	\$110m	Stolen data included the digital information encoded onto the <b>magnetic stripe</b> built into the backs of credit and debit cards. Thieves can use that data to <b>counterfeit cards</b> by imprinting the same stolen information onto fabricated cards.
		<b>TJX</b>	<b>2006-2007</b>	Retail	46m	\$90m	Hackers circumvented a store's wifi network and stole customers' debit and credit card data.
		<b>Adobe</b>	<b>Sep 2013</b>	Technology	36m	-	Data breach resulted in <b>credit and debit card information</b> being stolen for <b>3.1m customers, encrypted passwords for 33m customers</b> and the source code for packages incl. <b>Adobe Photoshop.</b>

Sources: ccdcoe.org, New York Times, Marsh, Financial Times, Aon data, Insurance Information Institute, Wall Street Journal, NPR, Bloomberg, Ponemon Institute, Identity Theft Resource Centre

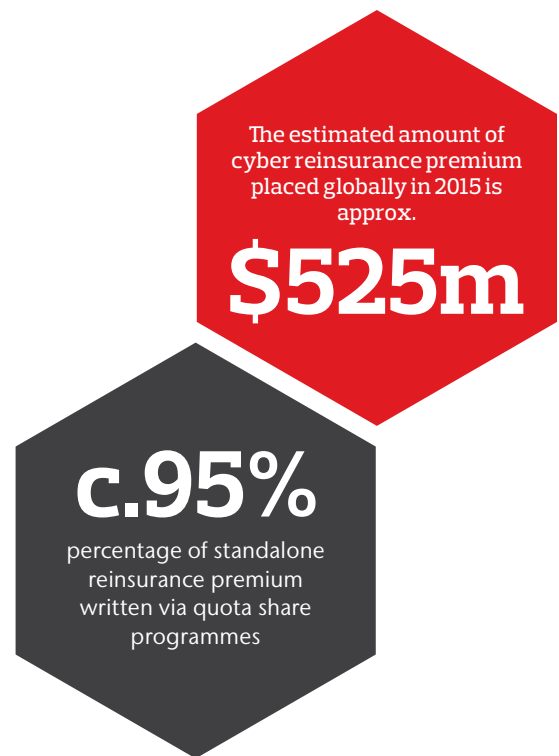
# A nascent reinsurance market

Many cyber insurers have been concerned about potential risk aggregation and the impact a systemic event could have on their portfolio. Although this type of catastrophic event is yet to be witnessed, large distributed denial-of-service attacks (DDoS attacks) such as the Dyn cyber-attack that took place on October 21st, 2016 are a reminder of the potential impact a large organised attack could have on industries that heavily rely on the internet. As a result, insurers have remained cautious about holding too much cyber risk on their balance sheet and have looked for simple reinsurance mechanisms to offload some of the exposure.

A study conducted by Aon Benfield, estimates the 2015 global reinsurance market to be worth c. \$525m in annual premium with approximately 95% written on a quota share basis. The reinsurance market is in its early stages. Prior to 2015, a large amount of risks was still believed to be packaged and placed in traditional financial lines and casualty treaties with only a few standalone cyber treaties placed in the market. Worries about potential silent cyber aggregates under traditional policies (i.e. addition of cyber endorsement, inclusion of cyber trigger..), allowed by lenient underwriting guidelines forced cedents to ask reinsurers to remove cyber exclusions from existing treaties. This approach had various level of success as it was perceived by reinsurers as a means to transfer the problem of silent aggregate from the insurance to the reinsurance market. However, as the insurance market develops a better understanding of the risk and moves towards standalone products, insurers will try to ring-fence their cyber portfolio to better manage their exposure, allowing the creation of separate cyber treaties. This is already happening. However, the reinsurance market faces two main challenges: the current lack of suitable data and modelling capabilities to evaluate exposure aggregate and the lack of underwriting talent with the expertise required to develop and make the market.

More than 15 reinsurers actively write standalone cyber treaties and the number is increasing. Some of them have been supporting the cyber reinsurance market for over a decade. They have built their book over time and are able to offer 20-30% line participation on quota share treaties. However, they remain conservative about their overall exposure to cyber risks and often require loss occurrence caps for business interruption on quota share treaties. More recent entrants have showed a clear appetite to quote business but are unwilling to take large lines and typically limit their participation below 20%.

While most ceded cyber premiums relate to US domiciled risks, a significant portion is reinsured outside of the US. A large amount of that premium flows to the London wholesale market and a few reinsurers also write cyber business from their Bermudan operations.



# Opportunities beyond risk transfer solutions

When looking at cyber, one also needs to look beyond the insurance and reinsurance market to obtain a complete picture of the fast growing cyber industry.

A recent study from Gartner estimates that worldwide information security spending increased by 7.9% to reach \$81.6bn in 2016, a significant increase compared to the 4.7% additional spending observed in 2015. This strong growth is primarily driven by the need for companies to access external services to improve their security position in the digital business era. The surge in the demand was answered by a booming industry sector, with investment in companies and start-up providing such security services growing at c.20% per year as reflected in some cyber indexes (ISE Cyber Security® Index).

Today, companies have access to a wide range of information security

services that can be grouped in two main categories: risk mitigation solutions and incident response services.

Risk mitigation solutions are aimed at obtaining a better understanding of a company's exposure to potential cyber threats in order to identify and deploy appropriate solutions to mitigate them. They include assessment of cyber risks, advisory services, security software, hardware solutions, training of personnel and compliance facilities. A company typically accesses these services to evaluate the security of its network, the quality of its IT governance and quantify the impact a cyber event could have on its business. Equipped with a better understanding of its exposure to cyber threats, a company can then evaluate if risk transfer solutions are needed for them to be comfortable with retention levels.

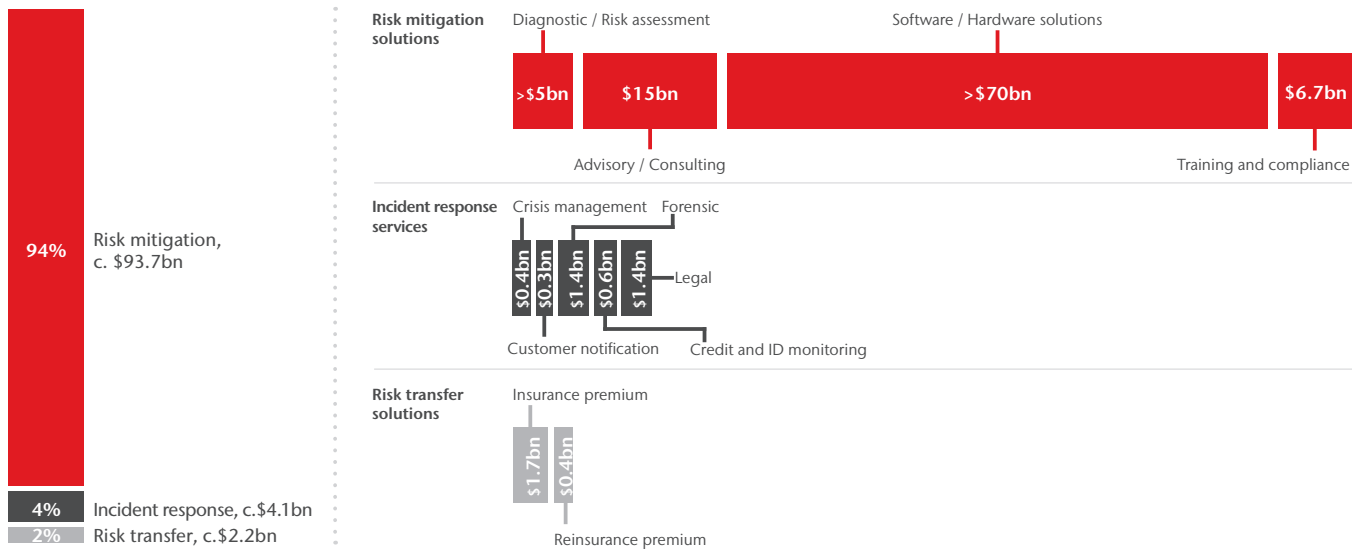
<b>Diagnostic and risk assessment</b>	Assess an enterprise's cyber security, identify potential risks and measure its exposure to cyber threats and impact on companies activity.
<b>Advisory and consulting</b>	Provide recommendations on how to improve network security, mitigate risks and advise on potential risk transfer solutions.
<b>Software and hardware solutions</b>	Deliver preventive hardware and software solutions and act as another barrier to prevent cyber incidents and potential external attacks.
<b>Training and compliance</b>	Offers training on how to comply with data regulations (e.g. HIPAA) and how to mitigate cyber incidents, often provided via online platforms.

Incident response services are intended to support companies that have experienced a cyber incident, including extortion, denial of access, system failure, hacking, and data breach. They comprise crisis management services, including access to a breach coach, forensic support to identify and remediate the cause of the event, customer notification services, credit and ID monitoring and legal support. The main objective of these services is to minimize the potential loss arising from a cyber incident by rapidly coordinating and managing the various aspects of the response from communication and notification of the event to forensic and legal support.

<b>Crisis management</b>	Provide support on how to deal with a breach and mitigate the impact, including coaching, coordination of services and public relationship
<b>Forensic</b>	Identify the cause of the incident and advise on solution to contain the loss and remediate the problem to return to normal operating conditions
<b>Customer notification</b>	Notify customers of security breaches and loss of personal data to comply with notification procedures dictated by local regulation
<b>Credit and ID monitoring</b>	Offer credit and monitoring services to detect fraudulent activities after customer details and payment card data have been compromised
<b>Legal</b>	Provide the company victim of a data incident with legal advice on how to respond to a breach and defend itself in case of a lawsuit

In a study, Aon Inpoint estimated the 2015 global revenue generated across all segments of the cyber service range (i.e. from risk mitigation to risk transfer and post-incident solutions) to be in excess of \$100bn. Most of it is accounted for by companies offering risk mitigation services, with those providing software or hardware security solutions representing over 70% of the global revenue. The insurance and reinsurance markets were estimated to account for a mere 2%.

## 2015 breakdown of total cyber security market (c.\$100bn) by segment



Sources: Company websites, Insurer websites, Broker websites, RIMS 2016, Aon Cyber Committee research, Cybersecurity Ventures, Owlser, Ranker, Hoover, Bessemer Venture Partners, Gartner, Verizon, MicroMarketMonitor, Aon Inpoint analysis

Risk mitigations and post incident services are particularly valued by small and medium sized companies which do not have the scale to develop in-house capabilities. While large and global companies sometime refer to external vendors for additional support in specific situations, they tend to develop and use their internal IT, PR and legal capabilities to mitigate their risks and respond to a breach.

As part of their cyber products, insurers have tried to offer or provide access to some of those services and have established partnerships with selected vendors. Some like AIG offer access to a long list of partners and vendors from breach and privacy counsel to forensic, notification and post-breach and public relations. Others like Beazley have opted for a reduced list of selected partners and formed breach response teams to coordinate those services as an integral part of their cyber offering. However, beyond the key players, other insurers have also focused their offering on the response services as a means to contain the losses resulting from a breach. Most of them do not provide clients with support in assessing their network security and reducing their exposure to potential attacks.

In 2016, Aon Inpoint reviewed over 600 of the most active companies in the cyber security space. Excluding

legal services, few are able to offer the full range of loss prevention and incident response services. Many of them only focus on one or two elements of the risk mitigation services and some aspects of data breach support.

The study highlighted the difficulty for companies to find a 'one stop shop' that could help them access the full range of services and risk transfer solutions. The gap has been identified by a number of players in the insurance market as an opportunity to differentiate and strengthen their cyber offering.

In October 2016, Aon announced the acquisition of Stroz Friedberg, a global leader in cyber security to create a comprehensive cyber risk management advisory group. With this, Aon will aim to provide companies with broader solutions, bringing together Aon's expertise in risk assessment and transfer solutions and Stroz Friedberg's cutting-edge cyber security governance, advisory services and incident response. Other brokers and cyber industry solutions providers are also entering into various joint ventures and other partnerships that add elements of cyber solutions.

## Global loss prevention and incident resolution sample service offerings

Provider categories	Sample count	Risk mitigation solution offering				% of sample offering incident response services				
		Diagnostic / Risk assessment	Advisory / Consultation	Software / Hardware solutions	Training and compliance	Crisis management	Customer notification	Forensic experts	Credit and ID monitoring	Legal experts
Full loss prevention offering	8	✓	✓	✓	✓	50%	13%	25%	13%	
	11	✓	✓		✓	9%		27%		
Extensive loss prevention offering	14	✓	✓	✓		36%		21%		
	45	✓		✓	✓	2%		7%		
	13		✓	✓	✓	8%				
Dual loss prevention offering	13	✓	✓			36%			9%	
	89	✓		✓		6%	1%	3%	1%	
	14	✓			✓			14%		
	10		✓	✓		40%		10%		
	5		✓		✓					
	43			✓	✓					
Specialist loss prevention offering	21	✓				17%		9%		
	23		✓			17%	9%	48%		
	228			✓		2%		3%	1%	
	5				✓					20%
Incident resolution focused	70					26%	14%	14%	7%	51%
<b>Grand total</b>	<b>612</b>	<b>215</b> (35%)	<b>95</b> (16%)	<b>450</b> (74%)	<b>144</b> (24%)	<b>56</b> (9%)	<b>15</b> (2%)	<b>47</b> (8%)	<b>11</b> (2%)	<b>37</b> (6%)

Sources: Insurer websites, Company websites, ARS Cyber Committee, RIMS 2016, Broker websites, Cyber Security Ventures, Bessemer Venture Partners, Gartner, Ranker.com, Aon Inpoint analysis

## Conclusion

The world is continuing its digital transformation with no sign of slowing down. The amount of data consumed by businesses increases every day. Companies are also ever more reliant on inter-connectivity of systems and technologies to operate. At the same time, hackers have become more sophisticated at exploiting networks and software vulnerabilities to achieve their goals and the number of reported cyber-attacks keeps increasing. In addition, the continually evolving technology environment has made it more challenging for companies to keep up with the latest security solutions, leaving them more exposed to potential threats. In this context, the insurance industry will play an important role in helping companies manage their exposure to potential cyber perils.

There are plenty of opportunities for insurers and reinsurers whether in existing or upcoming markets. As the digital and technology environment evolves, new risks will emerge and opportunities will appear as the demand for products and services develops.

Insurers that are trying to grow in this segment are actively developing their strategies. Many are investing in new capabilities, establishing partnerships with cyber security firms and hiring experts outside the industry to build a competitive edge. However, in this fast growing and changing market, those that stand still for too long are in danger of missing out on the opportunity. A clear strategy and early positioning will be essential to succeed in this environment. Late entrants will struggle to compete with established players and bridging the gap will be challenging.

Aon Inpoint has already helped several insurers with their cyber ambitions, ranging from market entry support and value proposition enhancement to assisting established players identify the next opportunities.

# Contacts

**Michael R. Moran**

Chief Executive Officer  
Aon Inpoint  
The Aon Center,  
200 East Randolph Street,  
Chicago, IL 60601, USA  
+1.312.381.3962  
michael.r.moran@aon.com

**Sherif Zakhary**

Global Head of Sales  
Aon Inpoint  
44 Whippany Road,  
Suite 220, Morristown,  
NJ 07960, USA  
+1.347.334.2216  
sherif.zakhary@aon.com

**Marguerite Soeteman-Reijnen**

Chief Marketing Officer  
Aon Inpoint  
Admiraliteitskade 62,  
Rotterdam, Netherlands  
+31.10.448.7756  
marguerite.soeteman.  
reijnen@aon.nl

**Paul Galvin**

Global Leader, Carrier Solutions  
Aon Inpoint  
The Aon Centre,  
The Leadenhall Building,  
122 Leadenhall Street,  
EC3V 4AN, London, UK  
+44.20.7086.0055  
paul.galvin@aon.co.uk

**Robert Woods**

Group Managing Director  
EMEA  
Aon Inpoint  
The Aon Centre,  
The Leadenhall Building,  
122 Leadenhall Street,  
EC3V 4AN, London, UK  
+44.20.7086.3344  
robert.woods@aon.co.uk

**Antony Ainsworth**

Group Managing Director  
Americas  
Aon Inpoint  
199 Water Street, New York,  
NY 10038, USA  
+1.212.441.1266  
antony.ainsworth@aon.com

**Giselle Walther**

Group Managing Director  
APAC  
Aon Inpoint  
80 Collins Street, Melbourne,  
VIC 3000, Australia  
+61.3.9211.3143  
giselle.walther@aon.com

**Jeremy Maginot**

Director, Consulting  
Aon Inpoint  
The Aon Centre,  
The Leadenhall Building,  
122 Leadenhall Street,  
EC3V 4AN, London, UK  
+44.20.7086.4502  
jeremy.maginot@aon.com

**Kevin Kalinich**

Global Practice Leader, Global  
Cyber Insurance Solutions  
Aon Risk Solutions  
The Aon Center,  
200 E Randolph Street, 8 E 03B,  
Chicago, IL 60601, USA  
+1.312.381.4203  
kevin.kalinich@aon.com

**Luke Foord-Kelcey**

Co-head, Global Cyber Practice  
Aon Benfield  
The Aon Centre,  
The Leadenhall Building,  
122 Leadenhall Street,  
EC3V 4AN, London, UK  
+44.20.7086.2067  
luke.foord-kelcey@aonbenfield.com

## About Aon Inpoint

---

### *Driving Value and Innovation for Insurers and Reinsurers*

Aon Inpoint is dedicated to delivering value, insights and innovation through data, analytics, engagement and consulting services to (re)insurers, across the full spectrum of insurance, reinsurance, and capital markets.

Aon Inpoint's focus is to always act in the best interests of Aon's insured and cedent clients by enabling (re)insurers to compete more effectively so that Aon can provide valuable solutions and greater choice to our mutual clients.

Consistent with confidentiality and data compliance protocols, Aon Inpoint provides (re)insurers with access to Aon's industry leading data analytics platforms, including Aon GRIP® and Re/View, combined with our consulting capabilities, enable (re)insurers to develop growth strategies, as well as to identify and execute business improvement and growth opportunities in new markets and product lines.

## About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

© Aon Inpoint (Aon) 2017. All rights reserved.

Written and published by Aon. This work is copyright and confidential. Other than as permitted by law, no part of it may in any form or by any means be reproduced, stored or transmitted without permission of the copyright owner, Aon.

### Disclaimer

Aon has taken care in the production of this document and the information contained in it has been obtained from sources that Aon reasonably believes to be reliable. Aon however does not make any representation as to the accuracy of any information received by third parties and is unable to accept any liability for any loss incurred by anyone who relies on the contents of this document. The recipient of this document is responsible for their use of it. Please feel free to contact us if you would like any further information.