Published: June 2015

2015 EMEA Cyber Impact Report

The increasing cyber threat – what is the true cost to business?

Research independently conducted by Ponemon Institute LLC and commissioned by Aon Risk Solutions

AON | Ponemon INSTITUTE

Table of Contents

Aon Foreword 3

Ponemon Institute Cyber Impact Research 4

Tangible versus intangible assets – a story of unequal risk 4

Data and security breaches – more common than you think 5

Management versus mitigation – the role and take-up of insurance 6

An industry challenge – limited experience with an evolving risk 7

Methodology 8

Aon Conclusion 10

Aon Foreword

In an era of global connectivity, online information and systems are playing an increasingly central role in business. According to data from Cisco, worldwide internet-connected devices will reach 50 billion by 2020, and with 15 billion devices already in 2015 it is apparent that an increasing numbers of companies, systems and information are working online.

As the tech revolution gathers pace however, so too do the associated risks. In 2014 Sony Pictures suffered a high profile and damaging hack, and early in 2015 the co-ordinated Carbanak attack on banks worldwide was estimated to have totalled up to US$1 billion in stolen funds. Further evidence of the growth in cyber risk is the +50% Compound Annual Growth Rate (CAGR) of Aon cyber insurance cover in the five years to 2014.

The financial consequences of a cyber breach can be wide-ranging, including business interruption, forensic IT costs, supply chain disruption and intellectual property theft. Attacks have the potential to affect virtually every industry, from manufacturing, through to retail, life sciences, and healthcare - the issue is not confined to financial institutions or global brand management companies.

It is against this backdrop that, in March 2015, Aon commissioned the Ponemon Institute, a leading research firm on privacy, data protection and information security, to conduct a groundbreaking global cyber risk study (including almost 550 interviews with EMEA business leaders).

We sought to understand how organisations qualify and quantify the financial statement exposures of their intangible (cyber) assets, relative to tangible assets like property, plant and equipment. The research found that in EMEA, only 11% of potential loss to intangible assets was covered by insurance, compared with 49% for tangible assets. This is despite almost four in ten companies having experienced a cyber breach in the past 24 months. This bias means information and system assets are too often exposed without appropriate coverage, which has significant implications for increasingly connected global businesses.

Our intention is that this cyber risk study will assist risk managers, finance, IT and legal in taking a broader look at their organisation's overall risk profile and ensuring sufficient insurance coverage is in place for the relative financial impact of all risks – not only the traditional, tangible ones.

Bill Peck
CCO EMEA,
Aon Risk Solutions

Karl Hennessy
CBO EMEA &
CEO Global Broking Centre,
Aon Risk Solutions

Ponemon Institute
Cyber Impact Research

This research was commissioned by Aon and independently conducted by Ponemon Institute LLC. This report focuses on the research findings for EMEA only, based on the perceptions of 545 EMEA business leaders, largely in finance, risk, information security and compliance. Further information on the research methodology is provided on page 8.

Aon Expert Perspective

"The preparedness and protection mechanisms of companies against a tangible assets disruption is greater; there are more contingency/ emergency plans in place as risks are better known and understood, while tangible assets can also be more easily replaced. Conversely, disruption against intangible assets such as know-how, and intellectual property which, once lost, are lost forever, is harder to plan for and protect against."

Claudia Beatriz Gomez
Financial Lines Director,
Aon Risk Solutions, Spain

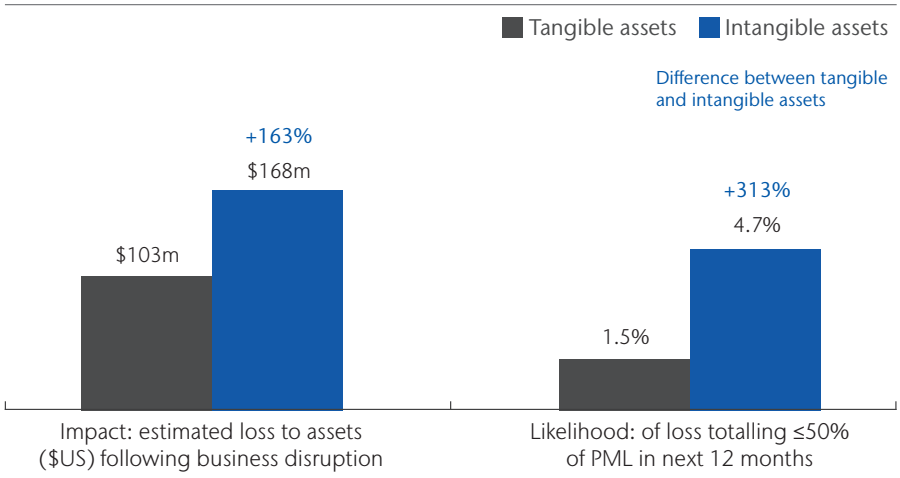
Tangible versus intangible assets – a story of unequal risk

The survey reveals that the perceived value of both tangible and intangible assets is relatively similar, with just 3% difference. On average, the total value of tangible assets reported was US$872 million, compared to US$845 million for intangible assets.

When asked to estimate an average figure for the loss or destruction of all their intangible assets (or probable maximum loss / PML), again the estimation was similar (US$638 million for intangible assets, compared to US$615 million for their tangible assets).

In contrast, both the impact of business disruption to intangible assets and the likelihood of an intangible asset or data breach occurring is seen as significantly greater than for tangible assets. The estimated impact of a business interruption to intangible assets is US$168 million, 63% higher than US$103 million for tangible assets; while the likelihood of experiencing a loss is 4.7%, compared to 1.5% for tangible assets (for losses totalling no more than 50% of PML over the next 12 months).

Incident impact and loss likelihood

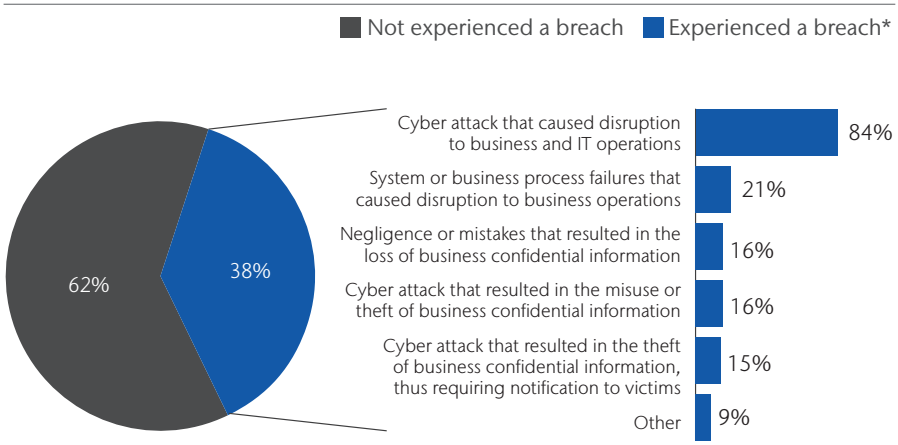


Data and security breaches – more common than you think

While some risk professionals may feel a cyber incident is unlikely in their business or industry, the reality is quite different, with the survey revealing that almost four in ten (38%) have experienced a material or significantly disruptive loss relating to a data breach or security exploit (vulnerability) in the past 24 months. The average financial impact of these EMEA incidents was US$1.1 million, with the most common involving a cyber attack disrupting business and IT operations (84%).

Cyber is clearly on the corporate risk agenda for four in ten businesses, with 38% placing cyber as a top five business risk. Further, just under half (46%) expect cyber risk exposures to increase in the next two years, while 40% think the level of risk will stay the same.

Data and security breaches



**Breach is a material or significantly disruptive security exploit or data breach one or more times in past 24 months*

Aon Expert Perspective

"Cyber incidents have complex implications and are becoming increasingly common. For example, in late 2014 a European steel mill suffered huge damage resulting from hackers gaining entry to the plant's network and causing an unscheduled furnace shutdown. Here we saw an intangible asset incident having very real implications on physical assets and business interruption. As mobile devices, cloud computing, data and analytics and 'the internet of things' continue to grow and become even more integral to business operations, the opportunities for cyber incidents increase at a similar pace."

Mark Buningh
Cyber Risk Practice Leader,
Aon Risk Solutions, Netherlands

Aon Expert Perspective

"Some organisations think cyber insurance will have too many exclusions, or is too new, unproven or specialist. There is also a perception that quotations require a lot of time, so these perceptions are rarely challenged and organisations continue to rely on self insurance.

However, cyber cover has been available for more than 15 years and getting an indication of price and exactly what is covered is relatively easy these days. Further, many aspects that EMEA organisations don't expect to be covered (e.g. human error, third party incidents, system failures and notification costs to victims) are often included in cyber insurance policies, or can certainly be negotiated with insurers.

And with a tangible proposal that can be discussed at board level, organisations can make more deliberate and informed decisions about cyber insurance, rather than leaving it 'out of sight, out of mind'."

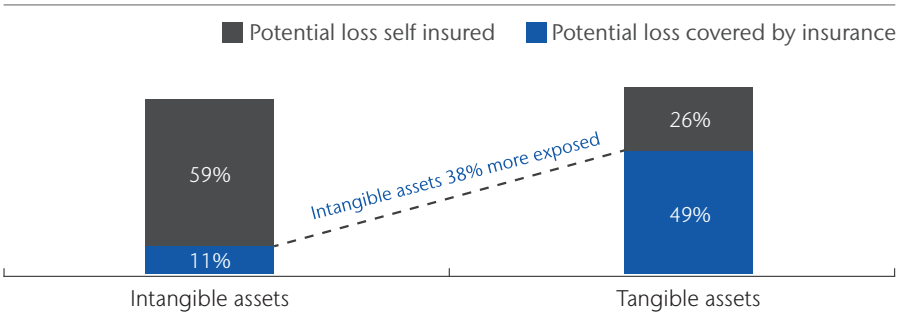
Jonathan Case
Chief Broking Officer,
Aon Risk Solutions, Finland

Management versus mitigation – the role and take-up of insurance

Despite this growing awareness of cyber risk, there is a huge insurance gap. When comparing intangible assets to tangible assets, EMEA business leaders indicated that intangible assets are 38% more exposed than tangible assets on a relative value to insurance protection basis.

Nearly half the potential loss (49%) to tangible assets is covered by insurance, but only 11% for intangible assets. In contrast, self insurance – retaining the risk on their own balance sheets rather than buying an insurance policy – is far more common for intangible assets.

Percentage of assets covered by insurance



Focusing specifically on cyber insurance cover, 79% of businesses surveyed don't currently have cyber insurance in place. And on average, there seems to be a stronger perception of exclusions than inclusions. Less than 3 in 10 EMEA businesses surveyed believe incidents involving human error or affecting third parties are covered, nor the costs to notify data breach victims. In contrast, most perceive external cyber criminal and internal malicious attacks would be covered (see table overleaf).

Perceptions of cyber insurance in EMEA

	Expect to be included	Don't expect to be included
Incidents	External attacks by cyber criminals	Human error, mistakes and negligence
	Malicious or criminal insiders	Incidents affecting business partners, vendors or other 3rd parties that have access to your company's information assets
		System or business process failures
Coverages	Forensic and investigative costs	Brand damages
	3rd party liability	Revenue losses
	Legal defence costs	Communications costs to regulators
	Replacement of lost or damaged equipment	Regulatory penalties and fines
		Notification costs to data breach victims
Services	Access to cyber security forensic experts	Identity protection for breach victims
	Access to legal and regulatory experts	Credit monitoring for breach victims
	Assistance in remediation of the incident	Assistance in the notification of breach victims
		Advanced warnings about ongoing threats
		Access to specialised technology and tools

Respondents considered what incidents, coverages and services are included in cyber insurance

- *"Expect to be included" is aspects of cyber cover 70% or more agree with*
- *"Don't expect to be included" is aspects of cyber cover 30% or less agree with*

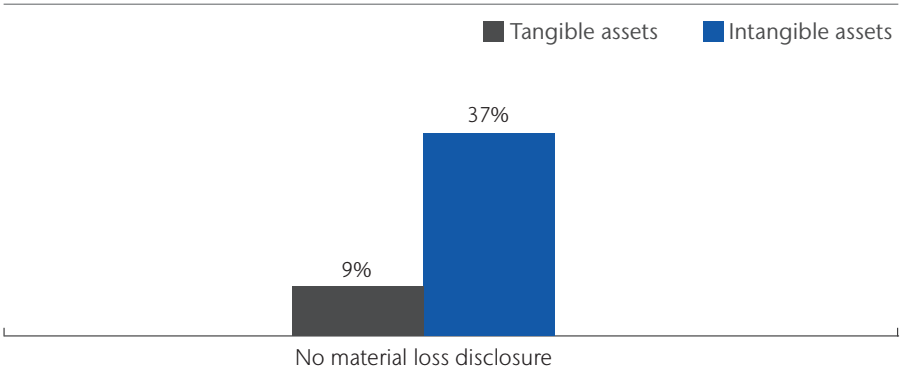
An industry challenge – limited experience with an evolving risk

Reflecting the relatively low take-up of cyber insurance, there is also a clear lack of formal risk assessment around cyber risk with 44% determining their business's level of cyber risk based on intuition, informal internal assessment, or without any assessment at all.

The research also revealed a low level of awareness and understanding of the consequences of cyber risk. For example, only 23% of respondents said they were fully aware of the legal and economic consequences that could result from a data breach or security exploit in other countries in which their business operates.

In addition, 37% of businesses would not disclose a material loss to their intangible assets in their financial statements, whereas only 9% would not disclose a material loss to tangible assets. This under reporting for intangible assets (driven by different regulatory requirements) results in the frequency and magnitude of cyber risk being under-represented in the public realm.

Financial statment disclosure of material losses



Aon Expert Perspective

"Almost all organisations recognise cyber as a growing concern, but many still perceive it to be a 'new' or unfamiliar risk. Depending on an organisations' risk maturity, some don't have the experience to both assess and quantify the risk effectively, nor risk manage it within their organisations. But once the risks are better understood and valued, then organisations can intelligently consider cyber solutions, risk management procedures and what an insurance policy can bring to the table."

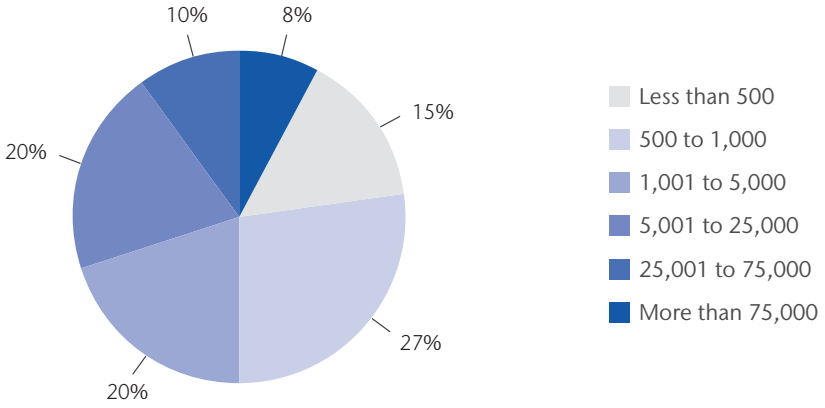
Jonathan Upshall
Cyber Insurance Broking Director,
London Global Broking Centre,
Aon Risk Solutions, UK

Methodology

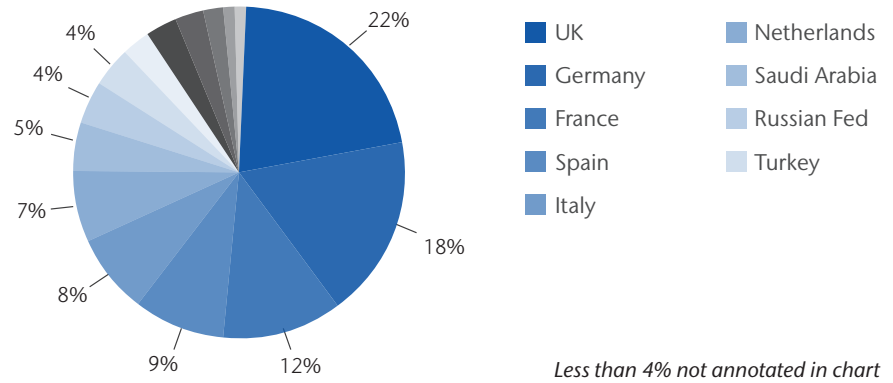
This global cyber impact research was independently conducted by Ponemon Institute LLC, and commissioned by Aon. The research was conducted in March 2015 and included 2,243 companies in 37 countries across Europe, Middle East, Africa (EMEA), North America, Asia, Pacific, Japan and Latin America.

This report focuses on the research findings for EMEA only, based on surveys with 545 companies in 15 countries throughout EMEA. The profile of the survey sample is summarised in these charts.

Employees (worldwide)

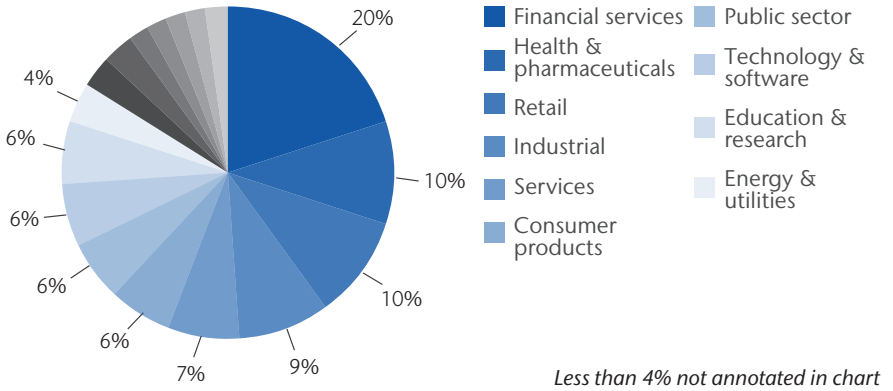


Country



Less than 4% not annotated in chart

Industry



Less than 4% not annotated in chart

Key definitions

In the context of this research:

- **Cyber risk** means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.
- **Intangible (cyber) assets** includes customer records, employee records, financial reports, analytical data, source code, models methods and other intellectual properties.
- **Tangible (property, plant and equipment) assets** includes all a company's fixed assets plus supervisory control and data acquisition systems, and industrial control systems.
- **Probable maximum loss (PML)** relates to the maximum loss a business can suffer following an incident.
    - For tangible assets this assumes the normal functioning of passive protective features – such as firewalls, non-flammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.
    - For intangible assets this assumes the normal functioning of passive protective cybersecurity features – such as perimeter controls, data loss prevention tools, data encryption, identity and access management systems and more.
- **Total Value** is an estimate of the value based on full replacement cost (not historic cost).
- **Average financial impact** of security exploits or data breaches includes all costs, including out-of-pocket expenditures such as consultant and legal fees, indirect business costs such as productivity losses, diminished revenues, legal actions, customer turnover and reputation damages.

Aon
Conclusion

The Ponemon Institute 2015 Cyber Impact Report research has revealed a troublingly low level of understanding and insurance risk transfer for intangible assets, particularly when contrasted with EMEA businesses' approach to tangible assets.

Specific highlights from the Ponemon Institute 2015 Cyber Risk Study research include:

- Information technology assets are 38% more exposed than property assets, with 11% of potential loss to intangible assets covered by insurance, compared with 49% for tangible assets.
- This is despite the fact that estimated value and maximum loss is on a par for intangible and tangible assets (e.g. probable maximum loss of US$638 million and US$615 million respectively).
- Almost four in ten (38%) of businesses surveyed experienced a material or significantly disruptive loss relating to a security or data breach in the past 24 months. The average financial impact of these incidents was US$1.1 million.
- 37% of businesses would not disclose a material loss to their intangible assets in their financial statements, whereas only 9% would not disclose a material loss to tangible assets.
- Four in ten (44%) determine their businesses' level of cyber risk based on intuition, informal internal assessment, or without any assessment at all.

Given the limited level of cyber risk assessment and cyber incident disclosure, it is unsurprising that cyber risks often remain misunderstood or unquantified. We would recommend companies take a proactive approach to assessing their cyber risk exposures and consider more closely the significance and business disruption impact of intangible asset incidents. Further, as cyber cuts across many areas of an organisation, cross functional engagement is key, including risk/compliance, IT, finance and legal.

Contacts

Mark Buningh
Cyber Risk Practice Leader
Netherlands
+31 (0)6 5134 6614
mark.buningh@aon.nl

Jonathan Case
Chief Broking Officer
Finland
+358 201 266 281
jonathan.case@aon.fi

Claudia Beatriz Gomez
Financial Lines Director
Spain
+34 91 340 5645
claudiabeatriz.gomez@aon.es

Jonathan Upshall
Cyber Insurance Broking Director
United Kingdom
+44 (0)20 7086 1897
jonathan.upshall@aon.co.uk

Ponemon Institute
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO),we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

About Aon

Aon plc (NYSE:AON) is a leading global provider of risk management, insurance brokerage and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 69,000 colleagues worldwide, Aon unites to empower results for clients in over 120 countries via innovative risk and people solutions. For further information on our capabilities and to learn how we empower results for clients, please visit: http://aon.mediaroom.com.

Follow Aon on Twitter: twitter.com/Aon_plc
Sign up for News Alerts: aon.mediaroom.com/index.php?s=58

AON | Ponemon INSTITUTE