BELRIM Prize 2022

Sebastien Kelles
Priyenka Gurung
Marie Lheureux
Olivier Van Coppenolle
Lucas Kinoo

Table of content

General Introduction

The goal of this study is to analyse to which extend Belgian companies are protected and aware of operational risks and to raise awareness among Belgian risk managers. The study focuses on natural disasters and cyber risks. These subjects will be evaluated and analysed by two professional tools provided by AON: **CyQu** (Cyber Quotient Evaluation) and **NatCat** (Natural Catastrophe analysis for flood and storm risk). These tools will provide overall data on the risk exposure to respectively natural disasters and cybersecurity of the companies.

Both research subjects have become increasingly more significant in recent years. Therefore, the purpose of this study is to inform risk managers about our findings and to present a few key take-aways for risk managers in Belgium. In order to reach a large audience, our research results will therefore be shared via LinkedIn. We deliberately choose to publish our results via LinkedIn and to present them in an approachable way so a large audience can be reached and the key-takeaways don't get lost. Both the LinkedIn posts can be found below. In order to reach a larger audience, AON will share these post on LinkedIn, that's why it's written in the third person and we are referred to as "the students".
We will also organize an event to give the risk managers of the participating companies insights into their individual results. We will be assisted by AON to break down their results in detail and discuss possible solutions.

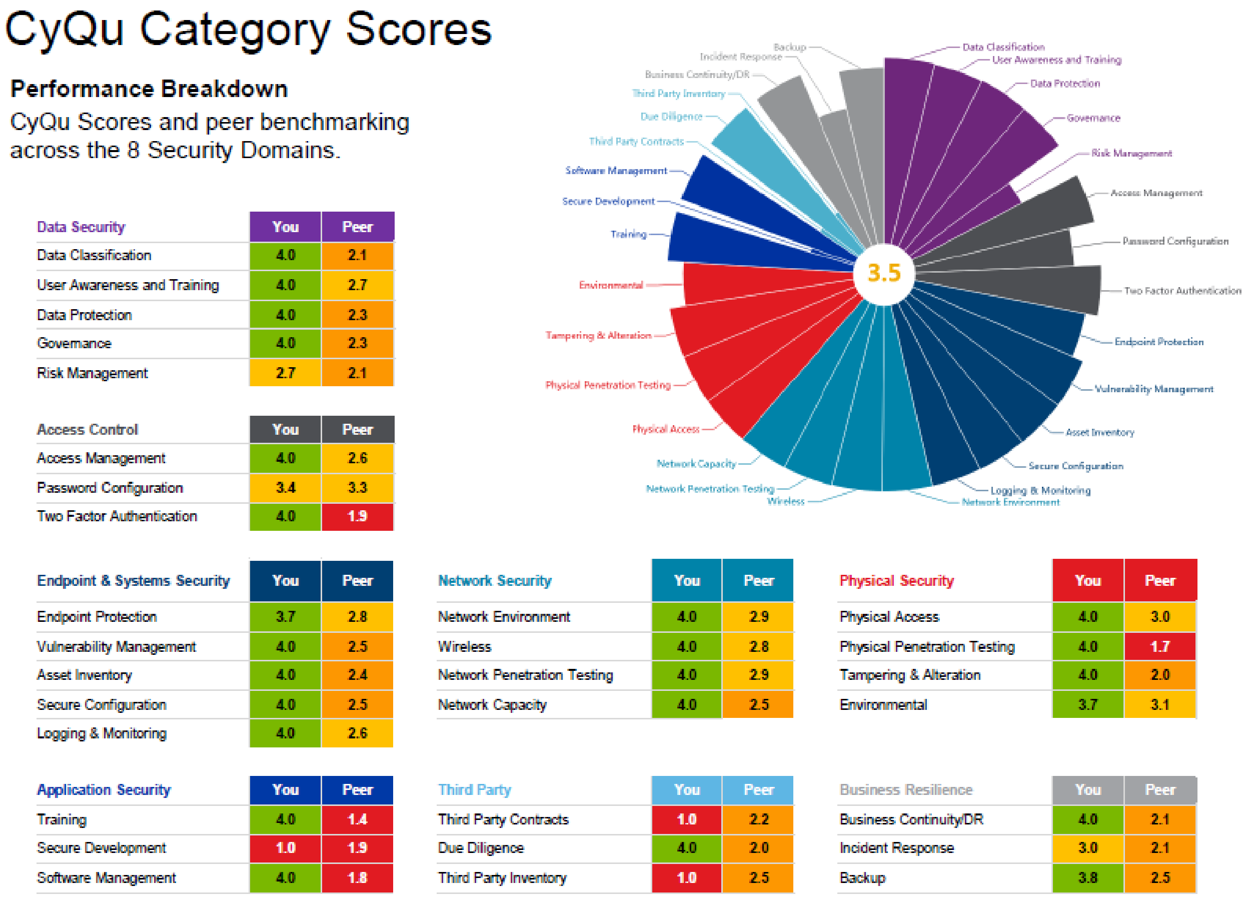
This study is carried out by a team of five students in collaboration with AFC Leuven (Academics for Companies, a student organisation), BELRIM (Belgian Risk & Insurance Management Association, the association of risk managers of the largest Belgian companies) and the international risk and insurance specialist Aon. The study is also supported by Tim Wouters, visiting lecturer at KU Leuven and CRO at ERGO INSURANCE.

LinkedIn Post – Cyber Risks

Cyberextortion is rampant in Belgium just like anywhere else in the world, but what are Belgian midsized companies doing against it? What is their current state of cyber protection? And what can be done in daily practice to improve it?

To answer this question, a group of university students gathered together by AFC (Academics for Companies) conducted a survey of Belgian based corporations with a revenue higher than 80m euros. Their work was done in the spring of 2022, in collaboration with the association of Belgian risk managers Belrim, university professor Tim Wouters, and insurance broker Aon.

The students used Aon's global CyQu tool, an online cyber questionnaire to gauge the participating company's level of cyber protection in various domains. They produced a score for 8 different security domains in the participating companies and benchmarked it against the industry average.



CyQu Category Scores

Performance Breakdown

CyQu Scores and peer benchmarking across the 8 Security Domains.

Data Security	You	Peer
Data Classification	4.0	2.1
User Awareness and Training	4.0	2.7
Data Protection	4.0	2.3
Governance	4.0	2.3
Risk Management	2.7	2.1

Access Control	You	Peer
Access Management	4.0	2.6
Password Configuration	3.4	3.3
Two Factor Authentication	4.0	1.9

Endpoint & Systems Security	You	Peer
Endpoint Protection	3.7	2.8
Vulnerability Management	4.0	2.5
Asset Inventory	4.0	2.4
Secure Configuration	4.0	2.5
Logging & Monitoring	4.0	2.6

Network Security	You	Peer
Network Environment	4.0	2.9
Wireless	4.0	2.8
Network Penetration Testing	4.0	2.9
Network Capacity	4.0	2.5

Physical Security	You	Peer
Physical Access	4.0	3.0
Physical Penetration Testing	4.0	1.7
Tampering & Alteration	4.0	2.0
Environmental	3.7	3.1

Application Security	You	Peer
Training	4.0	1.4
Secure Development	1.0	1.9
Software Management	4.0	1.8

Third Party	You	Peer
Third Party Contracts	1.0	2.2
Due Diligence	4.0	2.0
Third Party Inventory	1.0	2.5

Business Resilience	You	Peer
Business Continuity/DR	4.0	2.1
Incident Response	3.0	2.1
Backup	3.8	2.5

Out of the 48 participating firms, the students made a zoom on the results of eleven industry average representative firms to draw some high-level conclusions. Seven of the eleven scored below their international peer group. They were often weak in 3 specific domains: data security, third party management and general business resilience. Some participants scored significantly worse than their industry peers. They need to urgently focus on upgrading cyber protection and should probably develop a different vision on IT security all together. Apart from this, it also appeared that only a minority of the firms were GDPR compliant. The General Data Protection Regulation was already implemented back in 2018, but nonetheless only a few companies seem to have taken all the necessary steps.

Data security

Participating companies received a low score with an average of only 2,08 on a scale from 0 to 5. The below average performance stems from general deficiencies in data classification, user awareness and training, data protection, governance and risk management. It indicates clearly that risk management principles are in urgent need of being applied more rigorously, where possible with the help of a professional risk manager.

The poor performance on data security of the participating firms is often caused by the low results for data classification. Data classification is a crucial aspect in terms of cybersecurity and can be defined as the process of organizing data using relevant categories so that it can be located and retrieved easily. It also allows data to be used and protected in an efficient way. The fact that many firms received a bad score for data classification is even more alarming since data classification is an important topic for the GDPR.

Third-party

On the management of third-party cyber risk, most companies scored lower than their peers, with an average score of only 1.6. These firms need to focus more on quality of third-party contracts, third-party due diligence, and third-party inventory. Especially the due diligence part appeared to require close attention. It indicates weaknesses in these organization's supply chain in general. The outside parties typically have another security standard and may be used as a contamination channel towards the organization. Risk managers are generally advised to focus on due diligence which prevents and detects third party risk through standard security assessments.

Business resilience

The third deficient domain for the participating companies is business resilience where they scored an average of only 1.9. Business resilience can be defined as a company's ability to overcome disruptions while maintaining business operations. Risk managers are advised to elaborate more post-disaster strategies to minimize downtime and reduce vulnerability to unexpected cyber events. Many of the participating firms appeared to score poorly on business continuity and remote business continuity. It is crucial for companies to be prepared to react accordingly in case of unexpected events to prevent losses of data, security breaches and overall negative effects on their brand image. Additional formations and sensibilizations of employees are also a key factor to improve business resilience. The human reaction itself plays a very important role, that should be taken into account as well as the pure IT side of business resilience.

What should risk managers do?

For the participating companies to improve cyber scores, risk managers should focus primarily on a limited number of quick fixes to improve data security, third-party management and business resilience. These are often easy to implement, not very costly and can provide almost immediate positive results in terms of cybersecurity. The quick fixes can be highly specific for some industries and it's clearly not possible to provide a general "magic quick fix".

Additionally, risk managers should also try to influence IT budgets and IT resourcing. The participating companies spend on average 8% of their IT-budget to IT-security and their IT-budget consists on average of 1% of their annual revenue.

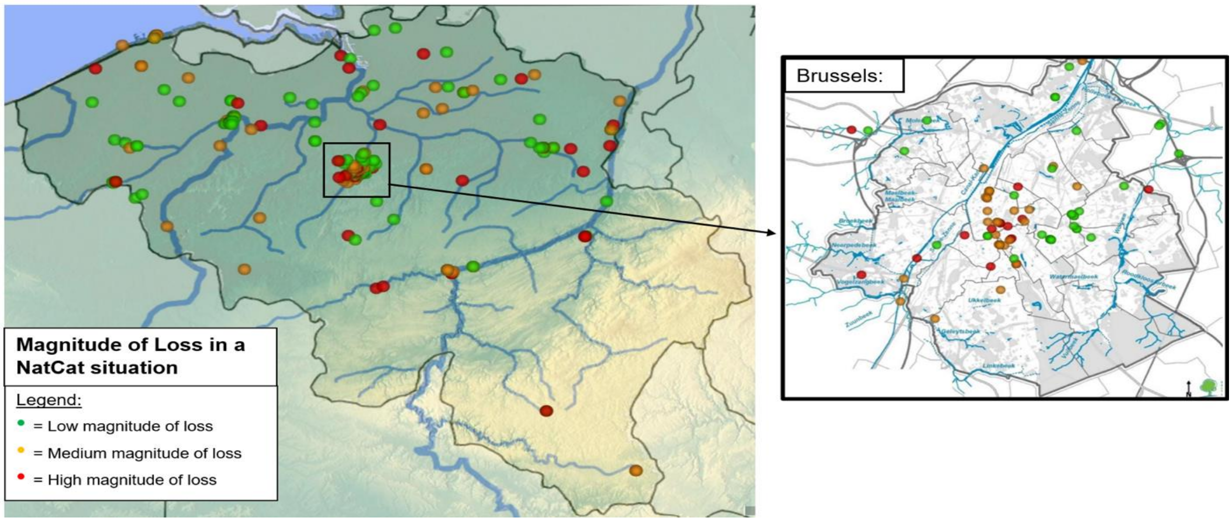
LinkedIn Post – Natural Disasters

Environmental, Social and Governance (ESG) issues have become critically important for companies. Ethical investing is the new normal and many governmental bodies are imposing regulations for companies to disclose their ESG efforts and investments. The Environmental perspective is a main pillar. Belgium has known several natural disasters over the decades which raises the following question: "What is the possible loss for Belgian companies when medium-sized businesses are faced with natural disasters?".

To answer this question, a group of university students gathered together in AFC (Academics for Companies) conducted a survey questioning the insured protection of over 200 Belgian company sites, active in various industries, against natural disasters. The aim was to present the exposure of medium-sized companies to natural catastrophes such as flood and wind risks. Their work was done in the spring of 2022, in collaboration with the association of Belgian risk managers Belrim, university professor Tim Wouters, and insurance broker Aon.
The students retrieved information from companies analysing the natural catastrophe (NatCat) exposure, location of their sites and their ESG efforts. The data was entered into Aon's QFLAT tool (Quantitative Flood Loss Assessment Tool) which is originally a geography tool to assess the risk of flood for residential buildings. QFLAT analyses four different categories of natural catastrophe risk: river flood, sewer flood, coastal flood and earthquake.

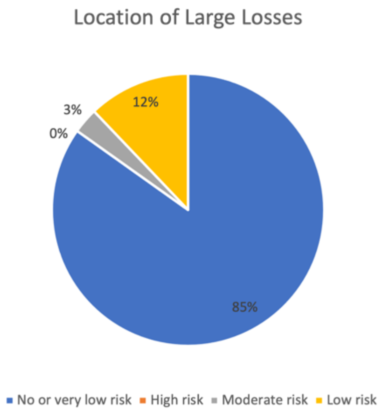
The students found some unexpected results which risk managers at midsized and large companies need to keep in mind.

Most locations are very low or no risk zones
9 out of 10 locations are situated in "no risk zones" for flood, based on the classification provided by the authorities. Intuitively, this corresponds to what the students had expected in a country like ours since most of our industrial sites are located securely away from flood areas. The below map indicates the location of each site based on the risk zone.


Brussels:
Magnitude of Loss in a NatCat situation
Legend:
● = Low magnitude of loss
● = Medium magnitude of loss
● = High magnitude of loss

A deceitful perception of security

On 215 surveyed sites, the students found that 187 are located in a no-risk or very-low-risk zone. However, in spite of this secure location, 15% of the estimated losses on these sites (after running the QFLAT model) are considered to be significant or large (larger than the mean of the estimated losses of the sample population). This indicates that a safe location is not a guarantee for the avoidance of a significant natural catastrophe loss.



Viewed from a different angle, the students also observed that 85% of the significant losses actually occur at locations situated in "no risk zones", again reinforcing the observation that large losses do indeed occur in seemingly safe locations. This observation begs the question of whether or not the officially recognized safe zones are indeed safe zone, or whether the classification needs to be reassessed.

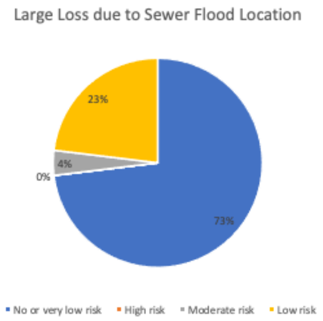
As an example: one of the participating companies, located in a safe zone in Brussels, is still incurring an expected €2.3m loss following a major flood situation.

River-induced flood vs sewer-induced flood

In general, out of the 215 sites, an average of 3 out of 4 are mainly influenced by rived-induced exposure (i.e., the risk of an adjacent rived flooding the actual site) and 1 out of 4 are mainly impacted by sewer issues (i.e., the flood risk being brought on by the insufficient water evacuation capacity of the nearby sewer infrastructure). However, when we zoom in only on the large losses, we observe that the portion of losses induced by sewer issues rises from 25% to no less than 60%. This indicates that the large loss exposure in our Belgian sites is somewhat more linked with infrastructure issues rather than with traditional river flooding issues. The hard surface issues in our country appear to have a significant influence. This finding clearly indicates the infrastructural weakness Belgian companies face. This raises awareness about Belgium's sewer infrastructure and begs the government to invest in their infrastructure. This result presents that Belgian companies could lower their risk when investments in sewer construction are made

Sewer-induced flood in no risk zones

In addition to the two observations above, the students also noticed that when zooming in on the large sewer losses, no less than 73% occur in perceived no-risk zones. For risk management purposes we take away that a no-risk zone is not a safeguard again the occurrence of the "danger" category of large sewer losses.



What should risk managers do?

When looking at natural catastrophe exposures of their sites in Belgium, risk managers should bear in mind that 15% of the NatCat losses in no-risk or very-low-risk zones are still to be considered as significant or large. In fact, even 85% of these significant losses occur in no-risk zones. Risk managers should warn their organizations on a possible false perception of security in our country. Furthermore, risk managers should be aware that out of all large losses, 60% are driven by sewer issues. Risk managers should warn their organizations to be extra cautious with public sewer infrastructure.