



Cyber Insurance: Recent Advances, Good Practices and Challenges

NOVEMBER 2016



About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

INSURANCE EUROPE, the European insurance and reinsurance federation

For providing insight for cyber insurance products and services: Mr. Giorgio APRILE (AON), undisclosed (AXA Global P&C), Dr. Andreas FUERST (Allianz), Mr. Nikos GEORGOPOULOS (CROMAR Coverholder at LLOYD'S), Mr. Nils HELLBERG (German Insurance Association)¹, Mr. Yuri ROBBERT (NN Group), Mr. Erik VAN DER HEIJDEN (If P&C Insurance), Mr. Christos VIDAKIS (Deloitte Certified Public Accountants S.A.), Ms. Amparo ZABALA (Zurich Insurance (Spain))

For providing key contribution during the report and validation workshop: Mr. Theodore P. AUGUSTINOS (Locke Lord LLP), Ms. Lyndsey BAUER (Paragon International Brokers), Mr. Aldo CAPPELLETTI (UBS), Mr. Jahangez CHAUDHERRY (Talbot Underwriting Ltd), Ms. Inga GODDIJN (Risk Based Security), Mr. Laurent HESLAULT (Symantec), Mr. Niko KALFIGKOPOULOS (PwC), Prof. Vasilis KATOS (Bournemouth University), Mr. Nicholas KITCHING (Swiss RE), Ms. Marina KROTOFIL (Honeywell), Mr. Eireann LEVERETT (Concinnity Risks), Prof. Michael MAINELLI (Z/Yen Group), Ms. Marisa MELLIOU (OPAP S.A.), Dr. Marie MOE (SINTEF ICT), Mr. Gerasimos MOSCHONAS (Alpha Bank), Mr. Thomas NIMMO (Cyberfense), Mr. Christoforos PAPACHRISTOU (Thales UK), Mr. Robert A. PARISI, JR. (Marsh FINPRO), Mr. Stamatis PASSAS (National Bank of Greece), Mr. Terry QUESTED (Associated Risk Managers of Ohio Agency, Inc.), Dr. Christopher RICHARDSON (Bournemouth University Cyber Security Unit – BUCSU), Dr. Douglas RUMML (Ohio Dominican University), Mr. Bob SARGENT (Tennant Risk Services), Mr. Alexander SCHMIDL (Munich RE), Prof. Costis TOREGAS (The George Washington University)

¹ Gesamtverband der Deutschen Versicherungswirtschaft (GDV)

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2016

Reproduction is authorised provided the source is acknowledged.

ISBN 978-92-9204-178-6, doi: 10.2824/065381

Table of Contents

Executive Summary	5
1. Introduction	6
1.1 Scope and Objectives	6
1.2 Audience	6
1.3 Methodology	6
1.4 Brief Demographics	7
2. Significant Developments	8
2.1 Awareness and Preparation	8
2.2 Regulation	9
2.3 Market Growth and Maturity	10
2.4 Service Improvement	10
3. Pre-Policy Risk Assessment: Key Knowledge and Good Practices	11
3.1 Key Knowledge	11
3.1.1 Business Coverage and Baseline Assessment	11
3.1.2 Provided Coverage	12
3.1.3 Adopting Standards or an Audit Strategy	12
3.2 Good Practices	14
3.2.1 Dedicated Resources	14
3.2.2 Policies and Procedures	15
3.2.3 Employee Awareness	16
3.2.4 Incident Response	16
3.2.5 Security Measures	17
3.2.6 Vendor Management	18
3.2.7 Board Oversight	18
4. Challenges	20
5. Recommendations and Findings	21
Annex A: Questionnaire and Metrics Map	23
A.1 Questionnaire	23
A.2 Risk Assessment: Metrics Map	24

Executive Summary

Cyber insurance was created to address risk that cannot be reasonably mitigated by security measures. While it initially started in a limited form, it developed to cover more and more types of cyber risk. In comparison with other insurance sectors, cyber insurance appears to have a lower adoption rate, while the growth projections remain high. Projections estimate the global cyber insurance market to reach \$ 7.5 billion in annual sales by 2020 – tripling the 2015 figure² – and over \$ 20 billion by 2025³. It is evident that regions with established cybersecurity-related legislation, have a higher cyber insurance adoption than regions that have recent or no formed legislation. The expected growth for the European market is anticipated to be further accelerated by the adoption of the GDPR and NIS directive.

Many Member States are recognising the importance of addressing cyber risk, and have taken relevant action by publishing guides of good cyber-hygiene^{4 5}. Furthermore, insurance federations have also a great interest on cyber insurance, with actions taking place on both European⁶ and national⁷ level. Among others, insurers are facing challenges around the lack of cyber-security incident data⁸ in support of risk assessment, gathering information on cyber security management, and the uncertainty around accumulating risk. Further to the reported good practices, ENISA had generated the following recommendations, directed to policy makers, insurers, and customers, for the improvement of cyber insurance constituency:

Policy Makers

- Encourage the active participation of European Commission on ENISA cyber insurance activities
- Avoid the introduction of mandatory requirements that might undermine the cyber insurance market adoption rate

Insurance Companies

- Improve the areas of pre-policy risk assessment that are found as the most underseen by insurers
- Invest in and advance the accumulating risk calculation
- Consider adopting common standards and methodologies
- Introduce explanatory sessions, and provide customer scenarios and generic examples of policy coverage
- Clarify the policy language and offer a transparent underwriting process

Cyber Insurance Customers

- Be more open on sharing data, possibly under a legal agreement (e.g. NDA)
- Get informed, prepare, and document their environment, before requesting a cyber insurance policy

² PwC “The Global State of Information Security® Survey 2016” <http://pwc.to/2dqFg4Y>

³ Allianz Global Corporate & Specialty “A Guide to Cyber Risk: Managing The Impact of Increasing Interconnectivity” <http://bit.ly/1YyMUrD>

⁴ France, ANSSI “40 essential measures for a healthy network” <http://bit.ly/2dr6nbA>

⁵ United Kingdom, Department for Business, Energy & Industrial Strategy “Cyber essentials scheme: overview” <http://bit.ly/1hkkmdz>

⁶ i.e. Insurance Europe

⁷ e.g. GDV in Germany

⁸ ENISA “The cost of incidents affecting CIIs” <http://bit.ly/2dlkNmo>

1. Introduction

Cyber insurance is a product that has been created to counter residual risk associated with the information systems of asset owners. Despite the large number of developments that have taken place over the last few years, the cyber insurance market is yet to receive the anticipated adoption rate. While some regions have made progress on the basis of supportive legislation, it is found that in comparison with other insurance sectors, the state of cyber insurance is at a less mature stage. With the general data protection regulation (GDPR) being adopted on April of 2016⁹, and network and information security (NIS) directive¹⁰ on July 2016, the need for cyber insurance is anticipated to grow¹¹; a growth that can be embraced by enabling an informative product development and adoption.

1.1 Scope and Objectives

The objectives of this report are to:

- Raise awareness for the most impactful market advances, by **shortly identifying the most significant cyber insurance developments** for the past four years (2012-2016)
- Capture the **good practices and challenges** during the early stages of cyber insurance lifecycle (i.e. **before an actual policy is signed**) – laying the ground for future work in the area.

1.2 Audience

The primary audience is **insurance companies**, who can either **benchmark themselves** against the market trends, **or evaluate good practices** before entering the market.

Additional beneficiaries are **customers interested to adopt a cyber insurance policy**, allowing them to take informed decisions and prepare in advance.

1.3 Methodology

The report consists of two streams; the first one identifies the most impactful advances, and the other captures the good practices and challenges of the insurer-driven pre-policy risk assessment.

Information gathering utilised publicly available information, and a cyber insurance stakeholders group, including representatives from cyber insurance companies. To ensure multidimensional feedback, there was a significant effort to have a diverse geographical and industry representation within the formed stakeholders group. ENISA has established contact with insurance companies that have an active cyber insurance business. Feedback was received by conducting interviews, using predefined and group-validated questions.

⁹ European Commission – Press Release “Joint Statement on the final adoption of the new EU rules for personal data protection” <http://bit.ly/1V3hmdM>

¹⁰ European Council – Council of the European Union “EU-wide cybersecurity rules adopted by the Council” <http://bit.ly/1WCtcMv>

¹¹ EurActiv.com “New EU digital laws could boost specialised cybersecurity insurance” <http://bit.ly/24sDJJF>

1.4 Brief Demographics

From a total of 37 participants approximately 78% (29) of the stakeholders group is based in EU/EFTA countries. Of these, 40% (10) of all participants comes from United Kingdom; a percentage that might be expected, since the British market exhibits a higher level of maturity in comparison with the rest of the region. The industry representation within the stakeholders group has been diverse, with 69% (24) of the representatives having an Academia/Research or Insurance background, and the other 31% (13) coming from Advisory, Defence, Finance, Gambling, Information Technology and Services, Legal Services and Non-profit. From the market of insurance organisations with a cyber insurance product, we had participation from Finland (1), France (1), Germany (2), Greece (2), Italy (1), Netherlands (1), and Spain (1).

2. Significant Developments

With cyber insurance being a relatively new product in its' current form¹², the market and environment that surround it are subject to change. By taking a record of the most impactful changes, it might be easier to understand which of them make a real difference. For the purpose of this work stream, we have asked the following question to the stakeholders group.

What would you consider as the most notable (not necessarily big, but certainly impactful) development(s) in the area of cyber insurance, in the past four years (2012-2016)?

2.1 Awareness and Preparation

Over a third of responders had recognized the increasing threat landscape complexity, with sophisticated attacks¹³ becoming prevalent and accessible by a larger number of adversaries. Modern tools can turn an **intent** to an **act** much more efficiently than before, and new technologies introduce a larger attack surface.

This results in a **growing**¹⁴ **recognition**¹⁵ by organisations and their leadership **that cyber is an operational risk that has to be addressed**. Many Member States have taken relevant action by publishing guides of good cyber-hygiene¹⁶ ¹⁷. Insurance federations have also a great interest on cyber insurance, with actions taking place on both European¹⁸ and national¹⁹ level.

Regardless of the increasing dynamic of awareness, the **level of understanding of an organisations' exposure to cyber risk is basic**. It has been shown that only a fifth (21%) of the organisations have a clear understanding³³, placing the rest in a relatively disadvantaged position³³.

Increasing awareness leads to better preparation, which could have the form of adopting traditional security measures, writing a new cyber insurance policy, or increasing existing policy limits²³. This **contradicts previous ENISA**



Figure 1: Cyber risk understanding of organizations in Europe (2015)³³.

¹² I.e. providing both first and third party coverage.

¹³ Such as: Doxing, Energy Outage, Espionage, IP theft, Vandalism

¹⁴ World Economic Forum "Global Risks 2015 10th Edition" <http://bit.ly/15wPuqV>

¹⁵ Financial Times "High-profile hacking raises cyber security fears" <http://www.ft.com/intl/cms/s/0/5870af72-e298-11e3-a829-00144feabdc0.html>

¹⁶ France, ANSSI "40 essential measures for a healthy network" <http://bit.ly/2dr6nbA>

¹⁷ United Kingdom, Department for Business, Energy & Industrial Strategy "Cyber essentials scheme: overview" <http://bit.ly/1hkkmdz>

¹⁸ i.e. Insurance Europe

¹⁹ e.g. GDV in Germany

findings²⁰ that an insured entity **might invest less in security measures due to a policy presence**.

Nowadays insurance companies not only require to know, but might also validate a customers' preparation level²¹, and may also assist them by offering cyber risk assessment resources and incident response services.

2.2 Regulation

Regulatory changes are found to impact cyber insurance to a great extent. Whether these have the form of mandatory notification, introduction of fines, or "right to know" for users²² – they ultimately **result in a better market preparation**, of which cyber insurance is a part of. In particular, the adoption of the EU NIS Directive and GDPR may have an effect similar to the one that relevant law-making had on the US cyber insurance market.

GDPR is aiming to safeguard personal data, while the **NIS Directive** requires operators to appropriately secure their networks and protect the service provision. Both regulations are **expected to drive a high level of interest in the Cyber insurance market**, particularly for the industries explicitly identified in the NIS Directive (Table 1).

Essential Services in Critical Sectors	Energy (Electricity, Oil, Gas)
	Transport (Air transport, Rail transport, Water transport, Road transport)
	Banking
	Financial market infrastructures
	Health sector
	Drinking water supply and distribution
	Digital Infrastructure
Digital Service Providers	Online marketplace
	Online search engine
	Cloud computing service

Table 1: Types of entities for the purposes of point (4) of Article 4 of NIS Directive

²⁰ ENISA "Incentives and barriers of the cyber insurance market in Europe" <http://bit.ly/1XoMZzX>

²¹ E.g. UK Insurance Act 2016, requiring an insured to make a "fair presentation of the risk"

²² European Commission – Press release "Agreement on Commission's EU data protection reform will boost Digital Single Market" <http://bit.ly/1J9ZUdt>

2.3 Market Growth and Maturity

There is evidence of market improvement despite the fact that the available data in support of the underwriting process are still inadequate. The growth of the cyber insurance market^{23 24} (Figure 2), has led to an **increased number of claims**. Claims can function as **feedback and an evolutionary force for the market**, allowing brokers and product development to improve over time. That improvement along with knowing the cause of loss²⁵ for the majority of claims (Figure 3), can lead to the reasonable assumption that these are the areas where the Cyber insurance industry has gained the most experience.

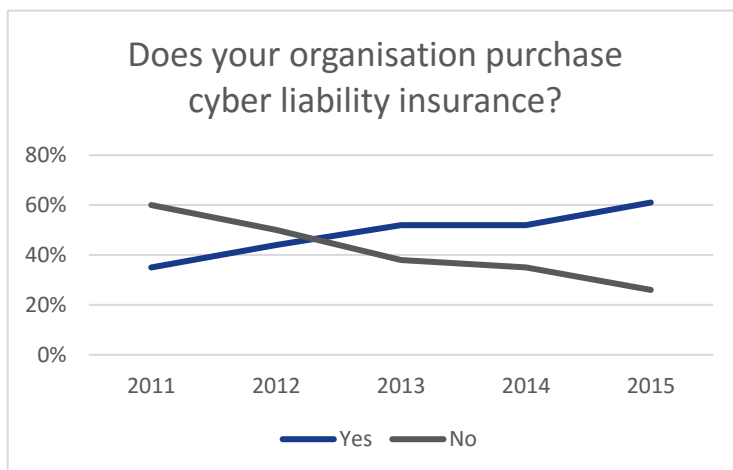


Figure 2: Cyber Insurance Adoption (2011 – 2015)²³.

A notable example of rising maturity is the one of British-based insurers, who have been writing policies for US-based companies for the past few years. The **exposure to a more legislative environment** and the presence of the **mandatory incident reporting** has given a **wealth of valuable lessons** to these companies, well in advance of the recently adopted EU regulations.

2.4 Service Improvement

Insurers can now offer a better service through the use of **efficient management and analytics**, allowing them to extend their portfolio by additional offerings such as **risk assessment and breach investigation**. Improvements on assessing risk over time allow covering more risk, which in turn may result in the introduction of policies that cover physical damage – when associated with a cyber-induced incident.

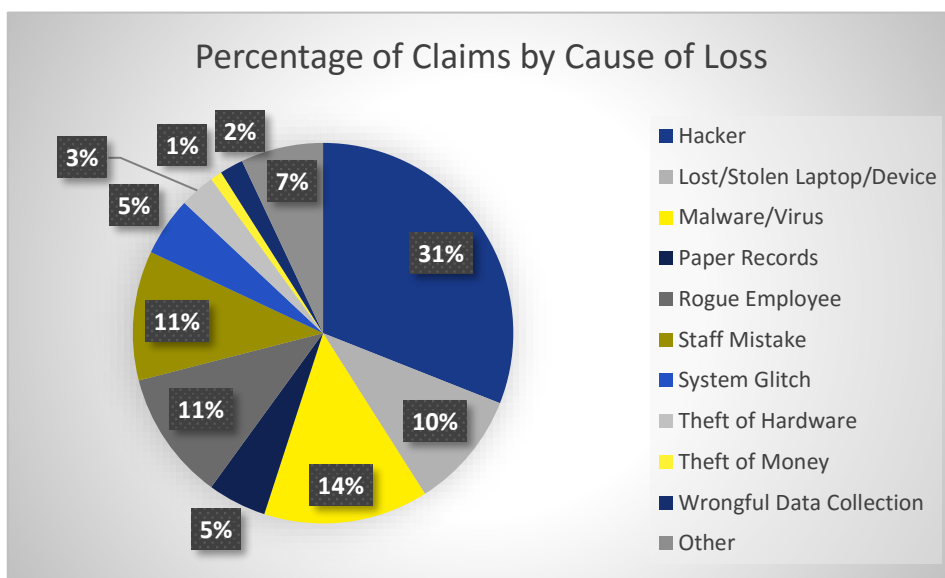


Figure 3: Claims by Cause of Loss (2012 – 2015)²⁵

²³ Advisen "Information Security and Cyber Liability Risk Management" <http://bit.ly/1M9Gyp0>

²⁴ Insurance Business "'Every large firm to have cyber cover in three years,' says Marsh leader" <http://bit.ly/1X0OELc>

²⁵ NetDiligence "2015 Cyber Claims Study" <http://bit.ly/1HbxynK>

3. Pre-Policy Risk Assessment: Key Knowledge and Good Practices

Risk assessment assists both insurers and consumers to adapt to the rapid change of the operational environment. This chapter will present basic knowledge and good practices on the **insurer-driven risk assessment**, before a policy is issued.

3.1 Key Knowledge

The following sections will present key risk assessment knowledge, as obtained by the questionnaire²⁶ answered by representatives of insurance organisations with a cyber insurance product.

3.1.1 Business Coverage and Baseline Assessment

The **vast majority** of the interviewed cyber insurance companies **provide cover to all business sectors**. A few notable exceptions that insurers could be hesitant to address are: Payment Service Providers – unless they would be part of a wider service²⁷, gambling, and the adult industry. Many **insurers have recognised the importance of the SME** market and develop tailored risk modelling, products and assessment for it. The reported industries with the highest interest for purchasing a cyber insurance policy are: Finance, Health, ISP, Legal, and Telecommunications; with an overlap between them and the NIS Directive list of applicable industries – which is statistically non-significant since there was no data to verify any assumptions.

Most insurers use the following information in carrying out a basic form of an assessment (i.e. Baseline Assessment) for all sectors, and depending on the results of it, an extended (or follow-up) assessment:

- Enumeration and geographical spread of business:
 - Size
 - Operations
 - Revenue
- Detail on business:
 - Sector
 - Activities
 - Services
 - Outsourced functions
 - Risk exposure
- Dependencies on IT infrastructure
- The use, storage, or sharing of data
 - Data volume
 - Data sensitivity (e.g. personal data, health, intellectual property, machine generated)
 - Derived liability
- Incident history (if they have been attacked)
- Corporate presence in social media
- Policy and claims history (if they had a policy, and any claims against it)
- Requested policy limit (or risk appetite of the insured)

²⁶ Available on document section A.1 Questionnaire

²⁷ e.g. Retail

Risk assessment might be performed on the basis of an established certification such as ISO 2700x, and it is found that the ultimate decision maker is the underwriter or insurer management, who might take into consideration factors that are not captured through the use of standard tools.

3.1.2 Provided Coverage

The core coverage by the majority of insurers is categorised as first and third party risk coverage, as detailed below. First party risks are the ones that directly affect the insured; while third party risks are risks that might initially affect someone other than the insured (first party) or insurer (second party), against which an insured would like to have coverage.

First Party Risk Coverage	Data breach
	Data leakage
	Business interruption
	Cyber extortion
Third Party Risk Coverage	Privacy liability
	Electronic media liability

Table 2: First and Third Party Risk Coverage among most insurers

Non common coverage that has been reported to be offered by a number of insurers includes the following: business revenue (dependent or not), digital assets disruption, insider threat (of a non-intentional nature), intellectual property, reputational harms, and targeted attacks.

Extra coverage that might take the form of an additional policy or accompanying services is: forensics, fraud, legal costs, PR measures, and ransomware.

The few instances of **coverage exclusion** have been reported to be around widespread non-targeted attacks, and third party intrusion. The latter exposes a **significant gap**, since there is a very low number of organisations that assesses the risk of third parties³³.

3.1.3 Adopting Standards or an Audit Strategy

None of the interviewed insurance companies would require the presence of a standard for assessing the risk of a potential client; however, standards were universally identified as evidence of good governance. All insurers have either recommended or endorsed as good to have, compliance with the following: **GRAMM–LEACH–BLILEY ACT, HIPAA, HITECH, ISO 2700x or derivatives** (e.g. DIN 27001), **PCI-DSS, SOX,**

and VdS²⁸. It might be worth mentioning that in a small number of cases, the presence of a standard would reduce premium or limit the risk assessment to the basic assessment questions (i.e. Baseline Assessment).

While the **majority of the insurers does not have an auditing requirement, they do consider it a good practise**, and would do a risk assessment whether an audit strategy is present or not. If the insurer-driven risk assessment exposes gaps, then an audit can follow up. Furthermore, since a recurring audit is something that most corporate customers do, not doing so would have a negative impact.

There was also evidence that audit results are found to affect not only the insurability, but also the policy limit. A small number of insurers would look at the global external audit reports for large corporate customers, and would require an audit for operators of essential services (as defined by NIS Directive, Table 1).

²⁸ Third-party certification body, subsidiary of the German Insurance Association (GDV)

3.2 Good Practices

Risk assessment is the key to assess the changing risk appetite of a business, and further allows an insurer to assess the level of preparation of a potential client. That can take the form of filing an application (with no further action), running an assessment²⁹, or obtaining evidence of a previous assessment.

Cyber insurance companies assess differently a clients' risk, and they do not uniformly accept a certification as validation of a customers' security level. Recently, several insurance companies have been engaged in an effort to develop common practices, and establish a higher degree of consistency in the market³⁰.

When assessing a clients' risk, insurers generally focus on the following main categories:

- Dedicated Resources
- Policies and Procedures
- Employee Awareness
- Incident Response
- Security Measures
- Vendor Management
- Board Oversight

Using these categories enabled a structured comparison of interview findings against the anticipated results^{31 32 33}, and the generation of good practices; with the latter being highlighted at the end of the following subsections. A visual and brief representation of the comparison and results can be found in section A.2 Risk Assessment: Metrics Map.

3.2.1 Dedicated Resources

Evidence has shown that insurers attach importance to the presence of leadership roles with Information Security focus³⁴ within an organisation, and enumerate the number of employees that are dedicated to Information Security. While both these points give a good indication of the dedicated resources, they could be significantly improved by a couple of additional checks.

Equally significant to the presence of an Information Security professional among leadership, is the time allocation to tasks other than what their role mandates; thus, it is advisable to not only evaluate the presence of such a role, but also examine their responsibilities. That could be done by conducting an interview, or viewing records of time and task allocation.

The reporting lines of a CISO, can impact the effectiveness of an Information Security program. It would therefore be highly recommended to evaluate the reporting line of a CISO (or equivalent), and whether that role is reporting directly to the CEO.^{35 36 37}

²⁹ Internal or external, self-assessed or not

³⁰ Cambridge Centre for Risk Studies "Cyber Insurance Exposure Data Schema V1.0" <http://bit.ly/1Pb1vVb>

³¹ FSSCC "Purchasers' Guide to Cyber Insurance Products" <http://bit.ly/1RT3TOM>

³² Allianz Global Corporate & Specialty "A Guide to Cyber Risk" <http://bit.ly/1YyMUrD>

³³ Marsh "European 2015 Cyber Risk Survey Report" <http://bit.ly/1L7XJdh>

³⁴ Such as: CIO, CISO, CPO, CSO

³⁵ CIO "Seven reasons the CISO should report to the CEO and not the CIO" <http://bit.ly/29xE5xl>

³⁶ DARKReading "Top Infosec Execs Will Eventually Report To CEOs, CISOs Say" <http://ubm.io/1XkWRNw>

³⁷ ThreatTrack Security "Why Your CISO Should Report to the CEO" <http://bit.ly/29FXutG>

In addition, it is advisable to examine the overall resources, in respect to both quality and quantity. Since the number of employees is not a reliable metric by itself, it could be enhanced by incorporating metrics that would compare current skillsets against the requirements, or metrics relevant to employee effectiveness³⁸.

As an example of a non-employee resource metric, an insurance company could request to view a list of completed Information Security projects, their alignment to corporate Strategy, allocated budget, and whether they have met the Critical Success Factor (CSF). While many of these details can be confidential, critical elements could be anonymised prior to sharing, or have an insurer view evidence and validate compliance.

Good Practices:

- Examine if leadership roles with Information Security focus have any responsibilities irrelevant to Information Security.
- Check whether the CISO (or equivalent) reports directly to the CEO.
- Measure the amount and quality of resources that a company invests on Information Security.

3.2.2 Policies and Procedures

Insurers have demonstrated an advanced maturity on assessing the policies and procedures of an organisation. However, while insurers check whether cyber security standards are followed, they were not found to thoroughly validate the existence of a comprehensive and formal Information Security program³⁹. The program would have to address Information Security in all possible dimensions of security controls (i.e. technical, administrative, and physical).

Furthermore, since working remotely⁴⁰ and the use of mobile devices^{41 42} are potential risks in a corporate environment, cyber insurance companies would be advised to appropriately check clients' preparation in that respect⁴³.

As the mere existence of a program does not imply an advanced capability, an insurer would also have to assess the cyber-security maturity of an organisation⁴⁴.

Good Practices:

- Validate the existence of a comprehensive and formal Information Security program.
 - Confirm it covers technical, administrative and physical measures for data protection.
 - Ensure the appropriate provisions for the security of mobile devices and teleworking.
- Evaluate the cyber security maturity of the organisation.

³⁸ As per ISO 27001, section 7.2 Competence (v. 113010)

³⁹ As per ISO 27001, section A.6.1 Organization of information security – Internal organization (v. 113010)

⁴⁰ The Guardian "The security risks of remote working" <http://bit.ly/2922A7t>

⁴¹ ENISA "Workplace IT: ENISA sees opportunities and risks in "Bring Your Own Device" trend" <http://bit.ly/1r8gjfy>

⁴² US-CERT "The Risks of Using Portable Devices" <http://1.usa.gov/1PcTXzu>

⁴³ As per ISO 27001, section A.6.2 Organization of information security – Mobile devices and teleworking (v. 113010)

⁴⁴ ENISA "Technical Guideline on Minimum Security Measures" <http://bit.ly/2aWGjD0>

3.2.3 Employee Awareness

While the human factor can pose a significant risk within an organisation, with proper training it can turn out to be a valuable defence mechanism – and an enabler for current controls. For example, an untrained employee who cannot recognise a phishing e-mail, is the weakest link for any security measure that can be applied; while one who is vigilant, will safeguard a company not only by not becoming a victim, but also by reporting the attempt to the appropriate department. In addition, an employee who is aware will not only implement policies and procedures, but also understand them – something of a great value.

Insurance companies were found to verify the presence of a formal Security Awareness program, which is a key element for securing the human factor within a company. Since phishing is the prevalent method for malware delivery⁴⁵, any simulations and exercises of such, would add a significant value to such a program. To secure the employees' commitment, an organisation would need to provide motives or measures for those who repeatedly pass or fail the exercises.

Good Practices:

- Check whether phishing exercises are taking place as part of a formal Security Awareness program.
 - Enumerate the actions (or rewards) that are taken (or offered) to employees who repeatedly fail (or succeed) these.

3.2.4 Incident Response

An Incident Response program defines the processes and resources that an organisation engages for addressing any Information Security incidents. Insurers validate the existence of a potential clients' Incident Response program in a formal form, and evaluate their tolerance level towards withstanding several incidents.

Incident notification is a key component of NIS Directive that requires the establishment of an Incident Response function within an organisation.

Similar to other functions, testing the capabilities of a defence mechanism is critical to the success of it; hence, confirmation of the presence of regular exercises in support of an existing Incident Response program⁴⁶ is recommended. A valuable finding is that the presence of an incident response team has the top positive impact on the per capita cost of a data breach⁴⁷ (Figure 4).

⁴⁵ Symantec "Internet Security Threat Report, Volume 21, April 2016" <http://symc.ly/1Ytqm9Y>

⁴⁶ Harvard Law School Forum on Corporate Governance and Financial Regulation "The Importance of a Battle-Tested Cyber Incident Response Plan" <http://bit.ly/29IUwf>

⁴⁷ Ponemon Institute "2016 Cost of Data Breach Study: Global Analysis" <http://ibm.co/1tz141c>

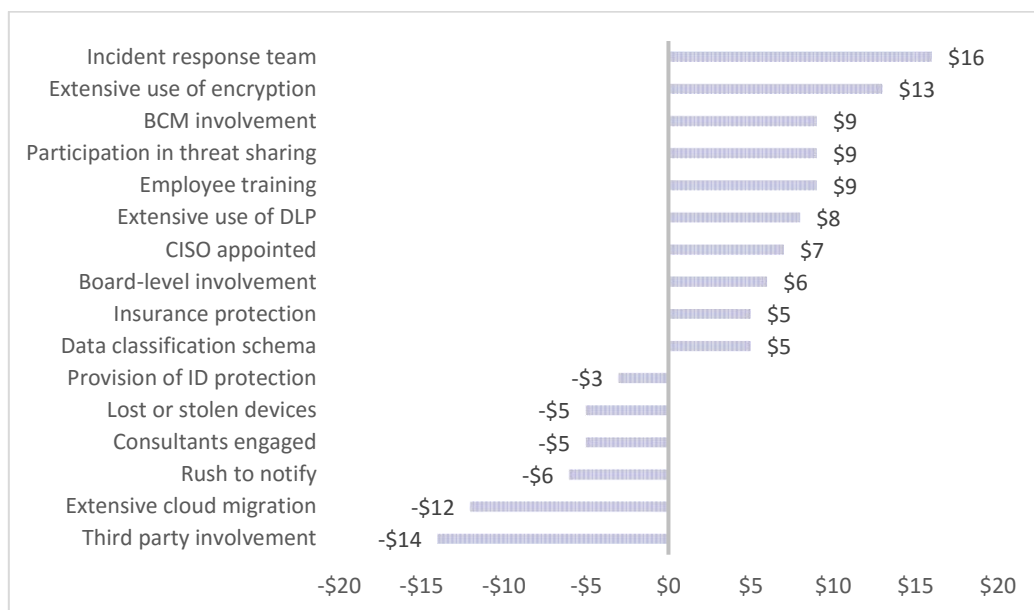


Figure 4: Impact of 16 factors on the per capita cost of data breach (2016)⁴⁷.

Good Practise:

- Confirm there are regular exercises in support of a formal Incident Response program.

3.2.5 Security Measures

Insurers have indicated as important that technical measures and solutions are checked thoroughly, and that a defined physical access is part of their security measures evaluation. However, it is important to receive information about any existing encryption strategy and the technologies involved, to ensure the proper implementation of technical measures such as data backup or remote connectivity. In addition to encryption, the proper implementation of the following would need to be confirmed:

- Business Continuity Planning⁴⁸
- Data classification⁴⁹
- Data retention
- Access control
- Log monitoring⁵⁰
- Intrusion detection
- Network segmentation⁵¹
- Network monitoring
- Vulnerability management⁵²
- Penetration testing

⁴⁸ As per ISO 22301

⁴⁹ As per ISO 27001, Control objectives and controls A.8.2

⁵⁰ As per ISO 27001, Control objectives and controls A.12.4

⁵¹ As per ISO 27001, Control objectives and controls A.13.1.3

⁵² As per ISO 27001, Control objectives and controls A.12.6.1

Good Practices:

- Confirm the proper implementation of: Business Continuity Planning, data classification, data retention, access control, log monitoring, intrusion detection, network segmentation, network monitoring, vulnerability management, and penetration testing.
- Receive information about any existing encryption strategy and the technologies involved.

3.2.6 Vendor Management

Vendor Management is a greatly overlooked weakness. It has been observed that only 23% of organisations assess suppliers for cyber risk⁵³. That can result in a significant exposure, since supplier networks are outside an organisations' control – with many examples of successful breaches supporting that conclusion^{53 54 55 56}.

The above finding should be of a particular attention to cyber insurance companies, since it could significantly affect a large number of potential or existing clients. It is recommended that insurers verify the existence of a formal third party management process, and receive details on due diligence, ongoing oversight, and contractual obligations.⁵⁷

Good Practices:

- Verify the existence of a formal third party management process.
- Receive details on: due diligence, ongoing oversight, and contractual obligations.

3.2.7 Board Oversight

The awareness of governing board concerning crucial information security issues is an early step for addressing risk. Should a board become aware of such issues in an irregular or delayed manner, there is a risk of the corrective action being unauthorised, badly timed, or disproportionate. Therefore, it is important to evaluate the frequency of reporting cyber-security risk issues and related action to the Board.

While it is important to have knowledge of crucial information security issues, a board may have a defined set for the approval of oversight, enough to have an impact on an organisation – without overwhelming the board with such requests. It is strongly advised that should such a detail exists, an insurer would obtain information about it.⁵⁸

The earlier paragraphs address the boards' frequency of being informed, and the level of involvement in a program. It has been found that although these two factors are of a great importance, the ongoing communication and direction throughout an organisation is the basis upon which the decisions and

⁵³ Computer Weekly "Home Depot traces credit card data hack to supplier compromise" <http://bit.ly/1XtDWxE>

⁵⁴ DARK Reading "Target Breach: HVAC Contractor Systems Investigated" <http://ubm.io/1Pwm8yM>

⁵⁵ SC Magazine "TalkTalk blames supplier for breach affecting 4m customers" <http://bit.ly/1F0rljd>

⁵⁶ Health IT Security "Potential Healthcare Data Breach Affects Over 19K Patients" <http://bit.ly/1t9Q7mL>

⁵⁷ As per ISO 27001, Control objectives and controls A.15

⁵⁸ IT Governance Institute "Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition" <http://bit.ly/1WddA0A>

messages will traverse⁵⁹. An effective communication and direction would be a facilitating factor for the decisions and information flow, which could be described as an organisations' equivalent of a neural network during an information security event; a slow message traversal would have a catalytic effect on the efficiency of its' content.

Good Practices:

- Detail the frequency of reporting cyber-security risk issues and related action to the board.
- Detail any existing board-level approval of oversight of the Information Security Program.
- Receive details of the organisations' internal information flow related to cyber-security, lines of communication, including crisis communication plans.

⁵⁹ KPMG "Connecting the dots: A proactive approach to cybersecurity oversight in the boardroom"
<http://bit.ly/1LMAdXn>

4. Challenges

The greatest challenge of insurers is the **lack of cyber-security incident data in support of risk assessment**, which would further allow them to differentiate customers on the basis of risk. The establishment of anonymized databases for cyber incidents, would help insurers better understand the risk and provide adapted cover. A further data-related challenge is **gathering information on cyber security management**, especially for multinational corporate customers with diverse activities and Mergers and Acquisitions (M&A) history. Furthermore, while **customers** are willing to discuss company related information without a record, they are **less likely to share information by official documentation** (e.g. incident report history, audit report). A rising concern among a number of insurers is the **uncertainty around accumulating risk**; for example, customers might not only migrate data to the cloud, but operations as well. In the event that an incident would occur, an insurer cannot be certain about the number of customers that would be affected. Customers will know if they use cloud, but not who else does. That concern becomes very realistic by knowing that such threats exist^{60 61}. An additional example can be around third-party vendors, where a formed relationship of trust could be taken advantage by an adversary. Other items that were noted as challenges from a smaller number of insurers are:

- Lack of customer awareness on cyber insurance
- Common understanding of policy terms and conditions
- Lack of internal (technical) expertise
- Cost calculation on the basis of an incident scenario
- Utilizing predictive analytics for the assessment of potential risks and impact

It is interesting to note that recent findings on challenges, as seen on Figure 5, could possibly be tackled together with present findings. For example, not understanding exposures or coverage, and the application process, could be addressed by **explanatory sessions**. Giving the **customer scenarios and examples of policy coverage** could act as a fast method to **raise awareness and understanding of cyber insurance**.

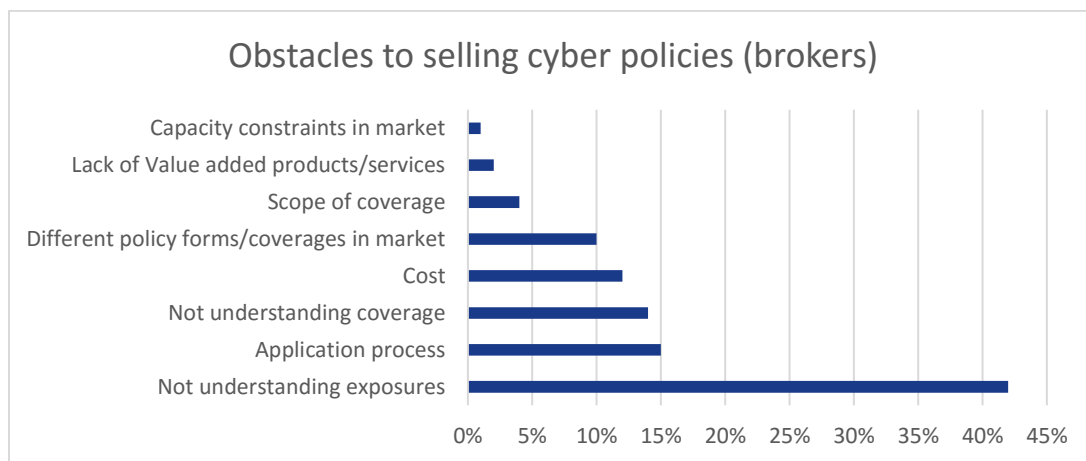


Figure 5: Obstacles to selling Cyber Policies (brokers) (2015)⁶².

⁶⁰ CrowdStrike "VENOM Vulnerability" <http://venom.crowdstrike.com/>

⁶¹ Xenproject.org Security Team "Xen Security Advisory CVE-2015-5154" <http://bit.ly/1gdvYVw>

⁶² Advisen "Cyber Liability Insurance, Market Trends: Survey" <http://bit.ly/29IJWF>

5. Recommendations and Findings

The interviews revealed a number of points that drove good practices, many of which are found to also reduce the cost of an incident⁴⁷. These can **improve the insurers risk assessment by adapting priorities and focus**, include new items for evaluation – and **improve customer preparedness by a thorough risk assessment checklist**.

Further to the derived good practices, the report had generated the following recommendations, directed to policy makers, insurers, and customers, for the betterment of cyber insurance constituency:

Policy Makers

- Encourage the active participation of European Commission on ENISA cyber insurance activities
- Avoid the introduction of mandatory requirements that might undermine the cyber insurance market adoption rate

Insurers – Risk Assessment

- Focus on an organisations' resources, and conduct a throughout review in terms of both quality and quantity
- Evaluate whether a customers' policies and procedures address the prevalent threat of remote working and mobile devices
- Consider the existence of recurring exercises as a key factor for evaluating the completeness of a customers' response or preparedness function
- Evaluate security measures on the basis of state-of-the-art practices, while considering a customers' environmental characteristics and needs
- Review an organisations' board involvement as thoroughly as any traditional security measure

Insurers – Risk Calculation

- Invest and advance the accumulating risk calculation, particularly in the areas of vendor management and cloud computing

Insurers – Business Enablers

- Introduce explanatory sessions, and provide customer scenarios and generic examples of policy coverage.
- Clarify the policy language, and avoid using generic terminology that can be interpreted in multiple ways
- Offer a transparent underwriting process, detailing the criteria and criticality that drives pricing

Cyber insurance Customers

- Be more open on sharing data, possibly under a legal agreement (e.g. NDA)
- Get informed, prepare, and document their environment, before requesting a cyber insurance policy

The past four years have been full of advances on the Cyber insurance frontier. Organisations and their leadership have recognised the importance of cyber as an operational risk. Since the understanding on cyber risk is basic, it is recommended that the organisations work to **understand risk before addressing it**. It was of significant importance to see that, in contrast to previous ENISA findings, **customers do not invest less in (traditional) security measures due to a policy presence**. The fact that insurers usually require an annual re-assessment might be reinforcing that different customer behaviour.

Regulatory changes are resulting in better preparedness, similar to the post-legislative adoption in US. Thus, both GDPR and NIS Directive are expected **to be followed by an increased market need** in EU. The increased **claims** have been found to **function as feedback that enhances market proposals**. European insurers who have been exposed to a more **legislative environment**, have obtained a **wealth of valuable lessons** that can now apply in EU.

The majority of **insurers cover all sectors**, with many of them recognising the **importance of SME** market and **develop customised solutions** for it. Underwriters and management are the ultimate decision makers following a risk assessment, where they would be called to take into consideration several more variables.

The **core coverage** by most insurers includes first and third party risks (Table 2), with **less common coverage** addressing business revenue (dependent or not), digital assets disruption, insider threat (of a non-intentional nature), intellectual property, reputational harms, and targeted attacks. Insurers offer **extra coverage** such as: forensics, fraud, legal costs, PR measures, and ransomware. The reported **coverage exclusion** around widespread non-targeted attacks, and third party intrusion exposes a **significant gap**, since **less than a quarter of organisations are assessing suppliers for cyber risk**.

The total of interviewed insurers have either recommended or endorsed as good to have, the following third party certifications: **GRAMM–LEACH–BLILEY ACT, HIPAA, HITECH, ISO 2700x or derivatives** (e.g. DIN 27001), **PCI-DSS, SOX**, and **VdS**²⁸. Auditing was not identified as a requirement but it is considered a best practise.

The core **identified challenges** of insurers, in respect to **pre-policy risk assessment** are:

- Lack of cyber-security incident data
- Gathering information on cyber security management
- Customers less likely to share any documentation
- Uncertainty around accumulating risk

Future work could focus on individual study findings, or evaluate the pre-policy risk assessment from a pure customers' perspective. A current theme would be to examine the post-insurance effects on a customers' environment, or in-depth on market growth and check any possible relation to the industries affected by the NIS Directive.

Annex A: Questionnaire and Metrics Map




The following questionnaire was utilised to receive feedback for Chapter 3, and was aimed towards Insurance companies with a current cyber insurance offering, focusing on the risk assessment phase of potential clients.
























A.1 Questionnaire

- Q1. What are the most impactful criteria (or questions) by which a potential customers' risk is assessed?
- Q2. Does your cyber insurance offering target **all**, or a **particular set** of business sector(s)?
- a. If a particular set, please enumerate the ones it does (e.g. Communications, Financial Services, Retail, etc.).
- Q3. Does your cyber insurance offering conduct the same risk assessment for all business sectors?
- Q4. Does your cyber insurance offering cover all, or a particular set of risks?
- a. If a particular, please enumerate the ones it does (e.g. data breach, data leakage, insider threat etc.).
- Q5. Does your cyber insurance offering **require or recommend** a particular **standard or good practice** for assessing the risk of a potential client?
- a. If yes, please identify and describe in a few words.
- b. If no, please name any standards or good practices you might have under consideration.
- Q6. Does your cyber insurance offering have an auditing requirement for a potential client?
- a. If yes, please provide details such as whether it is internal or external, and if any requirement(s) exist (e.g. being accredited, etc.).
- Q7. Does your cyber insurance offering face certain challenges regarding the risk assessment of potential clients?
- a. Examples:
- i. Conducting due diligence, i.e. to ensure that no breach has occurred before creating a policy.
- ii. Utilizing breach history or threat intelligence, i.e. to assess the magnitude of past, or probability of future breaches.

A.2 Risk Assessment: Metrics Map

Legend

Metric that insurers were found to:	be missing	
	use in addition to what was expected	
	have in place	

<ul style="list-style-type: none"> • Dedicated Resources <ul style="list-style-type: none"> ○ Validate the presence of leadership roles with Information Security focus <ul style="list-style-type: none"> ▪ Examine if they have any responsibilities irrelevant to Information Security ○ Check whether the CISO (or equivalent) reports directly to the CEO ○ Measure the amount and quality of resources that a company invests on Information Security ○ Enumerate the number of employees that are dedicated to Information Security 	    
<ul style="list-style-type: none"> • Policies and Procedures <ul style="list-style-type: none"> ○ Validate the existence of a comprehensive and formal Information Security program <ul style="list-style-type: none"> ▪ Confirm it covers technical, administrative and physical measures for data protection ▪ Ensure the appropriate provisions for the security of mobile devices and teleworking ○ Evaluate the cyber security maturity of the organisation ○ Check whether cyber security standards are followed ○ Existence of an Incident Response procedure, DRP, BCP ○ Evaluate the Security and privacy policy and its' integration within company structure ○ Compliance with HIPAA, ISO, PCI-DSS, SOX and reports of these ○ Query the existence of a policy for social media presence, or published information <ul style="list-style-type: none"> ▪ Verify whether there is a legal review for publishing new content in social media ○ Presence of Certifications, or any own assessments that rely on one ○ Detail the frequency of any external audits that might be in place 	          
<ul style="list-style-type: none"> • Employee Awareness <ul style="list-style-type: none"> ○ Verify the existence of a formal security awareness program <ul style="list-style-type: none"> ▪ Check whether phishing exercises are taking place as part of it <ul style="list-style-type: none"> ○ Enumerate the actions (or rewards) that are taken (or offered) to employees who repeatedly fail (or succeed) these 	   
<ul style="list-style-type: none"> • Incident Response <ul style="list-style-type: none"> ○ Verify the existence of a formal incident response program <ul style="list-style-type: none"> ▪ Confirm there are regular exercises in support of it ▪ Company tolerance level towards withstanding several incidents 	  
<ul style="list-style-type: none"> • Security Measures <ul style="list-style-type: none"> ○ Confirm the proper implementation of: Business Continuity Planning, data classification, data retention, access control, log monitoring, intrusion detection, network segmentation, network monitoring, vulnerability management, and penetration testing ○ Receive information about any existing encryption strategy and the technologies involved ○ Number of solutions in place (data backups, antivirus, patching, firewall, IDS, secure remote access, secure connectivity, secure cloud) ○ Defined physical access 	     
<ul style="list-style-type: none"> • Vendor Management <ul style="list-style-type: none"> ○ Verify the existence of a formal third party management process <ul style="list-style-type: none"> ▪ Receive details on: due diligence, ongoing oversight, and contractual obligations 	 
<ul style="list-style-type: none"> • Board Oversight <ul style="list-style-type: none"> ○ Detail the frequency of reporting cyber-security risk issues and related action to the board ○ Detail any existing board-level approval of oversight of the Information Security Program ○ Receive details of the organisations' internal information flow related to cyber-security, lines of communication, including crisis communication plans ○ Managements' awareness of crucial information security issues 	    



ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece



TP-04-16-979-EN-N



PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-178-6
doi: 10.2824/065381

