Aon Risk Solutions
Aon Centre for Innovation and Analytics

Exploring the Latest Cyber Risk Trends in EMEA

Aon Cyber Risk Diagnostic Tool, September 2014

Table of Contents

Introduction

No industry sectors are entirely immune from a cyber-attack. The digital interconnectivity of business operations, suppliers and customers means that any organisation is vulnerable to potentially catastrophic electronic data theft or sabotage. This inter-reliance between organisations, and the growing prevalence of cloud computing, social media, corporate 'bring your own device' policies, big data and state-sponsored espionage have catapulted cyber risk into one of the top concerns of business leaders today.

It is possible companies may not have the correct focus when it comes to tackling this emerging threat. They may be focused exclusively on protection, on encryption and firewalls for example, when they should be considering potential responses for when the systems are breached. An example of this type of behaviour could be the danger in relying solely on IT Departments to set the strategy for management on Cyber Risks. It is becoming increasingly apparent that guidance on these matters must come from the top down, and management must involve multiple stakeholders.

Aon's goal is to help clients succeed in and understand emerging risks, requirements and insurance implications, and to use risk understanding to drive better business decisions. It is our hope that this report helps you in Cyber risk identification and management.

As the leading global provider of risk management services, insurance and reinsurance brokerage, and human capital consulting, Aon is proud to provide our clients with the most innovative solutions and the most informative risk insights and data available. Aon's unmatched global network and extensive client base allows us to develop the industry's most comprehensive data, reports and analysis. At Aon we can benchmark your cyber exposures and help you build a cyber-risk management and mitigation plan giving you clarity and cover for your business.

By analysing the data gathered from Aon's Cyber Diagnostic Tool, this report highlights industries and scenarios which are particularly vulnerable to a loss of a large magnitude due to a cyber risk event across EMEA. In an effort to demonstrate how cyber risk can affect a myriad of industries, Aon's data combines the responses of companies in a large range of industries, everything from manufacturing to utilities.

We will also examine the importance of achieving Cyber Clarity for your business and outline some examples of how this can be done, highlighting the benefits of quantification.

Best regards,

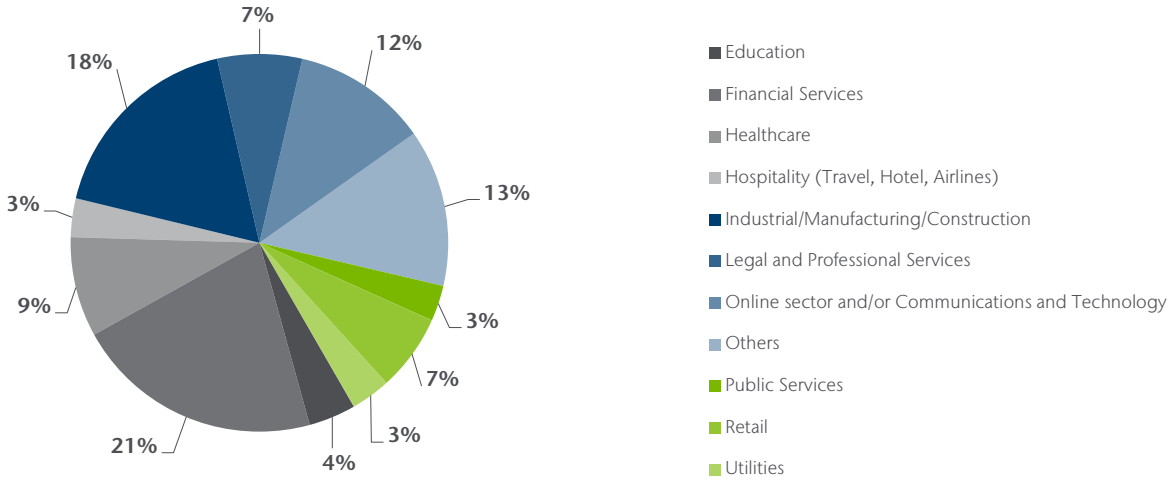
Adam Peckman
Senior Risk Management Consultant - Cyber
Aon Risk Solutions
adam.peckman@aon.co.uk

Constantin Beier
CEO
Aon Centre for Innovation & Analytics
Aon Risk Solutions
constantin.beier@aon.ie

The Aon Cyber Diagnostic Tool

The Aon Cyber Diagnostic Tool aims to help risk managers better identify and understand their exposure to cyber risk. The tool uses a series of multiple choice questions to assess how employees use technology, the current controls in place and management's attitude to cyber risk. The tool then provides meaningful insight into the most important cyber risk topics and includes practical guidance on related governance frameworks that should be in place, as part of an effective cyber risk management strategy.

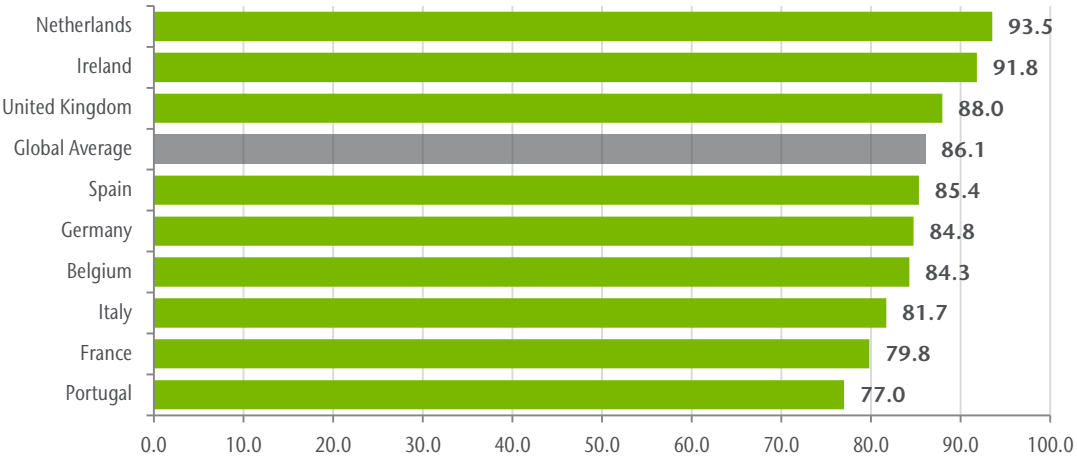
Respondents by industry



Data Source: Aon Cyber Diagnostic Tool 2014

Total risk score by country

Based on the overall responses to questions regarding the key internal and external factors that affect cyber risks, EMEA based companies report a high level of overall risk consistent with the Global average. As noted below, countries such as the Netherlands, Ireland, and the United Kingdom score particularly highly.

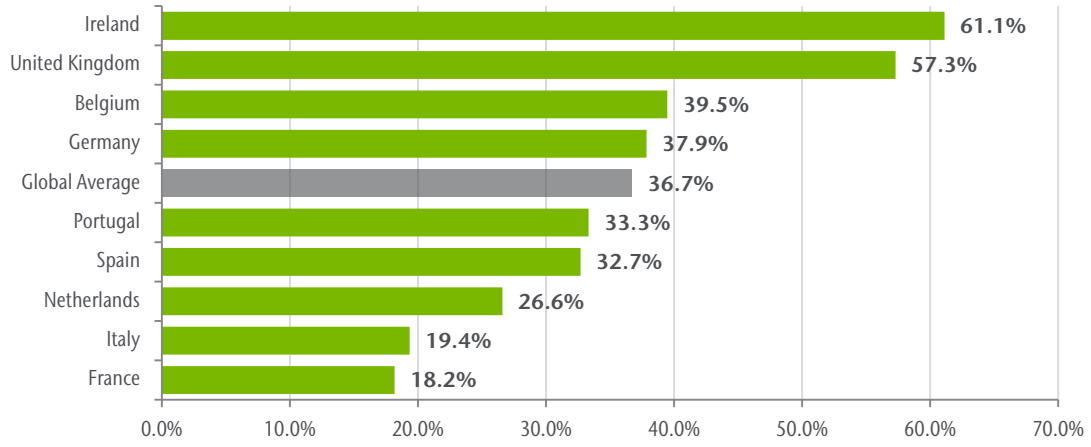


Data Source: Aon Cyber Diagnostic Tool 2014

There are numerous underlying factors which relate to this score.

EMEA – Varied Levels of Technical Protection

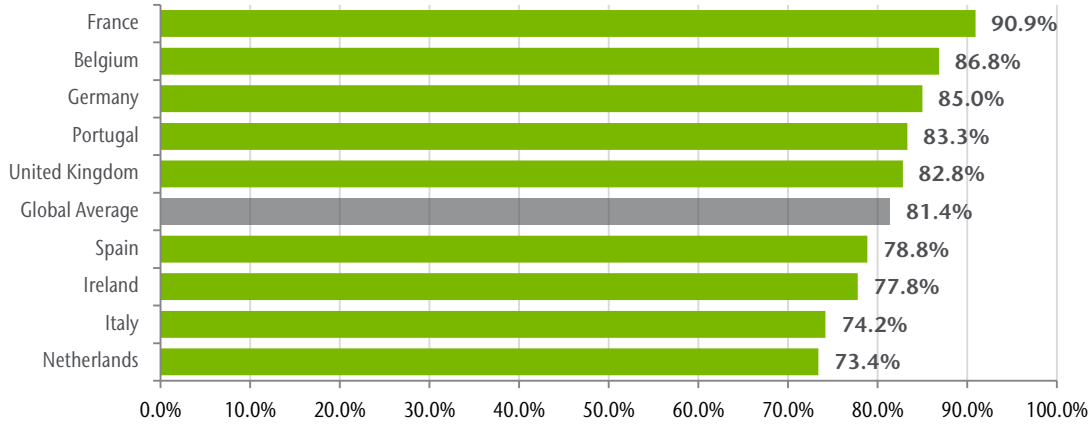
Is there consistent encryption of sensitive/critical data stored on your company laptops?



Data Source: Aon Cyber Diagnostic Tool 2014

The encryption of a company's mobile media is a fundamental step in creating an information security system. We found that certain countries across EMEA have consistent encryption of sensitive/critical data stored on company laptops. Four countries across EMEA score above the global average, demonstrating an awareness of the importance of encryption. However, even within the highest rated country, almost **four in ten** companies are not adequately protecting the digital information they hold.

Is there a formal process to manage and configure the critical application systems as well as the company's firewall, antivirus/antimalware software?



Data Source: Aon Cyber Diagnostic Tool 2014

Traditionally, anti-virus protection has been one of the primary tools used to minimize the likelihood of breach networks and devices from malicious attacks. Respondents were asked whether their organization has a formal process in place to closely monitor the usage of antivirus/antimalware software. The survey found that across a number of the EMEA countries standards are relatively high. However, some countries clearly view the matter as more serious than others. For instance, Ireland sits below the Global Average on this matter.

Increased Risk Factors

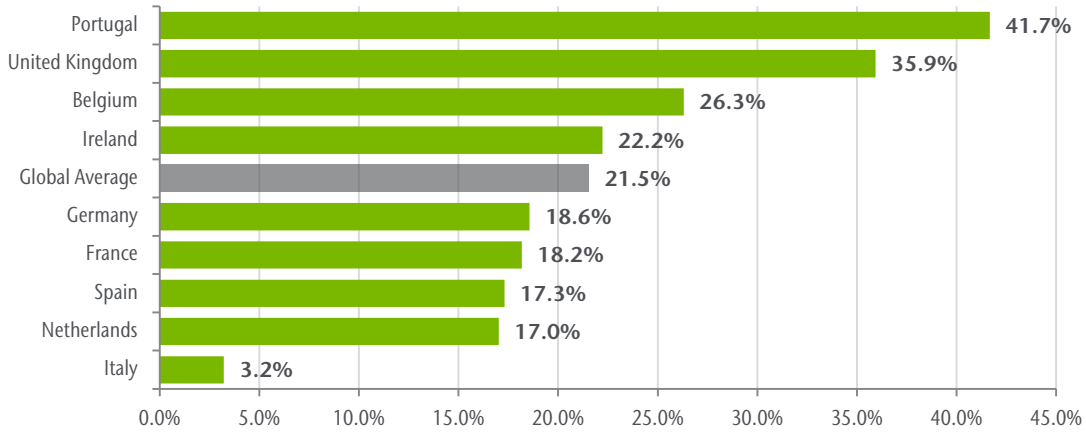
Boardroom Attitude Towards Cyber Risk

Recent data breaches at major corporations highlight the increasing sophistication and persistence of cyber-attacks. The challenge of protecting information systems and key data assets such as financial and personal information – and the financial, reputational and regulatory damage that arise when firms fail to do so – have led boards to increase their level of oversight of cyber security.

In order to make privacy and security key parts of any data management programme, a coordinated effort is required by a diverse range of stakeholders within an organisation. Increasing the level of boardroom focus on cyber risk helps define the culture of data protection within the organisation.

To assess whether boards are actively addressing cyber risk management, respondents were asked about the level of oversight related to cyber risk in terms of regular updates and reports.

Regular board updates, security updates and enterprise risk management stakeholder meetings, with constant monitoring of aggregate risk and elevated risk levels



Data Source: Aon Cyber Diagnostic Tool 2014

The chart above shows that there is a relatively low level of Board involvement across EMEA. Not surprisingly, this is also reflected in the Global Average. There will be increasing pressure on an organisation's Board to familiarise themselves with the company mechanisms associated with cyber risk and security. Recent high profile cyber-attacks and subsequent losses have left the positions of high profile executives untenable. An understanding of the severity of the threat has become an absolute requirement, imperative to the future of the business in many cases.

Blurring the Digital Perimeters

Use of Third Parties

Do any of your business partners hold personal data on your behalf (eg. payroll processing company, outsourcing administration), or provide IT services?

Data Source: Aon Cyber Diagnostic Tool 2014

In recent decades, the use of third party technology has transformed the way in which companies interact with their customers and business partners. In order to facilitate day-to-day activities, processes and systems have been developed to help minimize transaction costs and increase levels of customer service. However, entrusting your data to a third party does not relieve you of your duty of care with respect to protecting the security of that information which is something which companies need to be aware of.

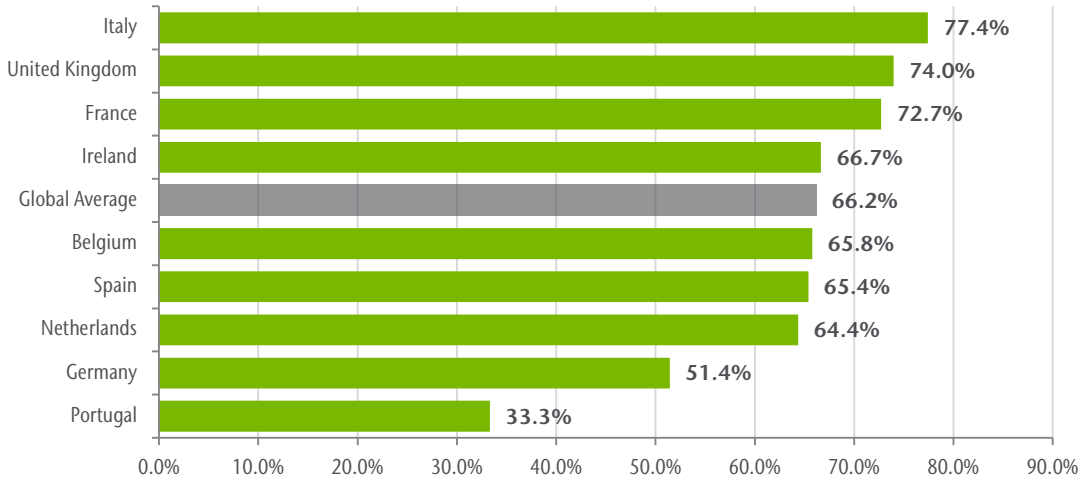
The Aon Cyber Diagnostic survey shows that Irish companies have the highest level of usage of Third Party data services within the sample of European countries. The Global Average figure shows that over 60% of companies entrust their data to business partners. While the benefits of sharing such information may help improve their products and services through increased efficiency, this increased data footprint may represent a higher level of risk with an increased dependence on a technological infrastructure which may not be fully within their control.

"Bring Your Own Device" (BYOD)

A recent key trend in the corporate world has been employee use of personal devices, such as tablets, phones and laptops, to conduct company business. This, while having practical benefits, opens a company up to new exposures.

Savings on cost and time are the two frequently cited benefits, but organisations must examine if the risks associated with such a business practise outweigh the benefits. Without ownership of all the devices and systems used for business, the company could find it increasingly difficult to safeguard from potential threats. The survey showed that two-thirds of Irish companies allow their employees to use their own devices to access privileged company information and applications.

BYOD in your company

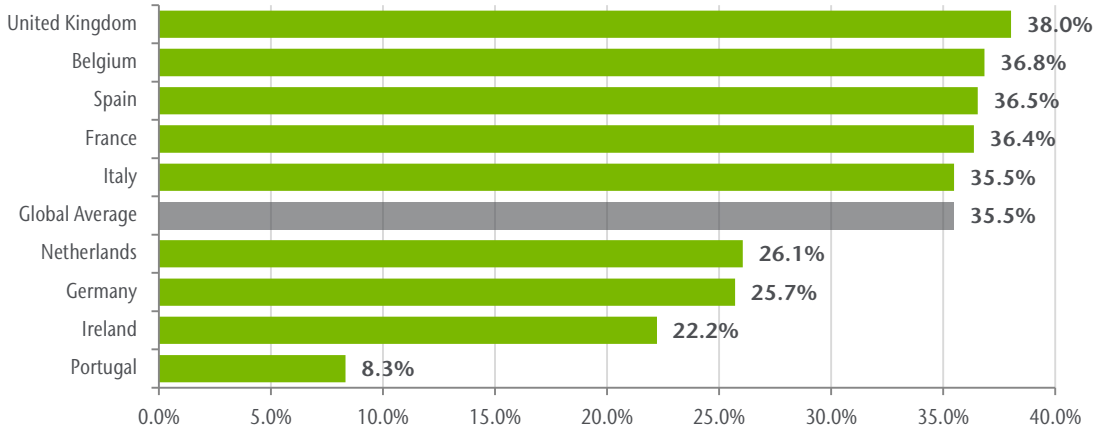


Data Source: Aon Cyber Diagnostic Tool 2014

Data Breach in the Past 12 Months

The results have found that in some EMEA countries a large percentage of companies had a data breach or a serious technical outage in the past 12 months. Countries such as the United Kingdom, Belgium, Spain, France, and Italy have the largest number of breaches or technical issues, while the global average indicates that one in three companies report suffering from some type of incident during the period.

Have you been subjected to any data breaches or significant system failures (whether due to malicious activity or not) in the last 12 months?

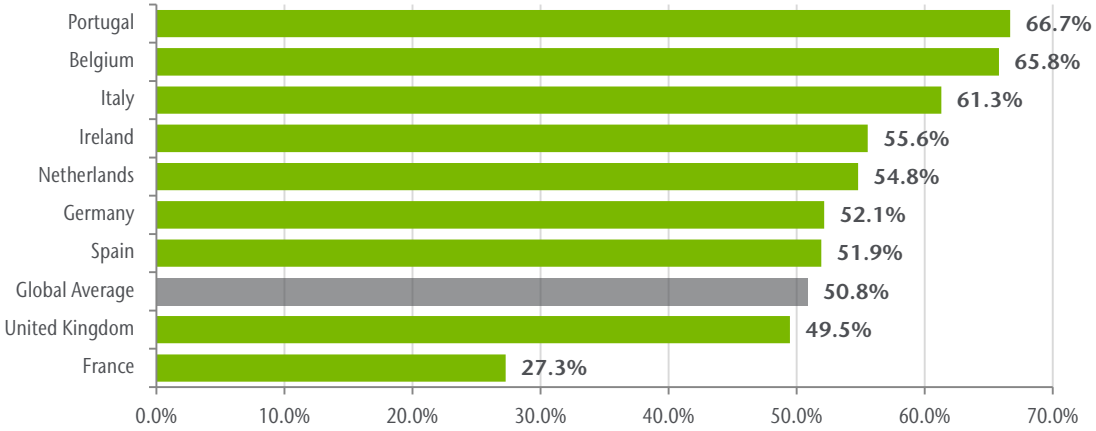


Data Source: Aon Cyber Diagnostic Tool 2014

Dealing with Loss of Systems

If systems or data are damaged or lost, it is highly likely that the functionality of the company will be restricted, if not stopped. Respondents in almost all countries believed there would there be a significant impact on their business should they lose access to critical applications and systems even for a few hours. This table highlights the importance companies now place on IT and the potential impact to business continuity that a cyber threat could cause.

How long do you believe your critical applications and systems can be shut down before significant damage is caused to your company? - Less than 6 hours



Data Source: Aon Cyber Diagnostic Tool 2014

In the next section we will demonstrate the importance of achieving Cyber Clarity in your organisation.

Aon's Cyber Clarity Process

It is of great importance for a company to understand the exposures it faces. Gaining cyber exposure clarity is now business critical. There are a number of different methods used to achieve this involving scenario testing, assessment of potential financial impact on a company, assessment or the risk maturity level of your cyber risk management procedures and also the insurability of your cyber risk.

Below we outline three important steps for each company to take when attempting to understand their exposures when it comes to cyber insurance.

Gaining Cyber Exposure Clarity

The entity will be required to qualify and prioritise certain cyber scenarios and develop a method whereby it can quantify the consequences of any exposures. This in turn should then allow the company to provide a high-level estimation of holes in coverage or losses which will give a subsequent quantitative assessment of business interruption from cyber.

Cyber Risk Management Assessment

A key aspect of protecting a company against risks is of course being sufficiently able to mitigate the risks where possible. Each company should assess their cyber risk management capabilities (firewalls, system operational procedures) and ideally benchmark these standards against ISO 27000, aspiring to be as efficient as possible.

Cyber Insurance Risk Review

Following the identification of potential threat scenarios the company should then analyse the insurability and transferability of these risks through a series of analytical processes. These will look at any potential policy response or coverage.

The above steps will allow the company to understand if current policies in action will cover any potential cyber loss. The company should use the results of this output to adjust the scope and limit of current insurance policies and to make a data-driven decision about purchasing a cyber insurance policy.

Through this method Aon has identified five main benefits of a company quantifying their cyber risks.

1. **Quantification defines the exposure and any potential impact**
   Developing an understanding of the effect of an incident instead of purely examining the cause which is often the case with most organisations.

2. **Quantification uncovers the relative severity of various cyber risks against financial objectives**
   All too often the implications of intangible asset damage are overlooked which can lead to a loss of intellectual property, negating years of research and development.

3. **Quantification focuses investment in mitigation (IT & processes)**
   Well-defined exposures can help steer IT investment to where it is needed proving beneficial to the entire organisation through the mitigation of potential risk.

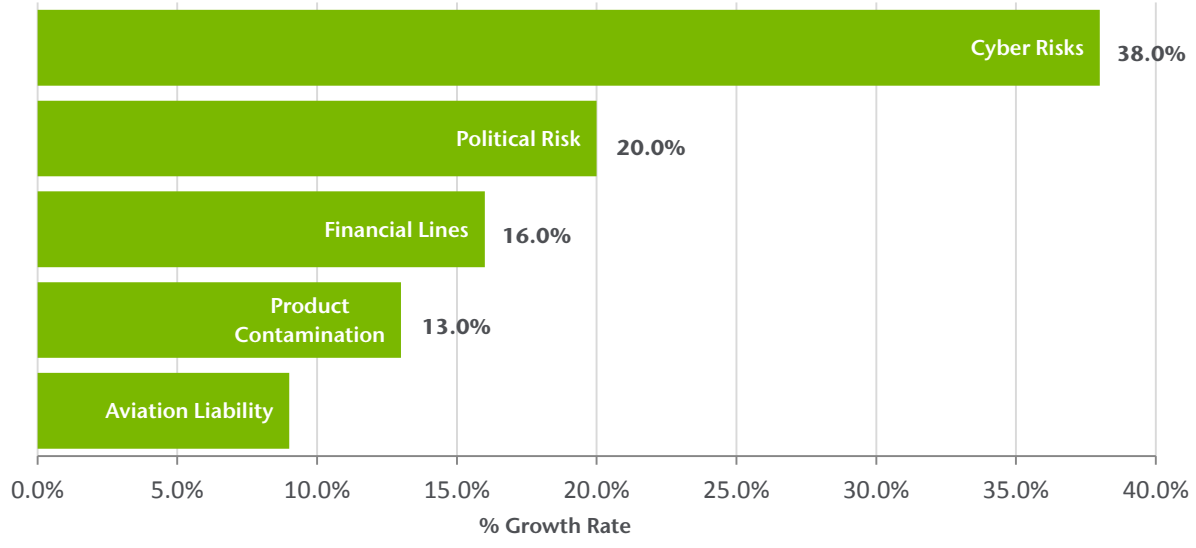
4. **Quantification is a catalyst to increase awareness in the organisation**
   Putting a value on an exposure organically increases interest and further can make it easier to communicate the importance of the exposure to the organisation.

5. **Quantification enables an informed discussion about the transfer of risk**
   Boiling down to the basics of insurance, the transfer of risk is fundamental to how organisations do business. Understanding this exposure will determine whether the company is paying the correct level of premium or transferring the correct level of risk.

Aon's Cyber Insurance Solution

In recent years, Boards of Directors and C-Suite Officers are becoming increasingly aware of the seriousness and complexity of cyber risk leading to a substantial increase in the adoption of Cyber Risk cover. The chart below shows that Cyber Risks cover has grown at a compound growth rate of 38% annually between 2009 and 2014 which made it Aon's fastest growing product during the period.

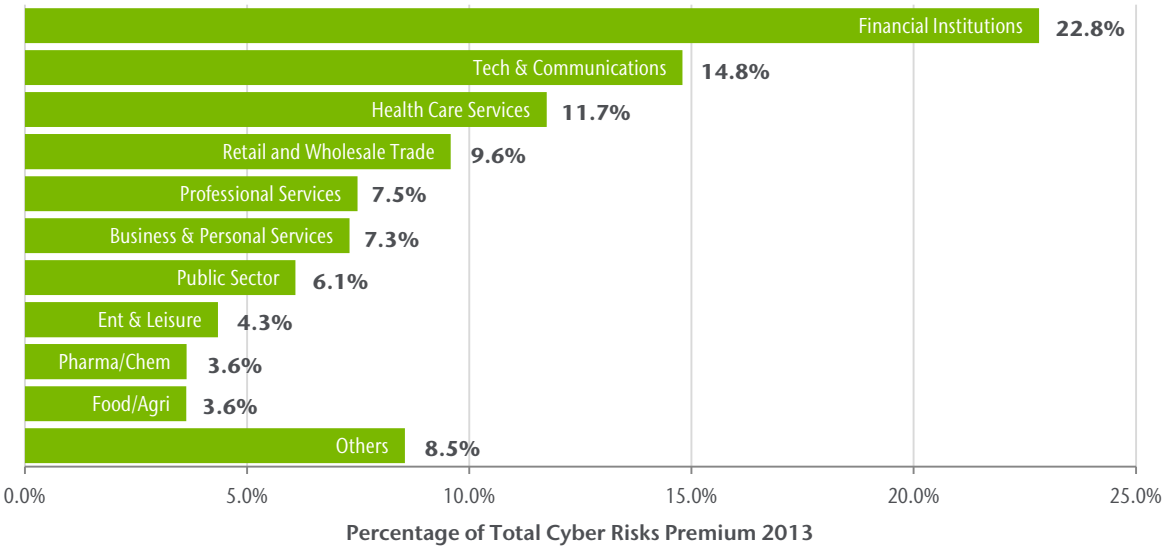
Total premium - compound growth rate 2009-2013



Data Source: Aon Global Risk Insight Platform (GRIP)

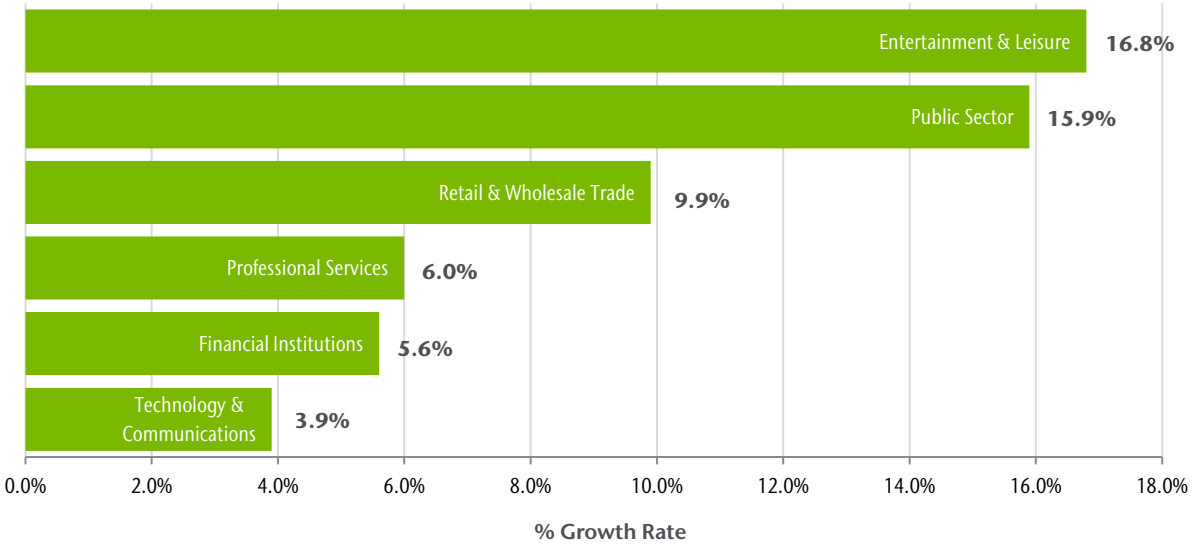
Companies that are most likely to purchase Cyber Risks cover are those in industries such as Financial Institutions, Technology & Communications, Health Care and Retail & Wholesale Trade. Each of these sectors stores large amounts of information about their customers and has a high degree of dependency on technology to manage this information and any cyber incident is more likely to have a material impact due to the very personal nature of the records being stored. The below graph ranks industry sectors by their share or the total cyber insurance premium placed by Aon in 2013 globally.

Cyber risks premium by industry



Data Source: Aon Global Risk Insight Platform (GRIP)

Average Limit Purchased - Compound Annual Growth Rate 2009-2013



Data Source: Aon Global Risk Insight Platform (GRIP)

The amount of limits purchased by companies also increased in the 2009 to 2013 period with average limits increasing across Entertainment & Leisure, the Public Sector and Retail & Wholesale Trade. Limits also increased across Financial Institutions and Technology & Communications as companies have become aware of the increasing need to protect their critical technology infrastructure.

Benchmarking Your Cyber Risk Exposures

Build a framework for discussion with Aon's Cyber Risk Diagnostic Tool, which will provide a high-level understanding of the risks facing your organisation. Upon answering a series of multiple choice questions, you will receive a tailored cyber insight report that will help identify the key internal and external factors that may affect your levels of cyber risks. The report also includes practical guidance on the related governance framework that should be in place as part of an effective cyber risk management strategy.

The tool is available in seven languages and in the coming year we expect to be able to provide more detailed and targeted cyber risk insights to our clients than ever before. Aon clients can receive customised benchmarking of their cyber risk report against peer companies, tailored by industry, geography, or specific risk factor.

Both the tool and the report can be used to engage other company stakeholders into the process, such as chief information officers, IT security, data privacy leaders, legal, HR and finance. To receive your complimentary report, complete the diagnostic at **aoncyberdiagnostic.com** or for further information please contact your local Aon office.

Key Contacts

Adam Peckman
Senior Risk Management Consultant - Cyber
Aon Risk Solutions
adam.peckman@aon.co.uk

Constantin Beier
CEO
Aon Centre for Innovation & Analytics
Aon Risk Solutions
constantin.beier@aon.ie

Michael Spellman
Director
Aon Global Risk Consulting
Aon Risk Solutions
michael.spellman@aon.ie

About Aon

Aon plc (NYSE:AON) is the leading global provider of risk management, insurance and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 66,000 colleagues worldwide, Aon unites to empower results for clients in over 120 countries via innovative and effective risk and people solutions and through industry-leading global resources and technical expertise. Aon has been named repeatedly as the world's best broker, best insurance intermediary, best reinsurance intermediary, best captives manager, and best employee benefits consulting firm by multiple industry sources. Visit aon.com for more information on Aon and aon.com/manchesterunited to learn about Aon's global partnership with Manchester United.

aon.com