Deloitte.

Cyber Value at Risk in the Netherlands

10 billion value lost through cyber risk in The Netherlands

Deloitte.

www.stateofthestate.nl

Insights drive performance Everywhere analytics

Preface

In the year 1609, during a period of extraordinary economic growth from naval trade that the Dutch refer to as “the Golden Age”, the Dutch legal scholar Hugo the Groot introduced the principle of Mare Liberum. Mare Liberum (Latin for “open sea”) is the term used in international law to designate the principle of free trade at sea.

According to this principle oceans and seas belong to everyone and all countries should have free access to the sea for travel and trade. The principle was hotly contested over the next few centuries, but it eventually led to a set of rules that, when properly enforced, have made naval trading into one of the worldwide drivers of economic growth.

This principle also applies to the communication network that is the source of growth in the information age: Internet Liberum. However, similar to all the different traders and nations sailing the seas during the Golden Age, we will have to fight for a safe and free cyberspace today. Certain individuals abuse the freedom and openness of the Internet by hacking into systems to steal and disrupt. The same things that make the Internet so valuable also make it vulnerable.

With great freedom comes great responsibility. To grow, you need to create as much safe space as possible. All organizations that navigate cyberspace need to take their responsibility and join forces in the battle against evil through a distributed network where everything is connected and nobody is in charge. If we are vigilant and respond effectively to attacks, we can keep the pirates at bay. If we organize our defenses, we can navigate, create and do business in a safe and open cyberspace.

In this spirit, the World Economic Forum launched its initiative “Risk & Responsibility in a Hyper-connected World” in 2011. One of the key initiatives to enable cooperation and information sharing between organizations was to create a shared cyber risk model. Together with the Forum, and with the input of hundreds of international experts, business and policy leaders in cyber risk management, this eventually led to our report on Cyber Risk Quantification and the introduction of the Cyber Value at Risk concept early 2015.

We have transformed the concepts developed with the Forum into an operational model to quantify cyber risk. As a first application of this model, our team has determined the quantitative impact of cyber risk on organizations in the Dutch sectors with largest risk exposure. This report presents the results of this endeavor. It provides insights in cyber risk in the Netherlands and enables Dutch organizations to benchmark their exposure against industry averages.

We believe that organizations should continue to strengthen their Cyber Risk Management strategy, policies and controls, both in terms of prevention as well as detection and response. We encourage Dutch organizations to use this model to quantify their cyber risks and share, discuss and interpret the results. We hope this leads to more effective cyber security investments as well as collaboration on improving the model. In the spirit of tending a shared space, we cordially invite you to join our community and further develop this model with us. We look forward to become your partner to ensure your portfolio of security investments is balanced and enables your organization to innovate with confidence.
We hope you enjoy reading this report.

Jacques Buith
Risk Services Leader - The Netherlands

Executive Summary

Information technology enables economic growth and creates value for organizations in all sectors. As technologies develop exponentially, it is a strategic imperative for your organization to accelerate its innovation by making your business technology-enabled and information-based. The increasing amount of data this generates creates value and in turn empowers employees and customers through easy-to-use information technology.

With this strategic value, your organization increasingly and unavoidably takes on risk of information abuse: confidential information may end up in the wrong hands, your ICT systems may get disrupted or, if certain information gets changed, you may lose control over your assets or product quality. This information abuse could lead to value loss for your organization, this is cyber risk. Such value losses would constitute either loss of intangible value (like market share or product quality) or loss of tangible value (like stolen cash or additional expenses through claims, fines and recovery).

Your organization needs to responsibly balance the strategic value of innovation with the unavoidable cyber risk this brings. This requires insight into the potential value loss and for this reason we have developed the Cyber Value at Risk (VaR) model. It is based on the Value-at-Risk concept widely used in managing investment risk. In essence, Cyber VaR estimates how much value might be lost in a "worst case" scenario, i.e. when it exceeds a typical or expected loss through cyber risk. This is important, because the Cyber VaR can be much higher than the expected value loss, thus identifying the level of uncertainty.

The Cyber VaR model is a work in progress. We encourage you to apply this method to your organization and compare your results with the outcomes presented in this report. We are keen to exchange the resulting insights and experience as this will lead to further improvements of the model benefiting everyone.

Overall, our major findings are as follows:

- For the Dutch economy as a whole, the expected value loss is about €10 billion annually, or 1.5% of GDP, in line with earlier studies. This is apparently the price we pay for our transition to a more digital and on-line economy, which also brings tremendous benefits to society.
- For most large Dutch organizations, the uncertainty from cyber risk is significant, but not critical. The potential value loss in a "worst case" scenario is typically 8 times higher than the expected value loss.
- Our study finds that the sectors with the highest cyber risk are Technology & Electronics, Defense & Aerospace, Public, and Banking (see page 13).

Our study also shows that a significant part of the value loss from cyber risk goes undetected or unreported. Using the Cyber VaR model, we estimated that information abuse leading to disruptions creates almost half of the total value loss (€4.6bn) for the Dutch economy. Another example of value loss that is hard to detect and little reported concerns reduced control over assets and products. This amounts to an expected loss of €1.5bn for the Dutch economy, about half of which occurs in the Public Sector. This is associated with pollution from mass (or "commodity") crime activity as well as abuse for cyber espionage and concerns integrity of our communications as well as control over public assets such as roads, bridges, and water-locks.

Cyber espionage also leads to the loss of Intellectual Property (€1.5bn) and Strategic Information (€1bn). This is value loss that is hard to detect and underreported[1]. Cases reported in the media are the tip of the iceberg. This leads to value loss in particular for the Technology & Electronics and Defense & Aerospace sectors. For both these sectors, the Cyber VaR is about 17% of their income, a significant amount and much higher than other sectors. For the Defense & Aerospace sector, this is partly caused by the fact that organizations in this sector are relatively small compared to other sectors[2]. Such abuse becoming public could be devastating for an organization, as confidentiality is an imperative in this sector.

Two other sectors bear high cyber risk mainly due to potential abuse of Third-party or Privacy-related Information. For the Business & Professional Services sector, the Cyber VaR is about 5% of income, which is 5 times higher than their expected value loss. For the Banking sector, Cyber VaR is about 7% of their income, which is 18 times larger than their expected value loss, which is a significant increase versus other sectors. In the event that a significant breach becomes public, organizations in these sectors, that have trusted and regulated relations with their clients, may effectively lose their license to operate.

Most attackers behind value loss through information abuse are well organized. They share information and attack methods through highly specialized criminal networks. Improving Cyber Resilience in the Netherlands also requires being organized through knowledge sharing and specialized cyber security services. All sectors would benefit from such cooperation to decrease cyber risks. This starts by properly investigating incidents and sharing information about abuse so we all learn from the problems that individual organizations encounter. Since we are all vulnerable, it is a sign of strength to share lessons learned on how we resolved these vulnerabilities.

We see the positive trend that organizations are preparing for a possible breach and understand that what limits the worst case value loss is the quality of how they respond to such a breach. The next step is to further improve collaboration between organizations in cyber defense.

In summary, we encourage organizations to:

1. Carefully assess where and how they may lose value in case of information abuse, also bearing in mind the potential longer term or intangible value loss;
2. Take responsibility for your part in the collective by responsibly sharing insights into cyber risk management;
3. Consciously make cyber risk transparent and quantify it - to take risk and unlock more value from innovation -by using the Cyber VaR model.

If you believe your organization can benefit from applying this quantitative lens to cyber security investments, we cordially invite you to join our community and further develop this model together.

1 See for instance https://www.aivd.nl/onderwerpen/cyberdreiging/inhoud/economische-cyberspionage

2 Smaller organizations tend to have smaller amounts of (valuable) information. Therefore, attackers can more effectively (i.e. quickly) locate and abuse the information they target. This effect should also be held in mind when applying our results to smaller organizations in other sectors.

Content

Introduction

Entrepreneurship implies taking risk. Reaping the benefits of digital technologies is no different. The automation, scaling, and now also cognitive, benefits of technology enable new ways of value creation at a rate seemingly unparalleled in history. However, the same applies to the "business models" of criminals, spy agencies, terrorists and activists. Understanding the size and nature of this threat to your organization is key to unlocking the potential value of digital technologies.

Motivation

Our mission is to make a positive, meaningful impact on society. As accountant and advisor, assessing and quantifying risk is in our DNA. By providing a comprehensive quantitative overview of the magnitude and nature of the economic consequences of cyber risk for Dutch organizations, we provide the information that helps organizations to make rational decisions related to cyber security investments. It also enables organizations to focus their efforts where they have the most impact. In this way, we believe we are taking an important step towards making cyberspace safe.

New vulnerabilities and cyber incidents appear in the media every day. However, the magnitude of cyber risks is often abstract and difficult to grasp. How much should be invested in cyber security? Does a technology company need to be as concerned as a telecommunication provider? What quantitative data provides a basis to select and prioritize investments in cyber risk management? The work Deloitte carried out with the World Economic Forum leading to the 2015 report "Towards the Quantification of Cyber Threats" introduced the "Cyber Value at Risk" concept. This report is a first for its application.

What is cyber risk?

For the purpose of this report, the term cyberspace means the collective of connected technologies. Cyber risk is defined as "the risk that an adversary abuses corporate information assets, with direct or indirect financial consequences". Our scope does not include human error, "rogue insiders" (i.e. malicious insiders operating independently of outsiders) or "natural disasters" such as the flooding of a datacenter.

Usage of this report

We have performed our analysis for the largest sectors in The Netherlands using a specially developed methodology based on common practices in financial risk management, our knowledge of each sector, as well as our extensive case work in advising large organizations about the management of cyber risk.

The normalized risk levels for each sector, as reported on the following pages, allow organizations to estimate their own level of cyber risk for each information asset. In using this report, it is important to be aware of its limitations. Results represent the largest organizations within each sector and are less accurate for smaller organizations, as well as somewhat atypical organizations within their sector (e.g. a purely online shop in retail). Results become more accurate when assumptions are tailored to your organization. Another important point is that we have analyzed the cyber risk for stand-alone organizations. Spillover effects from one firm to another across value chains have not been taken into account. In other words, we have not included correlation or diversification effects caused through a shared dependence on a critical infrastructure, for example. We aspire to include this perspective in future work.

The Dutch cyber landscape

Dutch sectors and organizations

In our analysis, taking data from the Dutch Central Bureau for Statistics (CBS) as a starting point, we have chosen the 14 largest sectors of the Dutch economy in terms of gross income as well as those with the largest exposure to cyber risk.

The Financial Services sector, often reported as a single sector, contains organizations with very different business models and thus different cyber risk exposures. For this reason, we have split this sector into three: Insurance, Banking, and Asset Management combined with Pensions.

For the Public Sector, we picked a combination of Healthcare, Education, and Central Government excluding Defense, which is included in the Defense & Aerospace sector. We have left these three sub-sectors separate for the purpose of the analysis. Where relevant, specific results per sub-sector can be found on the Public Sector results page.

Not covered in this report

Sectors that in our experience have a limited exposure to cyber risk or that are rather small, such as Leisure, Real-estate, and Construction, have not been extensively analyzed nor included in this report. Other relevant (sub-)sectors not covered in this report are Local Government and Small & Medium Enterprises (SME). We of course recognize that other values outside economic impact, such as the integrity of legal and democratic systems and public safety, are relevant for some sectors, especially for the Public Sector. However, these are also not in scope for our analysis.

Sector	Gross income (€bn)[3]	Percentage of GDP(%)
Oil, Gas & Chemicals	720	108%
Public Sector	389	58%
Wholesale & Retail	245	37%
Asset Management & Pensions	227	34%
Insurance	141	21%
Consumer Goods	130	19%
Banking	99	15%
Telecom	65	10%
Technology & Electronics	42	6%
Business & Professional Services	36	5%
Transportation	33	5%
Media	27	4%
Utilities	25	4%
Defense & Aerospace[4]	20	2%
Covered in this report	2,199	328%

3 According to annual statements of largest organizations within each sector.
4 Estimated number including Public Sector defense spending.

The Dutch state of cyber security

On average, the cyber security of organizations in The Netherlands is relatively mature when compared to countries with a similar threat profile[5]. Security is encoded in various laws and regulations such as the "Wet Computercriminaliteit" and the "Wet Bescherming Persoonsgegevens". Dutch policies are contained in the National Cyber Security Strategy as well as a Defense Cyber Strategy, which are both implemented by the National Cyber Security Center (NCSC). The Netherlands has many international partnerships with European and global organizations.

It is hard to accurately determine the cyber security of Dutch organizations based on public data. Standardized metrics for performance are lacking and not reported on, however, useful metrics can be found through extensive literature analysis. The annual Cyber Security Assessment Netherlands (CSAN) by the NCSC also provides useful figures. From our literature study of over 250 scientific and professional publications, we have inferred the maturity for each sector, which we have validated with our Deloitte sector experts as well as with our team of around 180 security experts with hands-on experience.

From this analysis, a couple of observations stand out. First of all, cyber security maturity levels tend to be higher for larger and heavily regulated organizations. This effect is further amplified when the organization in question is multinational. Another important factor is experience with cyber threats. As a result we observe that the Banking sector, the Oil, Gas & Chemicals sector, key components of Central Government as well as the Defense & Aerospace sector are relatively mature. On the other hand, most Small or Medium Enterprises (SMEs) as well as organizations in the Education, Healthcare and Utilities sectors have lower than average maturity levels.

Organizations may influence each other in their cyber maturity. For instance, all organizations benefit from the relatively mature state of cyber security of payments, leading to better Liquidity Integrity for all organizations. This explains the relatively low impact on Liquidity Integrity for all organizations, despite high threat levels.

We distinguish four main layers of cyber security controls: (I) prevention from entry (vulnerability management, firewalls, etc.), (II) detection and response (security monitoring and analytics, incident response, etc.), (III) prevention of abuse (e.g. encryption, data loss prevention, identity and access management), and finally, (IV) recovery of losses (business continuity management, crisis management, communications, legal, etc.). Maturity in all four layers is required to obtain optimal security. With the help of our quantification methodology, optimizing cyber security for individual organizations is also in reach.

The maturity level of cyber capabilities for an organization is of key importance to seize the opportunities of cyberspace while limiting the impact of potential cyber incidents. Organizations with a higher level maturity take risks with more confidence and are better able to innovate, or win and retain the trust of their customers. The efforts required for realizing a certain maturity level do not exactly scale with the size of the organization.

The cyber threat landscape

Overall, threat levels are apparent from cyber threat intelligence reports. Furthermore, we distinguish between threat profiles only to the extent that they are attracted to other information assets or utilize different tactics.
Based on threat intelligence reports as well as our own research, we make a distinction between fast and slow attackers. The rationale behind this is that sophisticated attackers often make use of highly specialized methods combined with an incentive to go undetected for as long as possible, while slowly accumulating abuse.

Less sophisticated attackers on the other hand take advantage of known exploits and have an incentive to act as fast as possible to take advantage of the delay in the defender's reaction. These attackers are by nature also more opportunistic, moving on to the next target with the same method until they find a vulnerable defender.

Another important characteristic that sets threat profiles apart is the type of information assets that are targeted. Some attackers focus on strategically important information assets, while others aim at disruption of Operational Continuity. Based on these insights, we defined four threat profiles displayed in the table on the next page.

5 Dutch Global Cybersecurity Index score 0.6765, ranked 6th according to ITU [54] and endorsed by the World Economic Forum [8]. Also see: www2.deloitte.com/nl/nl/pages/risk/articles/eu-voorzitter-loopt-op-dun-ijs-als-cyber-security-gidsland.html.

Threat profile	Sophistication	Abuse rate	Main targets
Espionage	High	Low	Strategic Information, Intellectual Property
Advanced Crime	High	Low	Liquidity Integrity, Strategic Information
Mass Crime	Low	High	Liquidity Integrity, Privacy-related Information
Disturbance	Low	High	Operational Continuity

It is no surprise that highly sophisticated threat profiles constitute the most significant part of the reported security incidents (CSAN). We also see a significant impact from these groups in our report.

With all threat profiles, we assume they will also target all other information assets, only significantly less than their main target. Attribution of the threat profiles to the individual sectors is proportional to the size of the information asset. The only exception to this is the Espionage profile; this profile may value some information assets far higher than reflected by the value impact to the organization. The perspective of Espionage is strategic with a big incentive for stealth.

Advanced Crime refers to highly organized and sophisticated groups with primarily a financial motive, preferring a large, well-prepared heist, while being opportunistic about other potentially valuable information assets. Part of this profile is assumed to target Strategic Information for the purpose of insider trading.

Mass Crime on the other hand has a low level of sophistication and thus generally utilizes a relatively standard set of tools that they deploy very widely to identify the “low hanging fruit” across many organizations. This includes use of malware, phishing, ransomware and others. As a side-effect from the many failed attempts by Mass Crime, loss of Operational Continuity and Control Integrity may occur.

Politically or ideologically motivated actors are classified under the Disturbance profile. Their main intent is to disturb operations of an organization and thus critical systems are targeted to compromise availability or integrity. In some cases, an actor in this profile is found to publish confidential information with the same intent to disturb an organization’s operation (possibly obtained by accident).

Value impact from abuse

Impact on economic value as a consequence of cyber threats follows from abuse of information assets. These information assets are a somewhat abstract notion, since information may be in multiple places at once, in transit as well as stationary. Information assets are different between organizations and even more so between sectors, so generalized categories for information assets are required to enable comparative analysis.

We have defined a list of seven information assets that relate to all potential forms of abuse, listed in the table to the right.

Information asset	Threat description	Main value impact
Operational Continuity	Availability of ICT systems related to operations, including income	Income
Control Integrity	Control over non-cash assets or customer products (unwittingly) lost	Assets
Intellectual Property	Competitive advantage from investment into IP (partially) lost	Equity
Strategic Information	Loss of company confidential information may lead to (M&A) opportunity loss and impair growth	Growth
Third Party Information	Leakage of confidential information on third parties may lead to loss of clients	Market share
Privacy-related Information	Confidential information on persons (including employees) may lead to loss of customers and talent	Market share
Liquidity Integrity	Financial transactions that are initiated or altered by cyber fraudsters may lead to direct financial losses	Liquidity

In estimating the value impact in case an information asset is abused, we took two factors into account: direct value impact as listed in the table as well as losses through claims and fines. The type of claims and fines vary between the information assets and the jurisdiction the organization is exposed to.

Note that it may take time before the value impact materializes. In case of Operational Continuity or Liquidity Integrity, losses are immediate, but with other information assets, it may take time before the loss gets uncovered and even then, it may still go unreported. In case of Third Party or Privacy-related Information assets, this may limit the value impact, but for the other information assets value is lost regardless.

The base value of the information asset (i.e. the business case leading to its existence) as well as indirect effects have not been included. This concerns reputational damage, impact on societal values, personal lives or impact on third parties such as with critical infrastructure. We recognize these effects are important, and aspire to perform further research to include these factors in the future.

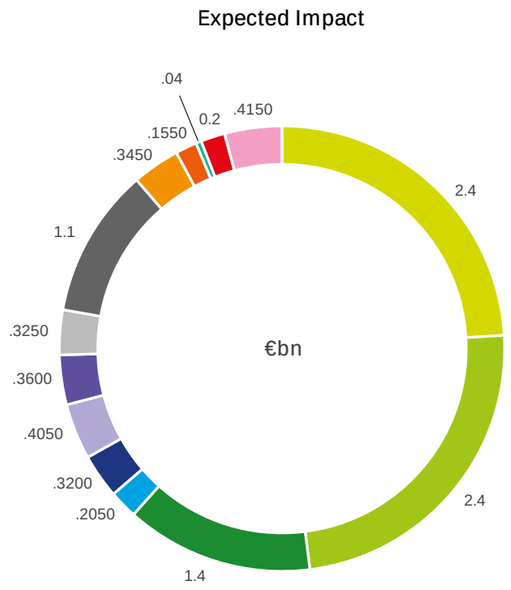
Based on threat levels related to cyber capabilities maturity per organization, we determined the value impact for each information asset. From this impact, we also determined the risk on solvency and creditworthiness of organizations. For this purpose, we assess the Cyber VaR against three different criteria:

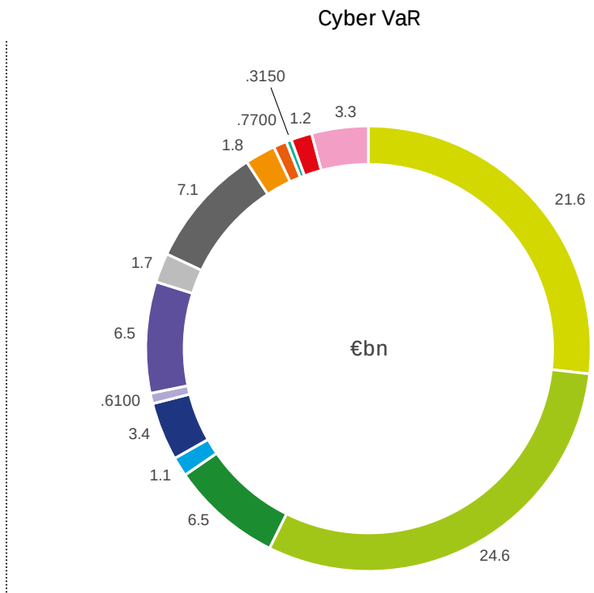
- Complete loss of equity leading to insolvency
- Equity over debt ratio worsens to 15% below sector average, impairing creditworthiness
- Losses exceeding three times annual profits, also impairing creditworthiness

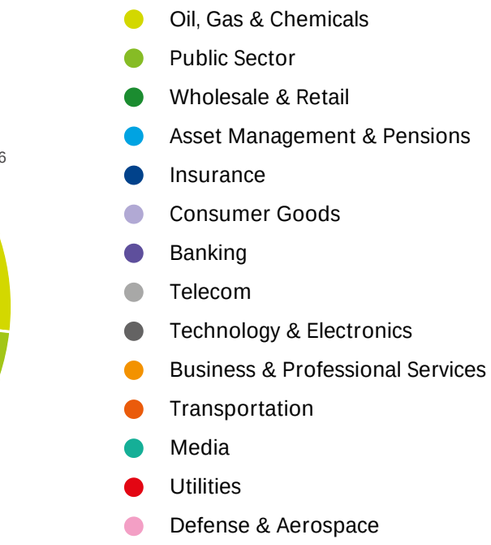
Attribution of impact

Value loss by sector

The absolute expected impact from cyber risk is not equally distributed over the sectors.
The pie-chart in the top-left corner displays the expected impact attributed per sector. This is the graph we use as reference for the results per sector.
In the top-right corner, a pie-chart displays the Cyber VaR per sector. Cyber VaR is a measure for the losses that occur with a low probability. Interdependencies between organizations have not been taken into account.
Sectors represented by less than 5% have been accumulated into the “Other” category.

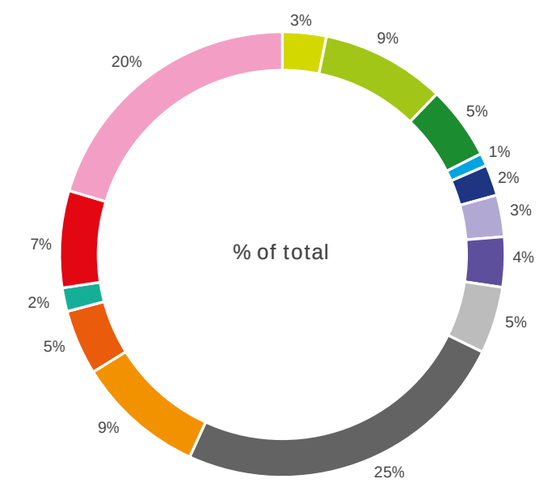


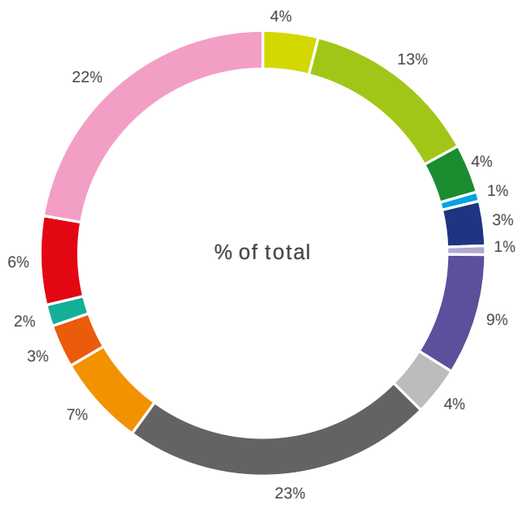




Value loss relative to income

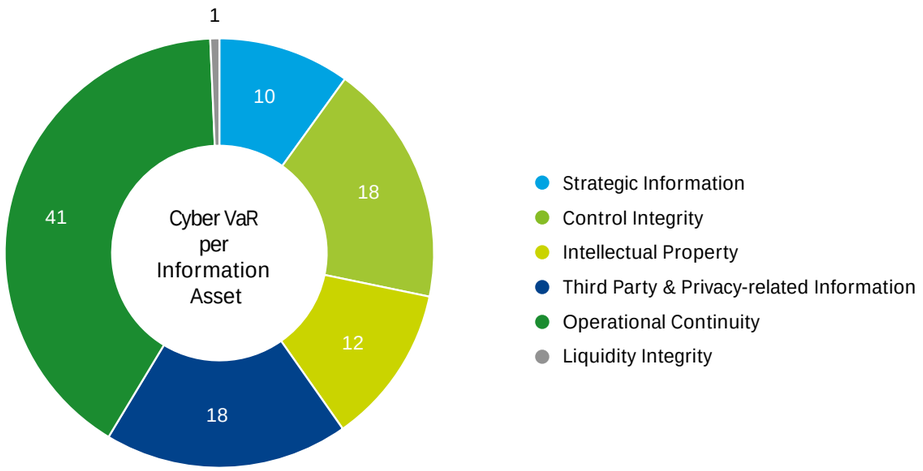
Cyber risk affects certain sectors more strongly than others. This can be seen from the value loss per income (in parts per thousand or ‰).
In the bottom-left corner, the pie-chart displays the expected impact per income, indicating which sectors experience the high expected cyber risk.
In the bottom-right corner, the pie-chart displays the Cyber VaR per income for each sector.
Sectors represented by less than 5% have been accumulated into the “Other” category.

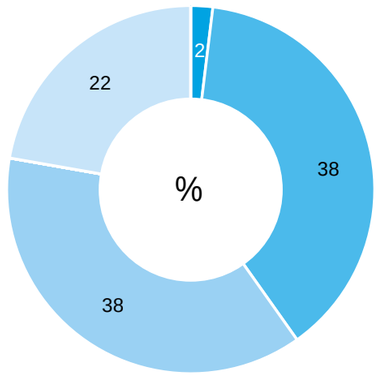


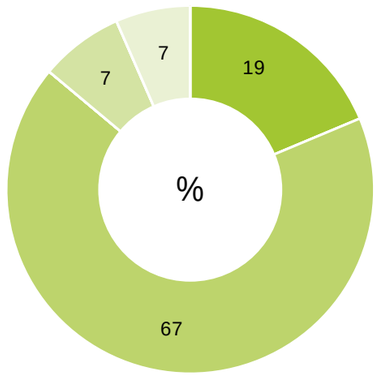


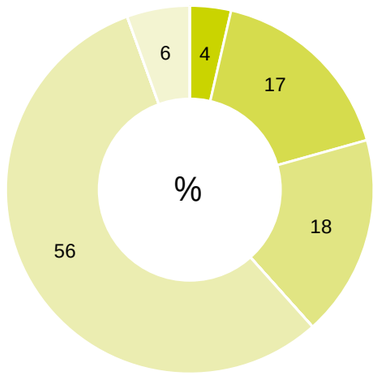
Attribution per information asset

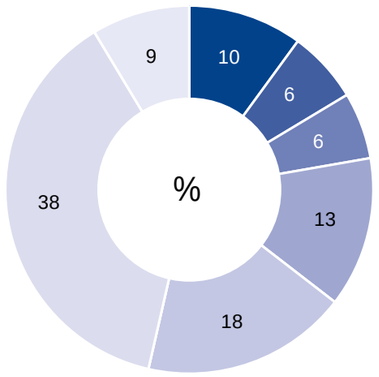
The contribution of each information asset to the combined Cyber VaR over all organizations is depicted in the donut-chart in the middle of the page. To see the sectors that most contribute to the Cyber VaR for each Information Asset, we displayed the attribution to the sectors in the surrounding pie-charts (largest information assets only).

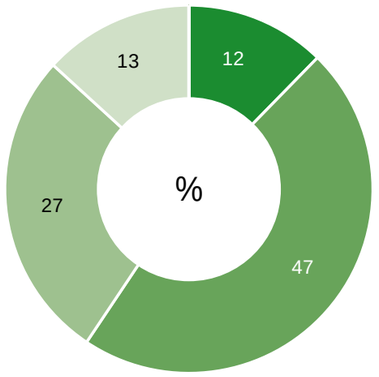












Sectors with highest cyber risk

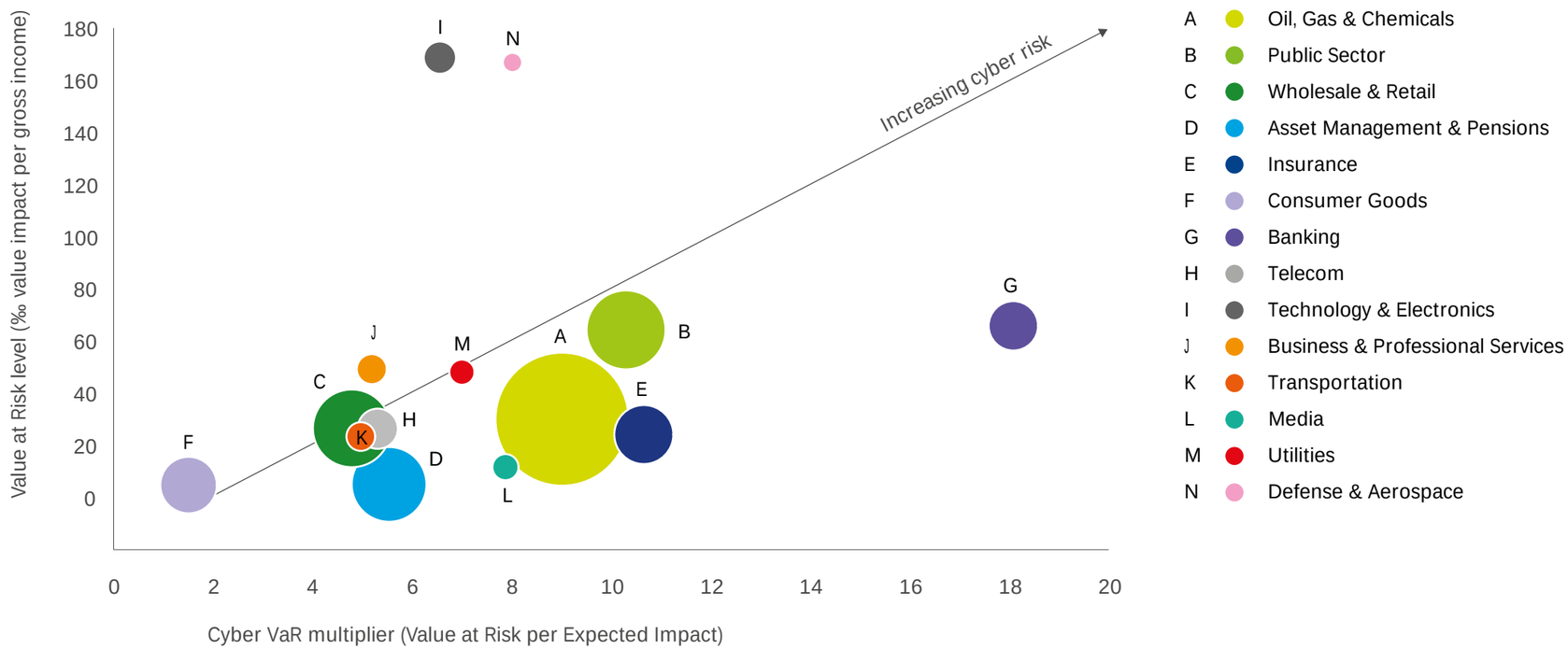
For a worst case event, there are two types of risk:

1. Cyber VaR per income is high(this is given by the Cyber VaR level,y-axis in the bubble graph);

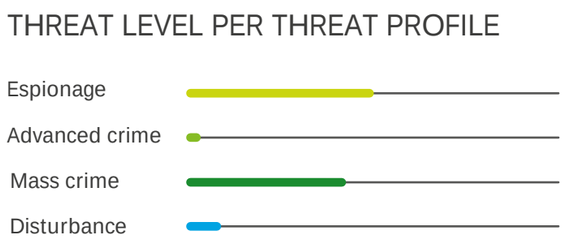
2. Cyber VaR is far higher than the expected value loss (this is given by the Cyber VaR multiplier, x-axis in the bubble graph).

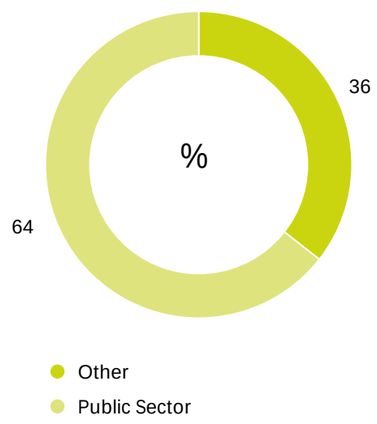
In the bubble graph on the right, we have plotted all the sectors against these two types of risk. The size of the bubble indicates the total amount of income for each sector.

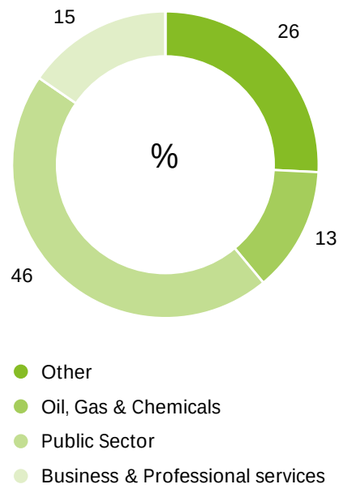
What we observe from the bubble graph is that sectors with the highest cyber risk are the Technology & Electronics, Defense & Aerospace, Public, and Banking sectors. Analysis shows that this is mainly because these sectors attract more Threat Profiles through their particularly valuable information assets.

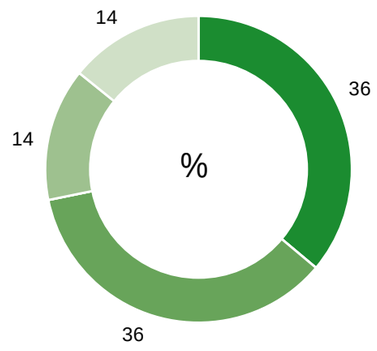


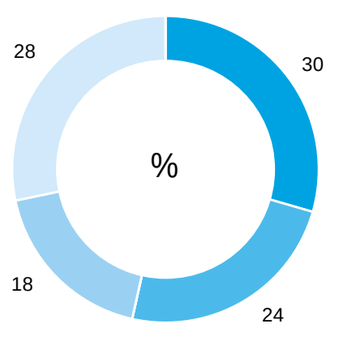
Cyber VaR per Threat profile and sector









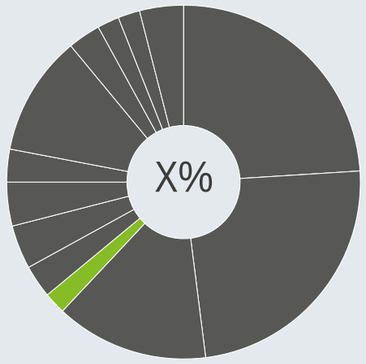


Interpretation guide

This text contains the main observations for each sector.

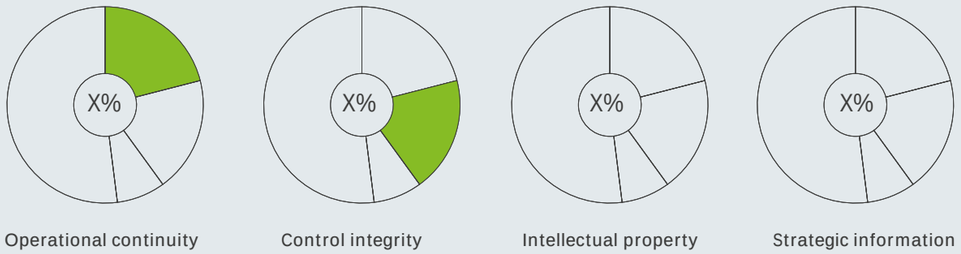
SECTOR IMPACT

INDUSTRY		
GROSS INCOME	€ XXX	BILLION (X%)
EXPECTED VALUE LOSS	€ X.X	BILLION (X%)
CYBER VAR	€ X.X	BILLION (X%)



Impact for the total sector
% is of all sectors.

INFORMATION ASSET IMPACT

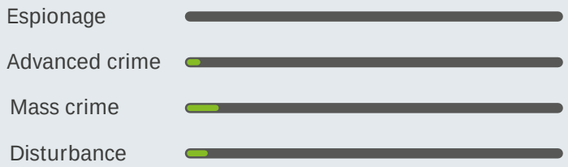


This overview provides a graphical summary of cyber risk.

THREAT OVERVIEW

This overview identifies the net threat level per threat profile relative to other sectors.

THREAT LEVEL PER THREAT PROFILE



This table provides a quantitative summary of the exposure per Information Asset. By multiplying the exposure with gross income an organisation specific exposure can be obtained. The Cyber Var multiplyer at the bottom is the ratio between the Cyber VaR and Expected impact.

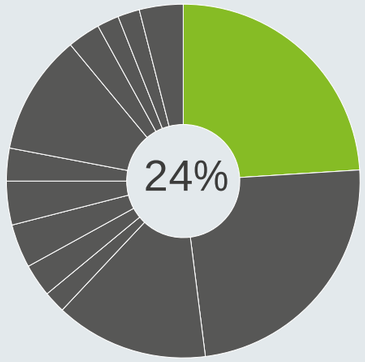
This area contains the most important considerations and observations that follow from our analysis of the results.

Oil, Gas & Chemicals

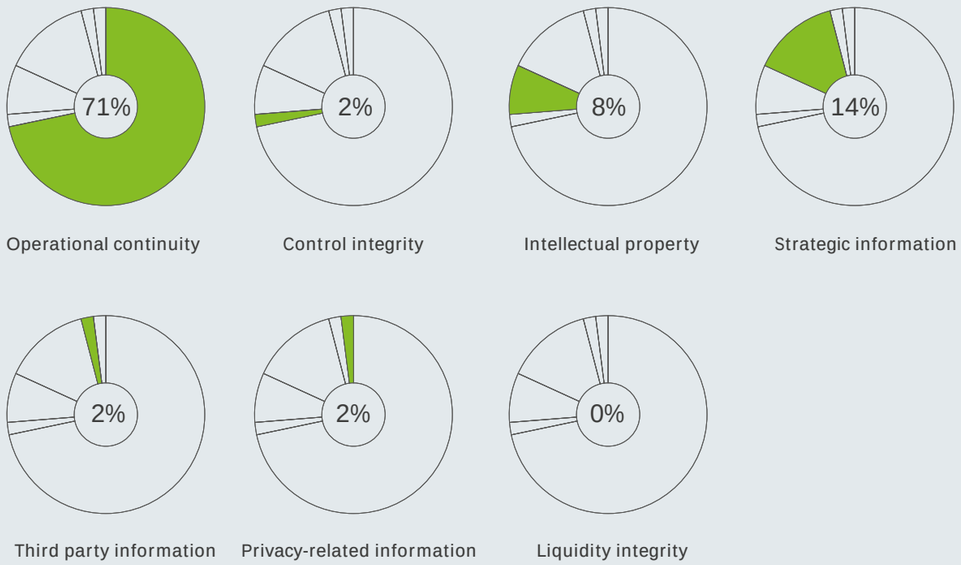
Oil, Gas & Chemicals is a large part of the Dutch economy and has relatively high maturity. Companies within the sector rely heavily on their critical systems which causes Operational Continuity to be one of their main concerns.

SECTOR IMPACT

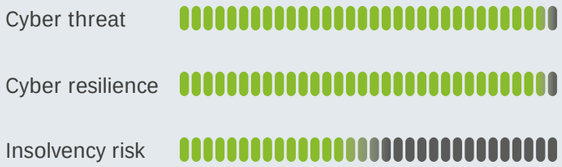
OIL, GAS & CHEMICALS		
GROSS INCOME	€ 720	BILLION (33%)
EXPECTED VALUE LOSS	€ 2.4	BILLION (24%)
CYBER VAR	€ 21.6	BILLION (27%)



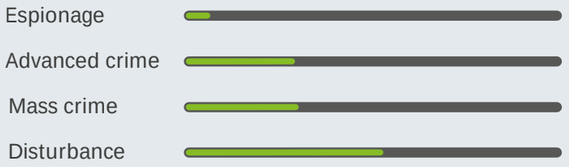
INFORMATION ASSET IMPACT



THREAT OVERVIEW



THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Operational continuity	2.3	21.4
Control integrity	0.1	0.7
Intellectual property	0.4	2.3
Strategic information	0.5	4.3
Third party information	0.1	0.7
Privacy-related information	0.0	0.6
Liquidity integrity	0.0	0.0
Total	3.3	30.0

Cyber VaR multiplier (expected : cybervar =) 9

SECTOR CONSIDERATIONS AND OBSERVATIONS

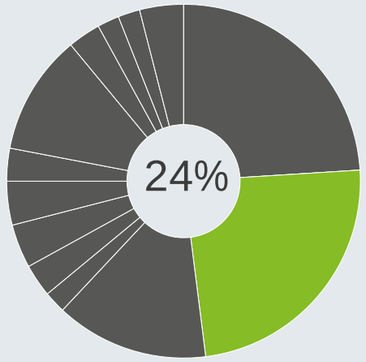
- The cyber security for this sector is mature because threat levels have already been high for quite some time.
- Operational Continuity and Strategic Information lead to approximately 85% of the total risk within this sector.
- Disruption of Operational Continuity can have an especially high impact if production facilities are concerned.
- The value of Strategic Information for this sector is quite high given the sensitive and confidential knowledge of natural resource locations.

Public Sector

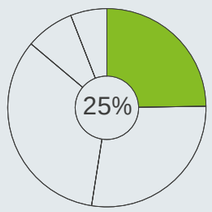
The Public Sector is attractive for all threat profiles. It therefore requires elevated cyber security capabilities. Lower cyber security levels for Education and Healthcare lead to significant risks for Intellectual Property and Privacy-related Information, respectively.

SECTOR IMPACT

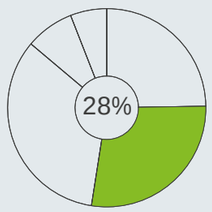
PUBLIC SECTOR		
GROSS INCOME	€ 389	BILLION (18%)
EXPECTED VALUE LOSS	€ 2.4	BILLION (24%)
CYBER VAR	€ 24.6	BILLION (31%)



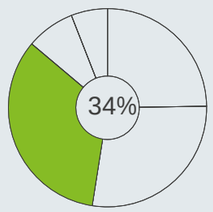
INFORMATION ASSET IMPACT



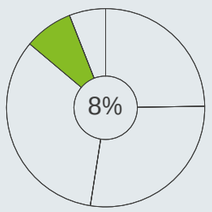
Operational continuity



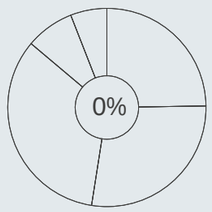
Control integrity



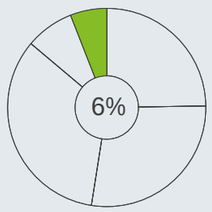
Intellectual property



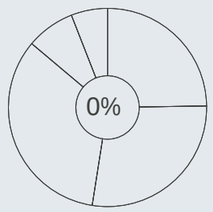
Strategic information



Third party information

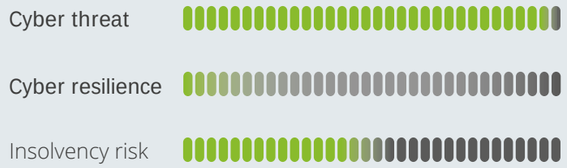


Privacy-related information

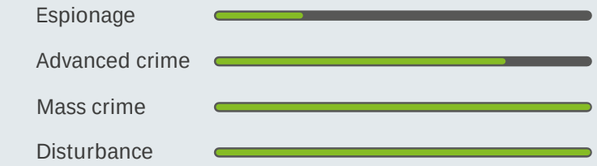


Liquidity integrity

THREAT OVERVIEW



THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Operational continuity	2.3	23.1
Control integrity	2.0	25.6
Intellectual property	0.6	4.4
Strategic information	1.0	7.7
Third party information	0.0	0.1
Privacy-related information	0.2	2.1
Liquidity integrity	0.0	0.2
Total	**6.1**	**63.2**

Cyber VaR multiplier (expected : cybervar =) 10

SECTOR CONSIDERATIONS AND OBSERVATIONS

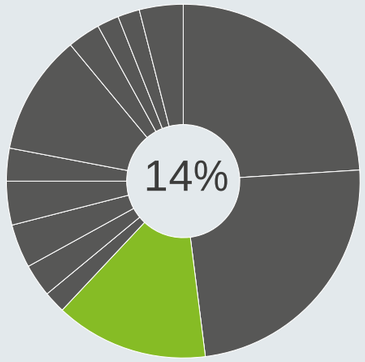
- Loss of Operational Continuity such as with the tax office or social benefits agencies would have a significant impact.
- Lack of Control Integrity of public infrastructure such as bridges, tunnels and water works would have a large impact.
- Given that the Public Sector processes vast amounts of Privacy-related Information, the resulting value impact is still relatively limited.
- The Public Sector is privy to large amounts of commercially sensitive Strategic Information leading to a significant Cyber VaR.
- Most of the threat in Intellectual Property stems from Education.
- Over half of the threat in Privacy-related Information stems from Healthcare.

Wholesale & Retail

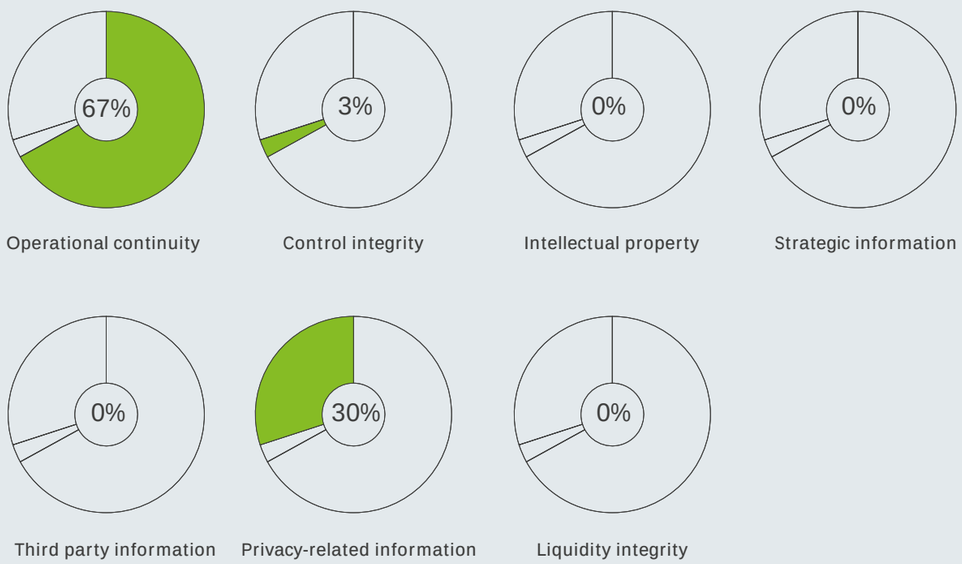
For Wholesale & Retail, the largest risk is interruption of business operations, followed by customer churn for some companies in case of a privacy breach. Maintaining integrity of operations is of utmost importance.

SECTOR IMPACT

WHOLESALE & RETAIL		
GROSS INCOME	€ 245	BILLION (11%)
EXPECTED VALUE LOSS	€ 1.4	BILLION (14%)
CYBER VAR	€ 6.5	BILLION (8%)

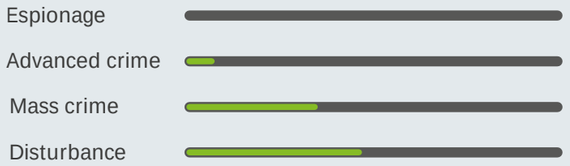


INFORMATION ASSET IMPACT



THREAT OVERVIEW

THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Operational continuity	4.0	17.6
Control integrity	0.1	0.8
Intellectual property	0.0	0.0
Strategic information	0.0	0.0
Third party information	0.0	0.0
Privacy-related information	1.4	7.9
Liquidity integrity	0.0	0.0
Total	5.5	26.5

Cyber VaR multiplier (expected : cybervar =) 5

SECTOR CONSIDERATIONS AND OBSERVATIONS

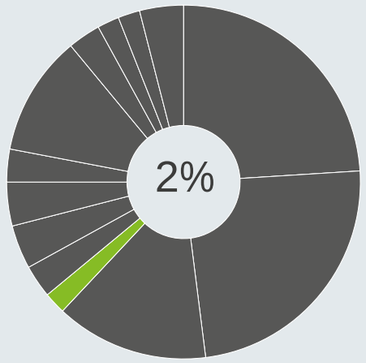
- Operational Continuity has the highest risk exposure.
- The risk on Operational Continuity depends on the length of the supply chain and will vary between companies.
- The Wholesale sector has little exposure from personal data, dampening the overall impact on Privacy-related Information for this sector.

Asset Management & Pensions

The Asset Management & Pensions sector is primarily exposed to Operational Continuity and Privacy-related Information as it forms a possible target for cyber Disturbance and Mass Crime.

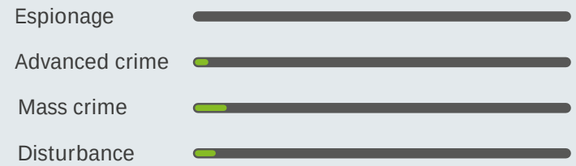
SECTOR IMPACT

ASSET MANAGEMENT & PENSIONS		
GROSS INCOME	€ 227	BILLION (10%)
EXPECTED VALUE LOSS	€ 2.4	BILLION (2%)
CYBER VAR	€ 1.1	BILLION (1%)



THREAT OVERVIEW

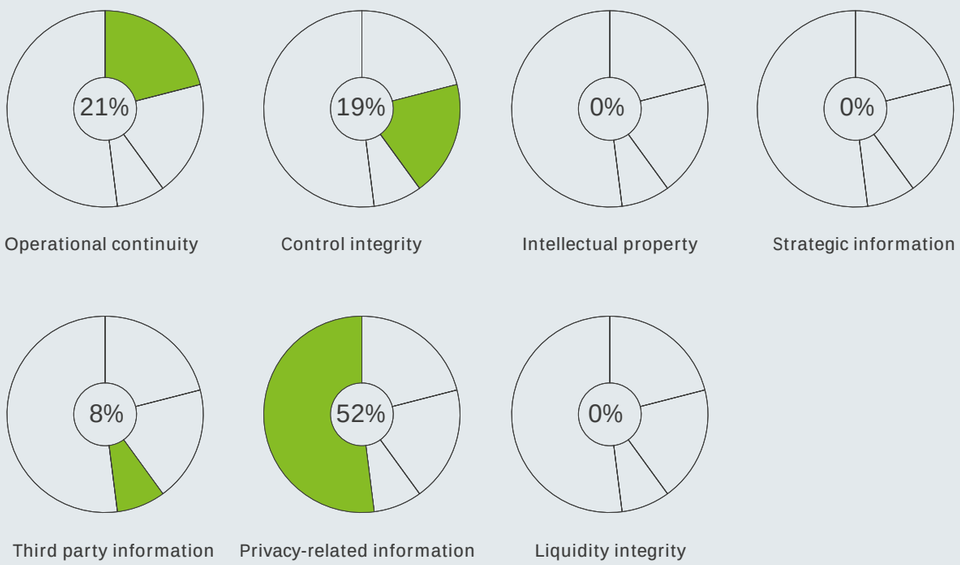
THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Operational continuity	0.2	1.1
Control integrity	0.2	0.9
Intellectual property	0.0	0.0
Strategic information	0.0	0.0
Third party information	0.1	0.4
Privacy-related information	0.5	2.6
Liquidity integrity	0.0	0.0
Total	0.9	5.0

Cyber VaR multiplier (expected : cybervar =) 6

INFORMATION ASSET IMPACT



SECTOR CONSIDERATIONS AND OBSERVATIONS

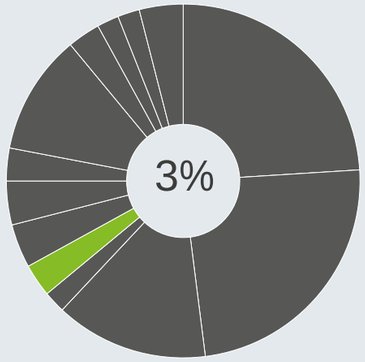
- The value exposure for pension funds is relatively small, but given the large size of the Dutch pension sector, the absolute impact is still significant.
- Liquidity Integrity impact is low, given high risk awareness of personnel and sound risk controls, so fraudulent transactions should stand out quickly.
- Operational Continuity primarily concerns Asset Management, while Privacy-related Information primarily concerns Pensions.

Insurance

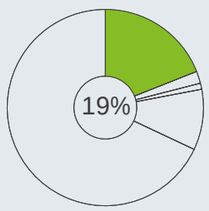
Health insurance firms will primarily be targeted for their Privacy-related Information. Operational Continuity of the asset and liability management, required to keep financial exposure low, is also under threat.

SECTOR IMPACT

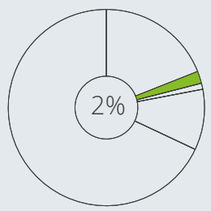
INSURANCE		
GROSS INCOME	€ 141	BILLION (6%)
EXPECTED VALUE LOSS	€ 0.3	BILLION (3%)
CYBER VAR	€ 3.4	BILLION (4%)



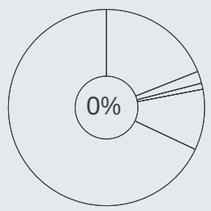
INFORMATION ASSET IMPACT



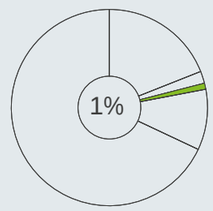
Operational continuity



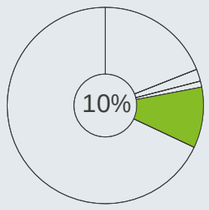
Control integrity



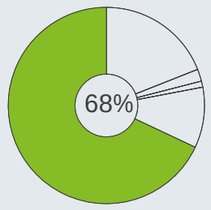
Intellectual property



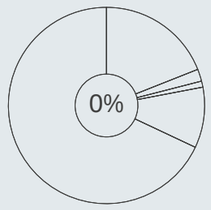
Strategic information



Third party information

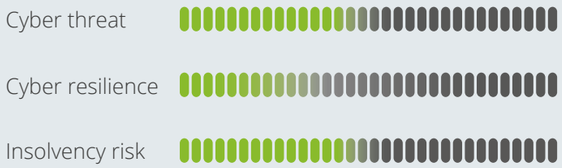


Privacy-related information

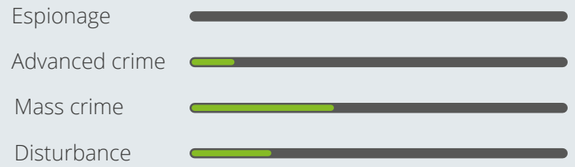


Liquidity integrity

THREAT OVERVIEW



THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Operational continuity	1.0	4.5
Control integrity	0.1	0.5
Intellectual property	0.0	0.0
Strategic information	0.0	0.1
Third party information	0.5	2.5
Privacy-related information	0.7	16.5
Liquidity integrity	0.0	0.0
Total	**2.3**	**24.1**

Cyber VaR multiplier (expected : cybervar =) **11**

SECTOR CONSIDERATIONS AND OBSERVATIONS

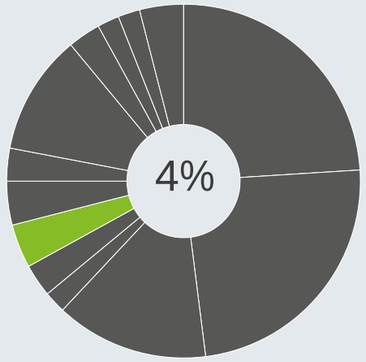
- A breach of Privacy-related Information can have a high impact, especially for large health insurance firms.
- Operational Continuity could harm life insurance firms in particular, given their large exposure on financial markets.
- Given the stringent demands from Solvency II, any impact from a cyber breach will have impact on an insurance firm's solvency position.

Consumer goods

The Consumer Goods sector produces perishable goods and depends heavily on spot market trading. Therefore, disruption of Operational Continuity provides the main risk. Incident response focusing on swift process restauration is of vital importance.

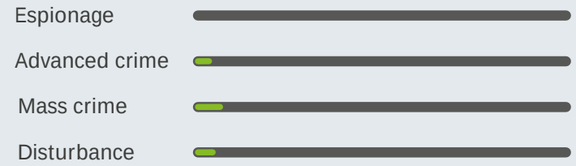
SECTOR IMPACT

CONSUMER GOODS		
GROSS INCOME	€ 130	BILLION (6%)
EXPECTED VALUE LOSS	€ 0.4	BILLION (4%)
CYBER VAR	€ 0.6	BILLION (1%)



THREAT OVERVIEW

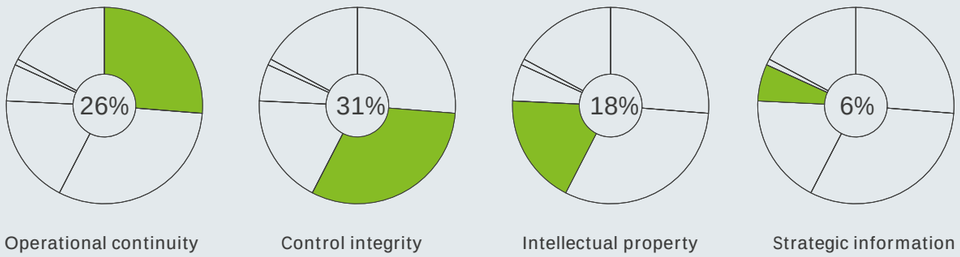
THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Operational continuity	1.4	1.2
Control integrity	0.9	1.5
Intellectual property	0.6	0.8
Strategic information	0.1	0.3
Third party information	0.0	0.0
Privacy-related information	0.2	0.8
Liquidity integrity	0.0	0.0
Total	3.1	4.7

Cyber VaR multiplier (expected : cybervar =) 2

INFORMATION ASSET IMPACT



SECTOR CONSIDERATIONS AND OBSERVATIONS

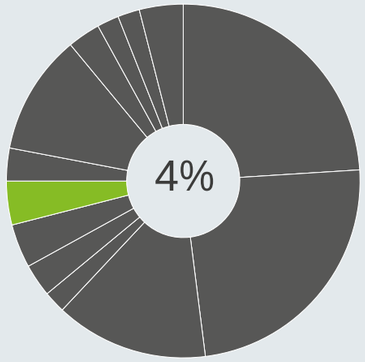
- Control Integrity is a relatively exposed asset because the scale of operation demands a high amount of process automation.
- Cyber-attacks on Strategic Information may have a substantial impact due to the high level of competition in the sector.
- Damage related to Privacy-related Information is caused primarily by claims of employees in case of HR leaks. Third Party Information is not considered a liability since this mostly constitutes supplier agreements.

Banking

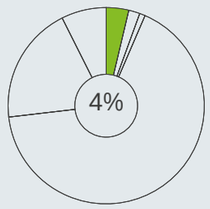
The Banking sector has a relatively high maturity, which is unsurprising as its Liquidity Integrity is an attractive target. Furthermore, Operational Continuity could become a more critical factor, especially if it persists for a longer period.

SECTOR IMPACT

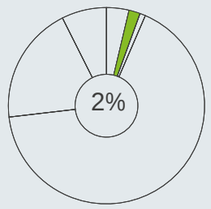
BANKING			
GROSS INCOME	€	99	BILLION (5%)
EXPECTED VALUE LOSS	€	0.4	BILLION (4%)
CYBER VAR	€	6.5	BILLION (8%)



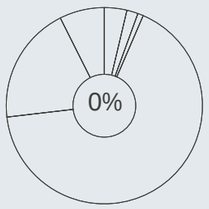
INFORMATION ASSET IMPACT



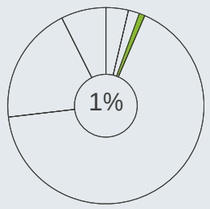
Operational continuity



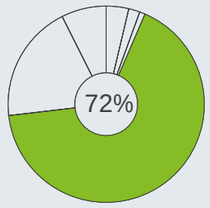
Control integrity



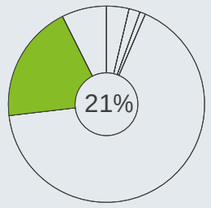
Intellectual property



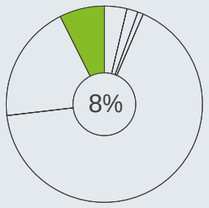
Strategic information



Third party information



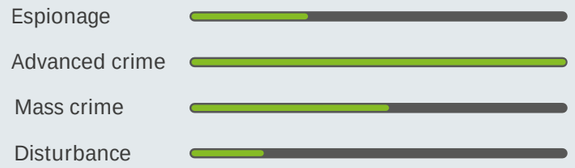
Privacy-related information



Liquidity integrity

THREAT OVERVIEW

THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Value exposure (in € mn per € bn revenue)		
Operational continuity	0.2	2.3
Control integrity	0.1	1.5
Intellectual property	0.0	0.0
Strategic information	0.0	0.6
Third party information	2.7	43.8
Privacy-related information	0.5	12.8
Liquidity integrity	0.3	4.7
Total	3.6	65.7

Cyber VaR multiplier (expected : cybervar =) 18

SECTOR CONSIDERATIONS AND OBSERVATIONS

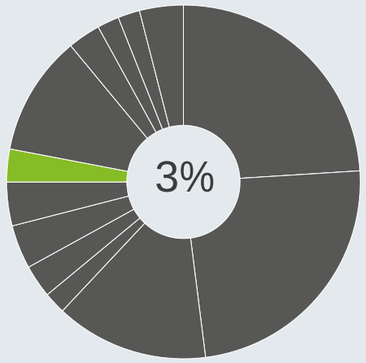
- Liquidity Integrity still plays a big role for the Cyber VaR in spite of the high level of cyber security.
- A breach of Third party Information would have significant impact, given that the license to operate as a commercial bank could be impaired. For Privacy-related Information this is similar.
- The impact on solvency in case of a significant cyber event is potentially quite high due to the stringent capital regulations and oversight.

Telecom

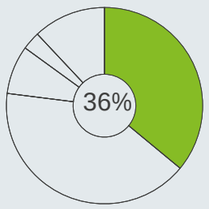
The core business of the Telecom sector is to provide undisturbed services to their customers. Therefore Operational Continuity and Control Integrity pose the largest risk. Mitigation efforts could include mutual services agreements with other operators.

SECTOR IMPACT

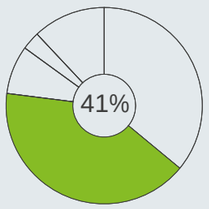
TELECOM			
GROSS INCOME	€	65	BILLION (3%)
EXPECTED VALUE LOSS	€	0.3	BILLION (3%)
CYBER VAR	€	1.7	BILLION (2%)



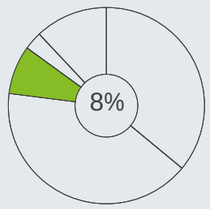
INFORMATION ASSET IMPACT



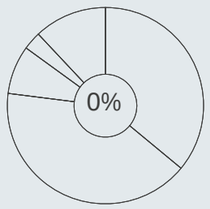
Operational continuity



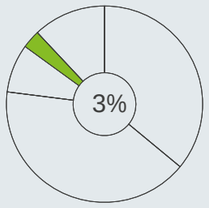
Control integrity



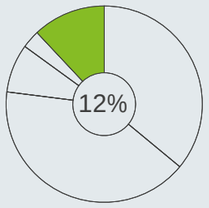
Intellectual property



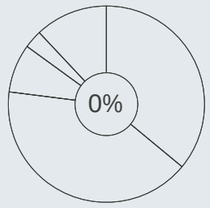
Strategic information



Third party information



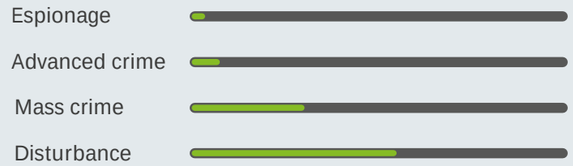
Privacy-related information



Liquidity integrity

THREAT OVERVIEW

THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Operational continuity	3.3	9.3
Control integrity	0.9	10.7
Intellectual property	0.5	2.1
Strategic information	0.0	0.1
Third party information	0.1	0.8
Privacy-related information	0.2	3.2
Liquidity integrity	0.0	0.0
Total	4.9	26.2

Cyber VaR multiplier (expected : cybervar =) 5.3

SECTOR CONSIDERATIONS AND OBSERVATIONS

- Operational continuity and Control Integrity generate a lot of value for this industry, which includes internet, telephony and cloud services.
- Cyber VaR for Control Integrity is far higher than the expected impact given its fundamental importance and value for this sector (the Belgacom hack is an excellent example, see for instance http://tinyurl.com/z397oyf).
- Impact on Privacy-related Information would primarily be caused by loss of customer (meta-)data, leading to increased customer churn.

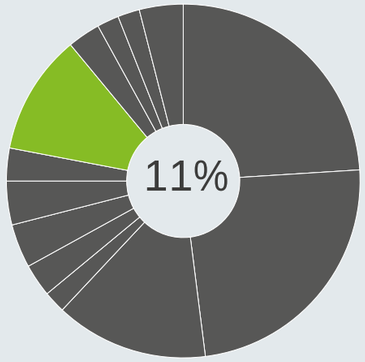
Technology & Electronics

Technology & Electronics is primarily exposed through its sizable R&D investments. Loss of Operational Continuity would amount to manufacturing interruptions, while products require sound Control Integrity to maintain their value for customers.

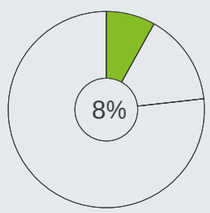
SECTOR IMPACT

TECHNOLOGY & ELECTRONICS

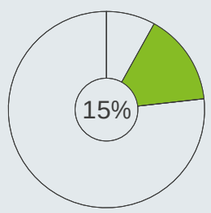
GROSS INCOME	€	42	BILLION (2%)
EXPECTED VALUE LOSS	€	1.1	BILLION (11%)
CYBER VAR	€	7.1	BILLION (9%)



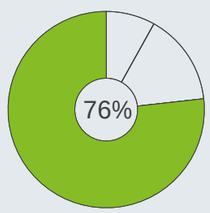
INFORMATION ASSET IMPACT



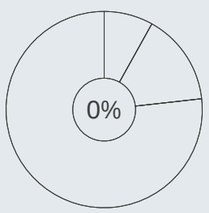
Operational continuity



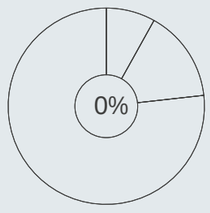
Control integrity



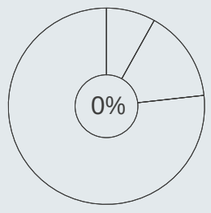
Intellectual property



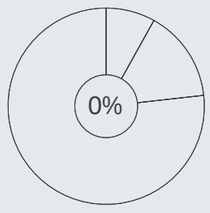
Strategic information



Third party information



Privacy-related information



Liquidity integrity

THREAT OVERVIEW

THREAT LEVEL PER THREAT PROFILE

INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Operational continuity	2.8	13.7
Control integrity	4.4	25.6
Intellectual property	18.4	128.3
Strategic information	0.0	0.1
Third party information	0.0	0.1
Privacy-related information	0.0	0.2
Liquidity integrity	0.0	0.0
Total	25.6	168.2

Cyber VaR multiplier (expected : cybervar =) 7

SECTOR CONSIDERATIONS AND OBSERVATIONS

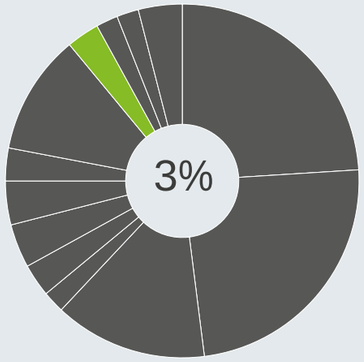
- Creditworthiness is at risk in case the Cyber VaR materializes.
- Lost Intellectual Property may constitute a breach of export controls resulting in fines, which have been included in the value impact.
- Impact of Control Integrity violation is based on a period of two weeks during which potential damages go unnoticed.
- Improvement of quality controls as well as reducing time to market for innovations would best mitigate these risks.
- Impact from Strategic Information is small because of limited M&A activity.

Business & Professional services

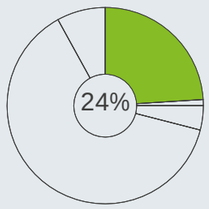
The Business & Professional Services sector is mainly exposed by the risk of losing their license to operate in the event that highly confidential information is leaked on a large scale (personal as well as third parties). Loss of Operational continuity is also impactful.

SECTOR IMPACT

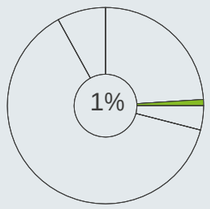
BUSINESS & PROFESSIONAL SERVICES			
GROSS INCOME	€	36	BILLION (2%)
EXPECTED VALUE LOSS	€	0.3	BILLION (3%)
CYBER VAR	€	1.8	BILLION (2%)



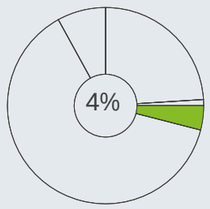
INFORMATION ASSET IMPACT



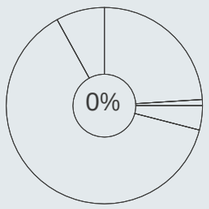
Operational continuity



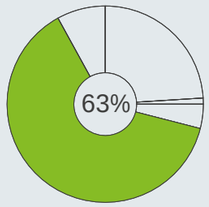
Control integrity



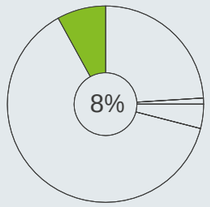
Intellectual property



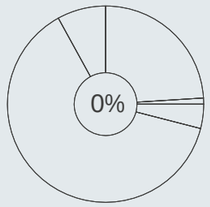
Strategic information



Third party information



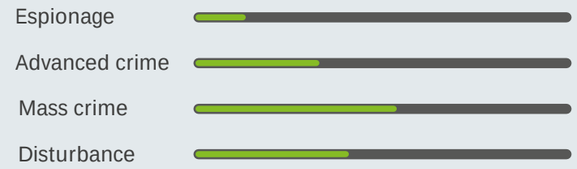
Privacy-related information



Liquidity integrity

THREAT OVERVIEW

THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Operational continuity	2.5	11.6
Control integrity	0.0	0.3
Intellectual property	0.1	2.1
Strategic information	0.0	0.0
Third party information	6.2	31.2
Privacy-related information	0.7	3.8
Liquidity integrity	0.0	0.0
Total	9.4	48.9

Cyber VaR multiplier (expected : cybervar =) 5

SECTOR CONSIDERATIONS AND OBSERVATIONS

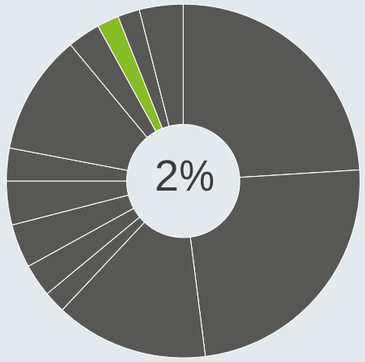
- The Business & Professional Services sector contains business-oriented services such as consulting as well as personnel-related services such as staffing agencies.
- Staffing agencies have more Privacy-related Information while business-oriented services more Third party information.
- All Business & Professional Services share a similar and average level of exposure to the risk of business disruption.
- This sector has a high insolvency risk if the Cyber VaR is lost because of low amounts of equity relative to churn.

Transportation

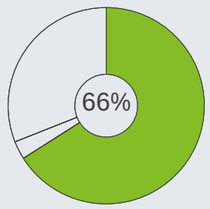
The greatest risk for the Transportation sector lies in interruption of business operations due to cyber Disturbance or Mass Crime activity. Privacy-related Information may also lead to significant value loss given the sensitive information in travelling records.

SECTOR IMPACT

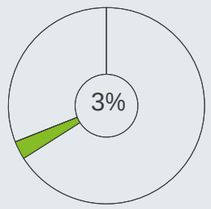
TRANSPORTATION			
GROSS INCOME	€	33	BILLION (2%)
EXPECTED VALUE LOSS	€	0.2	BILLION (2%)
CYBER VAR	€	0.8	BILLION (1%)



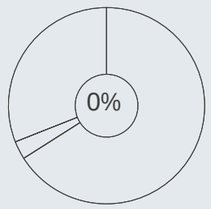
INFORMATION ASSET IMPACT



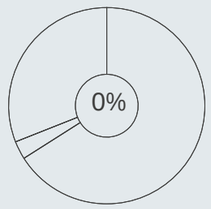
Operational continuity



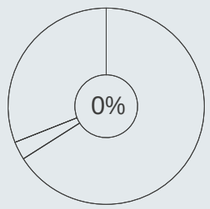
Control integrity



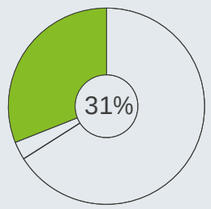
Intellectual property



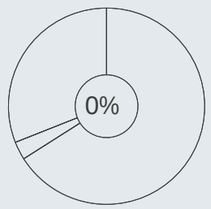
Strategic information



Third party information

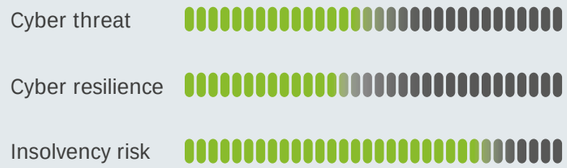


Privacy-related information

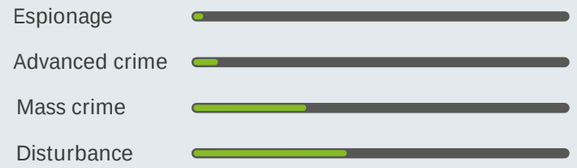


Liquidity integrity

THREAT OVERVIEW



THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Operational continuity	3.4	15.2
Control integrity	0.0	0.6
Intellectual property	0.0	0.0
Strategic information	0.0	0.0
Third party information	0.0	0.0
Privacy-related information	1.2	7.2
Liquidity integrity	0.0	0.0
Total	4.6	23.0

Cyber VaR multiplier (expected : cybervar =) 5

SECTOR CONSIDERATIONS AND OBSERVATIONS

- Logistics are quite sensitive to value loss in case of delays, explaining relatively high impact from potential loss of Operational Continuity.
- Low profit margins in the Transportation sector cause cyber disruptions to quickly impact the solvency position.
- Like elsewhere, startups possessing their own Intellectual Property are gaining ground in The Netherlands, but do not contribute to the Intellectual Property risk since their gross income is still small.

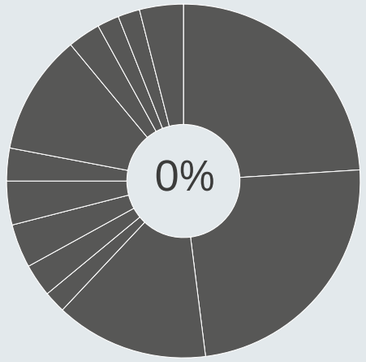
Media

The Media sector is mainly exposed through its Control Integrity and Operational Continuity related to the reliability of media contents. The remaining exposure stems from the value drivers for the media contents and the high M&A activity.

SECTOR IMPACT

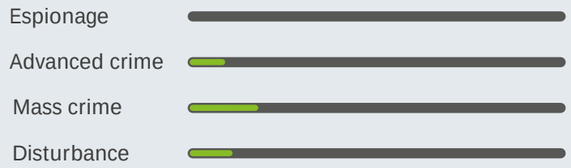
MEDIA

GROSS INCOME	€	27	BILLION (1%)
EXPECTED VALUE LOSS	€	0.0	BILLION (0%)
CYBER VAR	€	0.3	BILLION (0.4%)



THREAT OVERVIEW

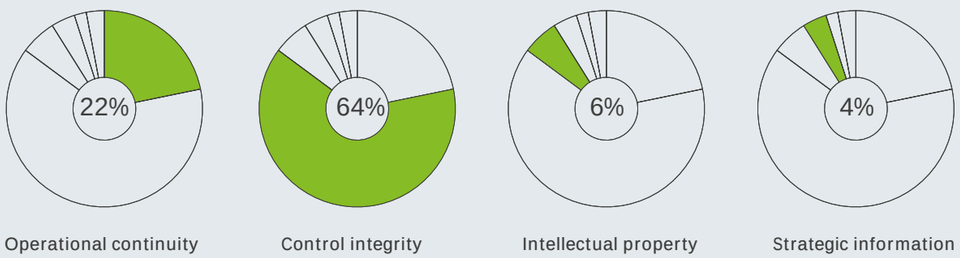
THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (‰)	CYBER VAR (‰)
Operational continuity	0.2	2.5
Control integrity	1.3	7.4
Intellectual property	0.0	0.5
Strategic information	0.0	0.4
Third party information	0.0	0.2
Privacy-related information	0.0	0.4
Liquidity integrity	0.0	0.0
Total	1.4	11.4

Cyber VaR multiplier (expected : cybervar =) 8

INFORMATION ASSET IMPACT



SECTOR CONSIDERATIONS AND OBSERVATIONS

- The amount of risk on the Media sector is relatively high, because the integrity and availability of the contents of the media is essential to its value.
- The large number of M&A deals increases its exposure on Strategic Information.
- Exposure also stems from Intellectual Property (media contents), Third Party Information (advertisers) and Privacy-related Information (source protection).

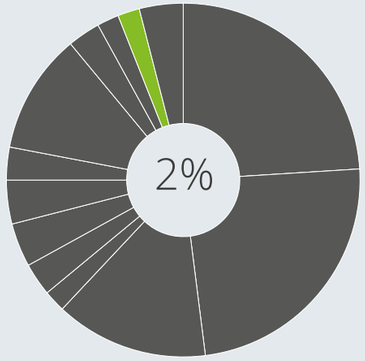
Utilities

Core business for the Utilities sector is providing The Netherlands with basic and vital needs. This makes this sector highly vulnerable for both Operational Continuity and Control Integrity abuse.

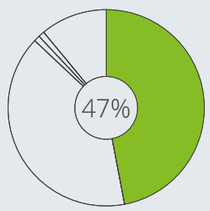
SECTOR IMPACT

UTILITIES

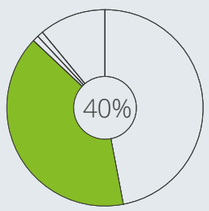
GROSS INCOME	€	25	BILLION (1%)
EXPECTED VALUE LOSS	€	0.2	BILLION (2%)
CYBER VAR	€	1.2	BILLION (2%)



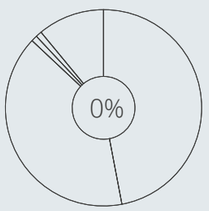
INFORMATION ASSET IMPACT



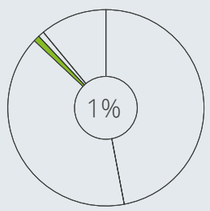
Operational continuity



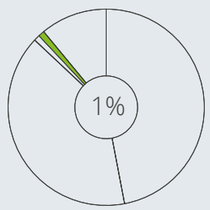
Control integrity



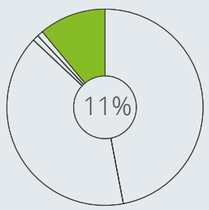
Intellectual property



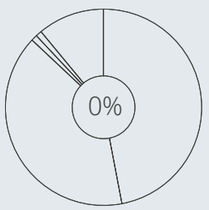
Strategic information



Third party information

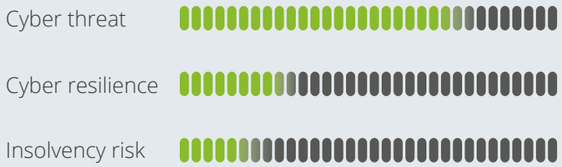


Privacy-related information

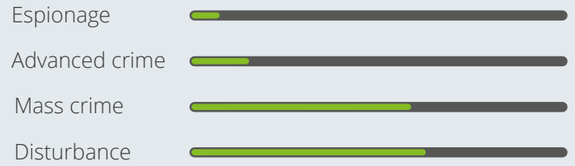


Liquidity integrity

THREAT OVERVIEW



THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (€)	CYBER VAR (€)
Operational continuity	1.2	22.3
Control integrity	4.5	19.4
Intellectual property	0.0	0.0
Strategic information	0.0	0.2
Third party information	0.0	0.2
Privacy-related information	1.2	5.4
Liquidity integrity	0.0	0.0
Total	**6.8**	**47.6**

Cyber VaR multiplier (expected : cybervar =) **7**

SECTOR CONSIDERATIONS AND OBSERVATIONS

- Results represent foremost electricity provision, given that this has the largest part to gross income.
- Given the extent of physical controls on utilities through cyberspace, the expected impact from abuse of Control Integrity is significant.
- Privacy-related exposure is small due to the monopolistic nature of the associated markets.
- The solid financial position of most utilities limits the risk for insolvency.

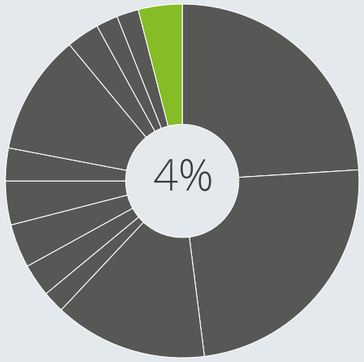
Defense & Aerospace

The Defense & Aerospace sector suffers from the strategic interest from the Espionage profile in their information assets. If a significant breach is disclosed, it may easily lead to significant losses that could terminate such firms.

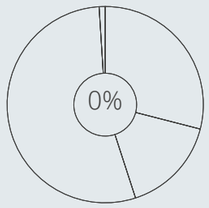
SECTOR IMPACT

DEFENSE & AEROSPACE

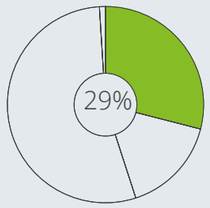
GROSS INCOME	€	20	BILLION (1%)
EXPECTED VALUE LOSS	€	0.4	BILLION (4%)
CYBER VAR	€	3.3	BILLION (4%)



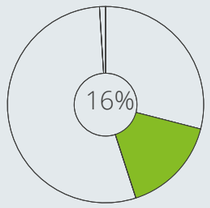
INFORMATION ASSET IMPACT



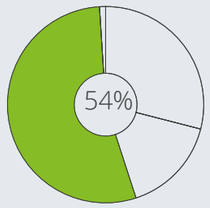
Operational continuity



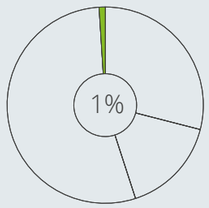
Control integrity



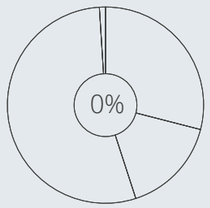
Intellectual property



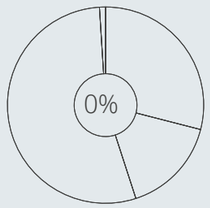
Strategic information



Third party information



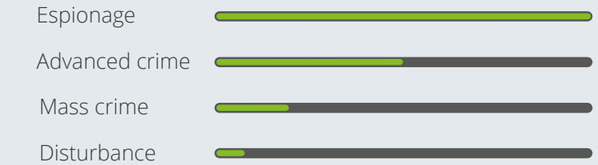
Privacy-related information



Liquidity integrity

THREAT OVERVIEW

THREAT LEVEL PER THREAT PROFILE



INFORMATION ASSETS Value exposure (in € mn per € bn revenue)	EXPECTED VALUE LOSS (€)	CYBER VAR (€)
Operational continuity	0.0	0.3
Control integrity	6.3	48.3
Intellectual property	3.3	26.7
Strategic information	11.0	89.3
Third party information	0.0	1.0
Privacy-related information	0.0	0.0
Liquidity integrity	0.0	0.0
Total	**20.7**	**165.6**

Cyber VaR multiplier (expected : cybervar =) **8**

SECTOR CONSIDERATIONS AND OBSERVATIONS

- Intellectual Property, Control Integrity of sold products as well as the Strategic Information of these organizations, are extremely valuable to nation states.
- In case such a breach would be disclosed, the value of the firm could quickly dwindle because only small customers might still rely on its products.
- Cyber VaR is disproportionate to the size of the relatively small organizations in this sector in The Netherlands. Apart from the Ministry of Defense, this would lead most organizations to insolvency.

Methodology and approach

This analysis of Cyber VaR for the Dutch economy is based on the Cyber VaR concept that Deloitte developed in collaboration with the World Economic Forum. This chapter introduces the model components, their workings and interrelations as well as the underlying assumptions.

Justification

To ensure quality and facilitate reproducibility, the model builds on previous studies in the field of cyber risk quantification and public data as much as possible. The model uses a set of logical relations to translate available data into model parameters. The scarcity of suitable cyber incident data is well known. Heuristic estimation methods are used where needed to determine parameters when data or reports were not available and have been demonstrated to be surprisingly reliable [51].

The model draws from Deloitte's insights from handling cyber incidents for our clients as well as experience gained in Deloitte's Cyber Intelligence Center. Furthermore, this report builds on the expertise of Deloitte professionals in areas ranging from cyber security, accounting to legal and HR. We have also extensively involved security experts at our clients, academia and government to validate our assumptions and methodology.

Dealing with uncertainty and Value at Risk

When dealing with risk, the expected impact does not tell the full story. When a significant event happens, the severity of the event for the organization is a major factor in actual risk assessments and decision making. The Cyber VaR concept deals with exactly this combination of expected, or average, impact and severity in the 'worst case'. More exactly, Cyber VaR determines the impact that will annually not be exceeded with a likelihood of about 95%. This implies that once in 20 years, the Cyber VaR may be exceeded with an unknown amount.

Inspired by its successful application in financial risk management, we use the same approach of (i) identifying the level of uncertainty around the expected risk and (ii) the resulting impact this uncertainty and 'worst case' impact have on an organization's value.

Due to imperfect data, this model is based on estimates and assumptions. In the Cyber VaR model these uncertainties are included by considering them as a contributor to risk in itself. The meaning of this is simple: not knowing your risk is a risk in and of itself.

"There was a statistician that drowned crossing a river... It was 3 feet deep on average."

– A random statistician joke

Model structure

In applying the Cyber VaR model, we have created a list of organizations that together comprise a large share of the Dutch economy. We collected publicly available data for each organization through their annual financial statements (or equivalent), supplemented by other public sources where needed. These organizations each fall into one of the 14 sectors. Each sector has a typical cyber security maturity profile and a certain exposure to types of cyber attacks. These attacks are performed by threat actors that have a certain way of operating and specific information assets they target. Each threat actor belongs to one of four threat profiles that characterizes their behavior.

Furthermore, we identify seven types of information assets that may be targeted (listed in the diagram above). Each threat profile targets the information assets in different ways.

Interaction between the three components "Threat profiles", "Cyber security" and "Information assets" is described by a few statements:

- Each threat profile is attracted to information assets according to the threat heat map (see table).
- Threat profiles distribute themselves over organizations proportional to the value the information asset has to them (i.e. how attracted they are to the value of an organization's assets).
- The value to the threat actor in case of abuse is assumed proportional to the value impact per information asset.
- The Espionage profile is more strongly attracted to information assets of certain sectors, indicating the perceived strategic value particular information assets may have to them.
- Threat profiles accumulate a certain level of abuse until they are either satisfied or neutralized by an organization's cyber security capabilities.

These interactions are described more in depth in the subsequent sections.

Threat heat map

Each of the four threat profiles is attracted differently to each type of information asset. The Espionage profile for instance is primarily attracted to Intellectual Property and Strategic Information. However, the ability to abuse Control Integrity or make abuse of Privacy-related or Third-party Information may also be of interest to cyber spies.

Both Advanced Crime and Mass Crime profiles are interested in cash from abusing Liquidity Integrity. Advanced Crime abuses Strategic Information to support insider trading. In addition to cash, Mass Crime profiles are after Privacy-related Information (mostly credit card data) as well as Control Integrity for the purpose of extorting an organization. As a by-product, Mass Crime can significantly impair Operational Continuity by overloading systems or infecting them with malware.

Finally, the Disturbance profile primarily targets Operational Continuity and to a lesser extent Controls Integrity and Privacy-related Information. This contributes to their primary goal of disrupting operations within an organization. Each threat profile is attracted to a small extent to all the other information assets, reflecting the somewhat unpredictable nature and motives of actual threat agents. A low attractivity in the diagram below constitutes a number 50 times lower than a high attractivity.

Threat heat map	Espionage	Advanced Crime	Mass Crime	Disturbance
Operational Continuity	L	L	M	H
Control Integrity	M	L	M	M
Intellectual Property	H	L	L	L
Strategic Information	H	M	L	L
Third Party Information	M	L	L	L
Privacy-related Information	M	L	M	M
Liquidity Integrity	L	H	H	L

Threat profiles

Each threat profile has its own level of maturity in operating (i.e. sophistication level) that determines an organizations effective level of defense against that threat profile. Based on the observed and recently modelled divide between slow and fast attacks [56], we assign either a high or a low sophistication level to the threat profiles. Espionage and Advanced Crime demand a slow approach to remain undetected and thus need a high level of sophistication. In contrast, attackers within the Mass Crime and Disturbance profiles generally have a low sophistication and act fast to optimize their gain. Although typical attacks can differ slightly from these assumptions, in general attacks can be attributed to one of these profiles.

Given the sophistication level of an attacker and its corresponding abuse rate (slow or fast), the total threat activity per type of information asset is calculated. The threat activity is then distributed according to the relative value impact for each information asset type. Simply put, this value impact determines how many attacks of a certain threat profile are carried out on the seven information assets.

The value impact for each information asset is determined per organization, based on business considerations such as the average income per sector, as well as taking into account historic cases of claims and fines in case of abuse.

We make an exception for the Espionage threat profile. Since this type of attacker is interested in information assets that are of strategic value to them, the attractivity of these assets may far exceed the actual value an information asset has to the targeted organization.

For instance, Strategic Information, Intellectual Property and Control Integrity within the Defense & Aerospace sector are highly attractive to attackers that fit into the Espionage threat profile.

Information assets

In order to determine the value impact an information asset has on an organization in case of abuse, a single question needs to be answered: what would the financial impact be in the event that the information asset would be exploited in its entirety?

For this purpose, we distinguish two factors: value impact in the form of reduced profits (either directly or in the future due to loss of sales) and costs due to claims by third parties, individuals and fines imposed by domestic or foreign regulators.

With the recent developments in privacy regulations and export controls these claims and fines can be substantial.

The direct value impact calculation differs per information asset, but generally consists of components based on yearly income, equity value and/or cash liquidity. We consider these factors in different quantities per organization depending on the sector or by using publicly available information on an organization.

Cyber defense capabilities

Based on historic events and sector specifics, the capabilities of an organization to prevent abuse of information assets by a certain threat profile is different. These defensive capabilities are divided into four cyber defense capabilities related to the attack-defense process: “prevention from entry”, “detection and response”, “prevention of abuse” and “recovery of losses”.

We then give each sector a baseline maturity score for each of these capabilities out of the five basic levels of maturity within cyber security.

The attack-defense process

About the actual process of a cyber attack, we define a simple model that has three phases: "non-criminal assessment", "criminal assessment" and "abuse". These phases are shown in the figure below.

The first (non-criminal assessment) state defines all potential attackers whom have not breached the entry barriers of an organization. These attackers could breach the first layer of defense (i.e. transitioning from non-criminal assessment to criminal assessment), depending on their level of sophistication.

Sophisticated attackers might by-pass protective barriers by utilizing backdoors, zero-day exploits or elaborate social engineering. Less sophisticated attackers might rely on phishing efforts or insider knowledge to gain access.

If an attacker transitions to the second phase of the model (criminal assessment), there is a second security function preventing abuse.

Typically the question is not whether an attacker will transition to the third phase of the model (abuse), but rather how long this will take. The detection and response capability of an organization versus the sophistication and speed of an attacker will determine this.
Less sophisticated attackers will require more time to actually abuse an information asset, leaving them vulnerable to detection.
After a certain amount of time (based on the "prevention of abuse" capability) an attacker is considered to be abusing the attacked information asset. This continues until the goal of the abuse has been reached or the abuse has been detected and neutralized.

The moment an attacker reaches the third phase of this model, losses are considered to be accumulating, and can only be diminished by the capabilities of an organization to recover from losses.

Although this model has an organization as its subject, the whole process equally applies to third parties acting as caretakers (guardians) of information for an organization. The third party's cybersecurity capabilities then become the frontline in preventing attacks.

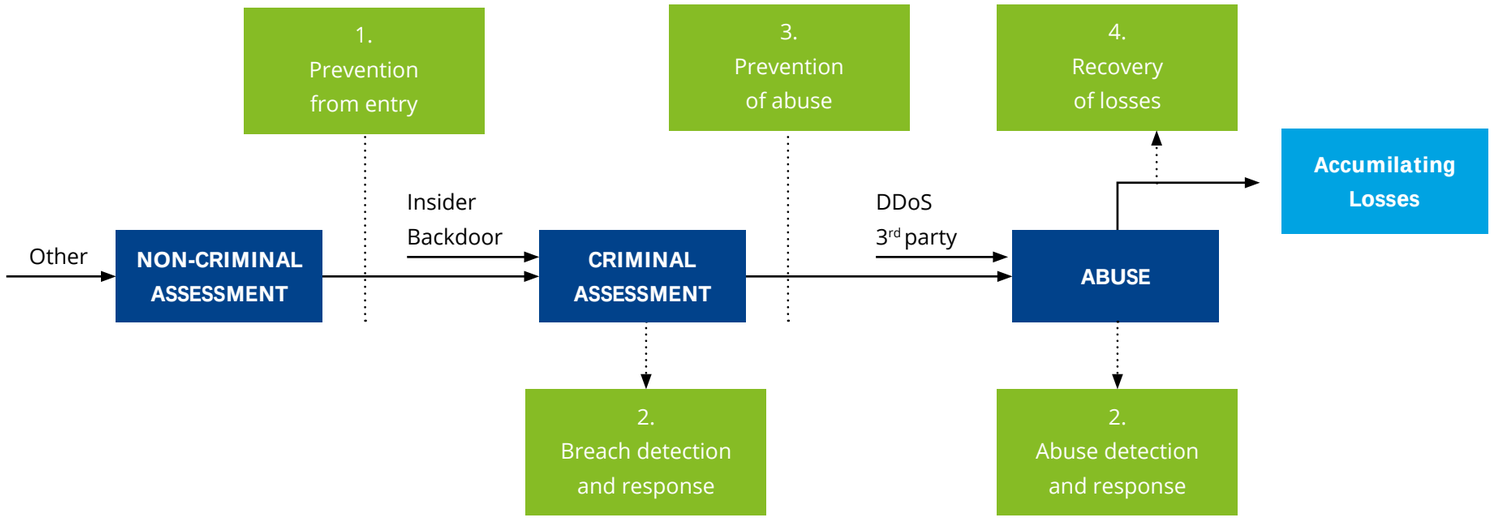
Final remarks

The described model gives an approach to measuring both Cyber VaR for individual organizations as well as for complete industries or economies. While it is based on known modelling techniques, the available data is of lesser quality and less complete than typically available for such models. We are convinced that despite this fact, this model is useful to obtain insights. In fact, the model can identify the level of risk associated to having low data quality and thus the value of having better data. As over time more data will become available, the quality of the outcomes will further improve.

We have created an approach that can serve as a generic reference in relating the technicalities of cyber risk to management, business and economic implications. We intend to further refine this model and its assumptions in the near future.

We invite experts who wish to contribute to reach out to us, be it through challenging our approach, by providing data and validations or by joining our team.

Capability	Description
1. Prevention from entry	The fraction of attackers who gain entry to an organization's systems.
2. Detection and response	The expected number of days after which an attacker is detected and neutralized. No distinction is made between entry and abuse.
3. Prevention of abuse	The expected number of days between the breach of security measures and the actual abuse of an information asset.
4. Recovery of losses	Capabilities to reduce damage incurred by the abuse of an information asset (resilience).



Contact

Marko van Zwam
Partner
Cyber Risk Services
+31 621272904
MvanZwam@deloitte.nl

Twan Kilkens
Managing Partner Clients & Industries
Risk Services
+31 612344894
TKilkens@deloitte.nl

Maarten van Wieren
Senior Manager Cyber Risk Quantification
Cyber Risk Services
+31 682019225
MvanWieren@deloitte.nl

Dick Berlijn
Senior Board Advisor
Deloitte Executive Office
+31 620789556
DBerlijn@deloitte.nl

About the authors

Maarten van Wieren

Senior Manager Cyber Risk Quantification

Maarten is a specialist in modelling complex systems and leads the cyber risk quantification team. He combines the latest insights in cyber risk with extensive experience in financial risk including his MSc degree in Financial Risk Management and his PhD in Mathematical Physics (specializing in complex systems). His other specialties include balance sheet optimization and economic models.

Esther van Luit

Senior Consultant Cyber Risk Services

Esther has a background in Economics and Management and specializes in the role cybersecurity plays in society. She has ample experience in cybersecurity governance, researches the cybersecurity skill gap and cyber risk quantification. She works on getting more women in security, improving security education and was nominated for “Woman of the Year 2015” by the Cybersecurity Awards.

Raoul Estourgie

Consultant Cyber Risk Services

Raoul studied at the Kerckhoffs Institute for Computer Security and specialized in cryptography. During his studies he did a minor in economics which created his interest for economic models. With his recent career launch at Deloitte he decided to focus more on this specific combination with a study in financial risk management.

Vivian Jacobs

Junior Manager Cyber Risk Services

Vivian has a Physics background and recently completed a PhD in Theoretical Physics at Utrecht University. She has an interest in mathematical modelling and its applications, and enjoys working in an interdisciplinary setting and building bridges between topics. Vivian joined Deloitte’s Cyber Risk Quantification team early 2016.

Jeroen Bulters

Junior Manager Cyber Risk Services

Jeroen completed his Bachelor degree in Computer Science in 2007 after which he gained experience as a software engineer and as Head of Development and Innovation. During this period he assisted clients in the insurance, fintech, shipping and retail sector with online innovations. Jeroen loves solving multi-disciplinary problems with a hands-on mentality.

Other Deloitte contributors

Dominika Rusek
Linda Peursum
Luuk Schrandt
Niek IJzinga
Richard Drewes
Roel van Rijsewijk
Ton Berendsen
Toon Segers
Yorick Breukers

Selection of literature

1. 2020 Cybercrime Economic Costs: No Measure No Solution. Armin, Thompson, Ariu, Giacinto and Kijewski; 2015.

2. ENISA Threat Landscape 2015. ENISA; 2015. Retrieved from: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015

3. Cyber Insurance: Covering the Basics. ISF; 2014.

4. The Economics of Information Security and Privacy. Böhme (editor); 2013.

5. ICT Kennis en Economie 2015. Ministerie van Economische Zaken, TNO and the Centraal Bureau voor Statistiek; 2015. Retrieved from: http://download.cbs.nl/pdf/ict-kennis-economie-2015-pub.pdf

6. Probability Analysis of Cyber Attack Paths against Business and Commercial Systems. Dudorov, Stupples and Newby; 2013. Retrieved from: http://www.csis.pace.edu/~ctappert/dps/2013EISIC/EISIC2013/5062a038.pdf

7. Damage Valuations of Trade Secrets: Evidence from the Economic Espionage Act of 1996. Searle, 2009. Retrieved from: http://www.epip.eu/conferences/epip04/files/SEARLE_Nicola.pdf

8. The Global Information Technology Report 2015. World Economic Forum; 2015. Retrieved from: http://www3.weforum.org/docs/Forum_Global_IT_Report_2015.pdf

9. Cyber Insurance as One Element of the Cyber Risk Management Strategy. Hurtaud, Flamand, de la Vaissière & Hounka; 2015. Retrieved from: http://www2.deloitte.com/lu/en/pages/risk/articles/cyber-insurance-element-cyber-risk-management-strategy.html

10. Incentives and Barriers for the Cyber Insurance Market in Europe. Moulinos; 2013. Retrieved from: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe

11. Q&A: Cyber Insurance Fundamentals for Security and Risk Professionals. Rose, McClean & Lisserman; 2012.

12. How to Structure the Decision-Making Process for Cyberinsurance Policies. Weiss; 2014.

13. Copula-based Actuarial Model for Pricing Cyber-Insurance Policies. Herath & Herath; 2011. Retrieved from: http://www.business-perspectives.org/journals_free/imc/2011/IMC_2011_1_Herath.pdf

14. The Role of Insurance in Managing and Mitigating the Risk. UK Government; 2015. Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf

15. The Growth of the Global Mobile Internet Economy. Bock, Field, Zwillenberg and Rogers; 2015.

16. The Mobile Revolution: How Mobile Technologies Drive a Trillion-Dollar Impact. Bezerra, Bock, Candelon, Chai, Choi, Corwin, Digrande, Gulshan, Michael, Varas; 2015.

17. Hackers Inc. Economist; 2014. Retrieved from: http://www.economist.com/news/special-report/21606421-cyber-attackers-have-multiplied-and-become-far-more-professional-hackers-inc

18. Microsoft Security Intelligence Report. Microsoft; 2015. Retrieved from: https://www.microsoft.com/security/sir/default.aspx

19. 2015 Trustwave Global Security Report. Trustwave; 2015. Retrieved from: https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf

20. 2015 Dell Security Annual Threat Report. Dell; 2015. Retrieved from: https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf

21. Akamai's State of the Internet Q3 2015. Akamai; 2015. Retrieved from: https://www.akamai.com/us/en/multimedia/documents/report/q3-2015-soti-connectivity-final.pdf

22. A Guide to Cyber Risk: Managing the Impact of Increasing Connectivity. Allianz; 2015. Retrieved from: http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

23. Cyber Risk Analytics. AON; 2014.

24. The Cost of Cyber Crime. Detica & Cabinet Office; 2011. Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

25. The Best of the 2014 Information Security Threat Reports. @k3strel; 2014.

26. 2013 Norton Report. Norton; 2013. Retrieved from: http://www.yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf

27. Cyber Theft of Corporate Intellectual Property: The Nature of Threat. The Economist & Booz Allen Hamilton; 2012. Retrieved from:

http://www.boozallen.com/content/dam/boozallen/media/file/Cyber-Espionage-Brochure.pdf

28. Is a Cyber Breach Inevitable? Cyber Security Challenges in the Netherlands. CGI; 2015. Retrieved from: http://automatie-pma.com/wp-content/uploads/2015/05/CGI-Cyber-Security-White-Paper-Final.pdf

29. The Rise of the Hacker. The Economist; November 7th, 2015. Retrieved from: http://www.economist.com/news/business/21677638-rise-hacker

30. 2015 Data Breach Investigations Report. Verizon; 2015. Retrieved from: https://msisac.cisecurity.org/whitepaper/documents/1.pdf

31. Cyber V@R: a Cyber Security Model for Value at Risk. Raugas, Ulrich, Faux, Finkelstein and Cabot; 2013. Retrieved from: https://www.cyberpointllc.com/docs/CyberVaR.pdf

32. Threat Intelligence Report 2012-2013 H1. Group IB; 2013. Retrieved from: http://report2013.group-ib.com/

33. The New Cybercriminals HPP – Hackers Profiling Project. UNICRI; 2012. Retrieved from: http://www.secure.edu.pl/pdf/2012/D1_1545_A_Bosco.pdf

34. Assessing Cyber Security: a Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks. Gehem, Usanov, Frinking & Rademaker; 2015. Retrieved from: http://www.hcss.nl/news/assessing-cyber-security/1292/

35. The Economics of Defense. Juniper Networks; 2015. Retrieved from: https://www.juniper.net/us/en/local/pdf/executive-briefs/3000091-en.pdf

36. Cyber Security Consulting. Hichman; 2013.

37. The Economic Impact of Cybercrime and Cyber Espionage. CSIS; 2013. Retrieved from: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

38. 2015 Cost of Data Breach Study: Global Analysis. Ponemon Institute LLC; 2015. Retrieved from: https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

39. Global State of Information Security Survey. HM Government; 2015. Retrieved from: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

40. Internet Security Threat Report. Symantec; 2015.

41. Cyber security: Everybody's imperative. Deloitte Canada; 2014. Retrieved from: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-cyber-security-everybodys-imperative.PDF

42. The Cost of Immaturity: the Business of Protecting Against Computer-hacking is Booming. The Economist; November 7th, 2015. Retrieved from: http://www.economist.com/news/business/21677639-business-protecting-against-computer-hacking-booming-cost-immaturity

43. Cyber Warfare: Building the Scientific Foundation. Jajodia, Shakarian, Subrahmanian, Swarup & Wang (Editors). Advances in Information Security 56, Springer; 2015.

44. Hackonomics: Cybercrime's cost to the business. Blue; 2014. http://www.zdnet.com/article/hackonomics-cybercrimes-cost-to-business/

45. VCDB Explorer. Veris; 2015. Retrieved from: http://vcdb.org/explore.html

46. Data Breach Reports. ITRC; 2015. Retrieved from: http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

47. Markets for Cybercrime Tools and Stolen Data. Ablon, Libicki & Golay; 2014. Retrieved from: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

48. Cyber Security Assessment Netherlands 2015. NCSC, 2015. Retrieved from: https://www.ncsc.nl/english/current-topics/Cyber+-Security+Assessment+Netherlands

49. Net Losses: Estimating the Global Cost of Cybercrime. CSIS; 2014. Retrieved from: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

50. The Hacked World Order. Segal; 2016.

51. Superforecasting: The Art and Science of Prediction. Tetlock & Gardner; 2015.

52. Risk Savvy: How to Make Good Decisions. Gigerenzer; 2015.

53. M-Trends 2015: A View from the Front Lines. Mandiant; 2015. Retrieved from: https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf

54. Global Cybersecurity Index. ITU; 2015. Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

55. Top Countries Best Prepared Against Cyberattacks. Santiago; July 22, 2015. Retrieved from: https://www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/

56. M. van Wieren et al., Understanding Bifurcation Between Slow versus Fast Cyber Attackers, submitted (2016)