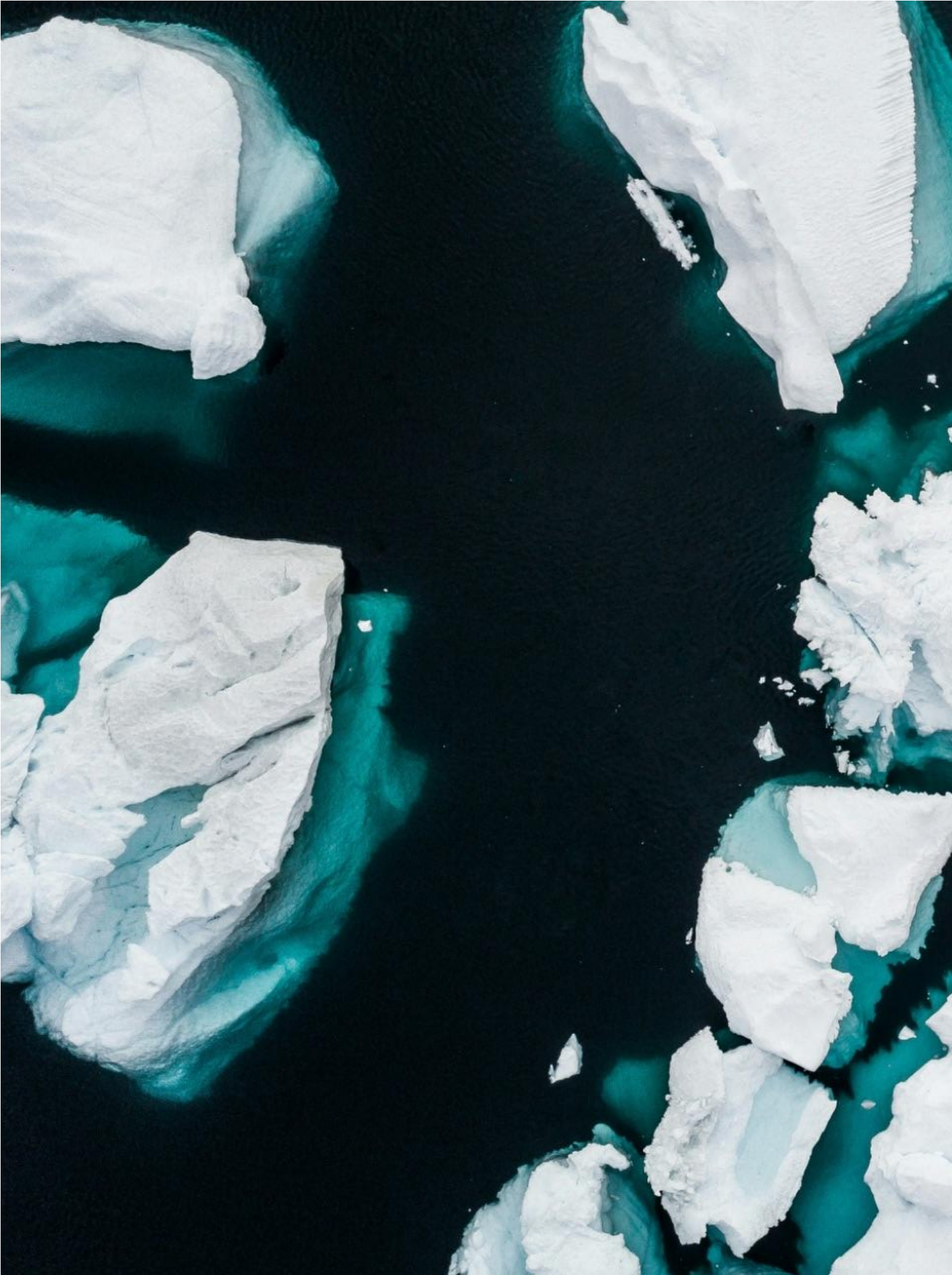


The Strategic CFO: Navigating the Financial Frontier of Cyber Risk



Utgard
Cyber Risk Consulting



Agenda

Executive Summary	4
Cyber risk is a business risk and therefore a financial risk	5
The evolution of cyber threat	7
Focus: Quantum threat will need a multi-year investment	10
The financial breakdown of a cyberattack	12
Focus: CDK Global, a systemic impact on the US automotive industry ..	15
The iceberg analogy of financial cyber impacts	17
Focus: Insights on Ransom payments	20
Focus: Insolvency following a cyberattack	26
Knowing the financial exposure to master cyber risk	27
Focus: Marks & Spencer, one year of profit erased	30
Measuring the value of cyber investment	31
Key takeaways	34

Executive Summary

From technical vulnerabilities to financial data

Cybersecurity is becoming a core determinant of **financial health** and **market valuation**. As organizations hyper-digitize, the attack surface expands, transforming cyber risk from a technical or compliance issue into a **systemic business risk**.

For the modern CFO, **security** is no longer just about preventing breaches; it is about **protecting financial performance**, **reducing cash-flow volatility**, preserving **EBIT**, limiting **credit-spread** fluctuations, and ensuring long-term **economic resilience**.

Traditional risk management qualitative heat maps (Red/Amber/Green) **fail** to **translate** cyber exposure into **financial terms**. This “color gap” often leads to **misaligned budgets**, where security spending is treated as a sunk cost rather than as a **strategic hedge** against **value destruction**.

The Iceberg analogy of financial cyber impact

The **true cost** of a cyber incident is a multi-dimensional **Iceberg** that impacts the organization across **three horizons**:



The Pinnacle (Immediate)

Direct cash outflows for remediation, incident response, and immediate shortfall in sales.



The Waterline (Mid-term)

Significant EBIT impact through revenue destruction, productivity loss, and compromised M&A valuations.



The Keel (Long-term)

Submerged, lasting costs including increased cost of debt (higher loan spreads), insurance premium hikes, and regulatory fines.

Transitioning to Cyber Risk Quantification (CRQ)

To bridge the gap between IT and Finance, organizations must adopt **rigorous quantification** methodologies such as **FAIR** or **SPICE**. By translating cyber threats into **monetary metrics**, CFOs can:



Prioritize Security spending



Enhance Decision-Making



Optimize Insurance coverage

Cyber resilience is the new **competitive advantage** that **Strategic CFO** must leverage through Financial Exposure Data to transform cybersecurity from a defensive necessity into a pillar of **strategic business value**.



Cyber risk is a business risk and therefore a financial risk

Over the last years, cybersecurity has become a **board topic**. But it has evolved from being a **technical topic** to a **compliance** topic due to new regulations (GDPR, NIS2*, DORA**, etc). For some companies, it is finally becoming a **business topic** because the truth is that **cyber risk is a business risk**.

IT and information security, as supporting assets, have become facilitators (if not enablers) of business activities. In **increasingly digitized** companies, it has become the **backbone** of all processes, tools and services: If the CRM is not available, no sales are possible; If the Warehouse Management System is compromised, there is no delivery possible; An encrypted ERP will shutdown almost everything.

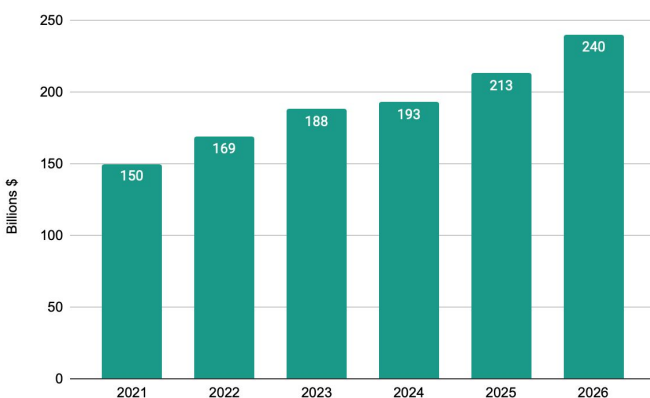


Exhibit 2: Evolution of spending on information security****

NIS2 Directive*: Securing Network and Information System
DORA** Digital Operational Resilience Act

Source: *** Cybersecurity Board Reporting - The Board's Perspective - 2025
**** Gartner Forecasts Worldwide End-User Spending on Information Security

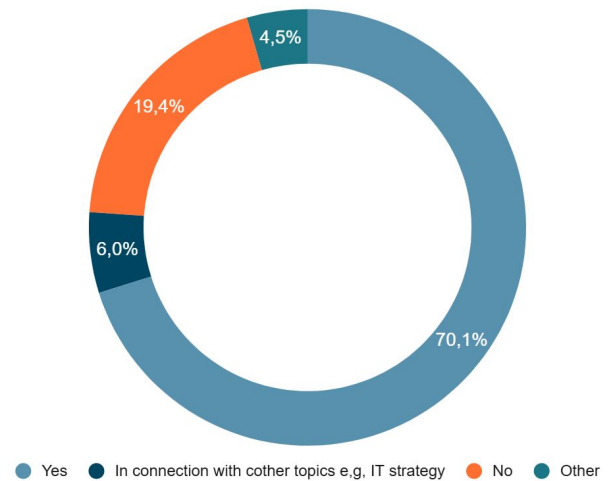


Exhibit 1: Cybersecurity Discussed at the Full Board***

As organizations invest in their **digital transformation**, to leverage technology for **increased performance**, they also **increase** their **attack surface**. Each new application or solution connected to the internet brings **new cyber threats**.

From a financial standpoint, cybersecurity poses a **real investment question**. Organizations have significantly increased their spending in cybersecurity. Yet, even a well-funded and protected organization can fall victim to a phishing email or a new vulnerability.

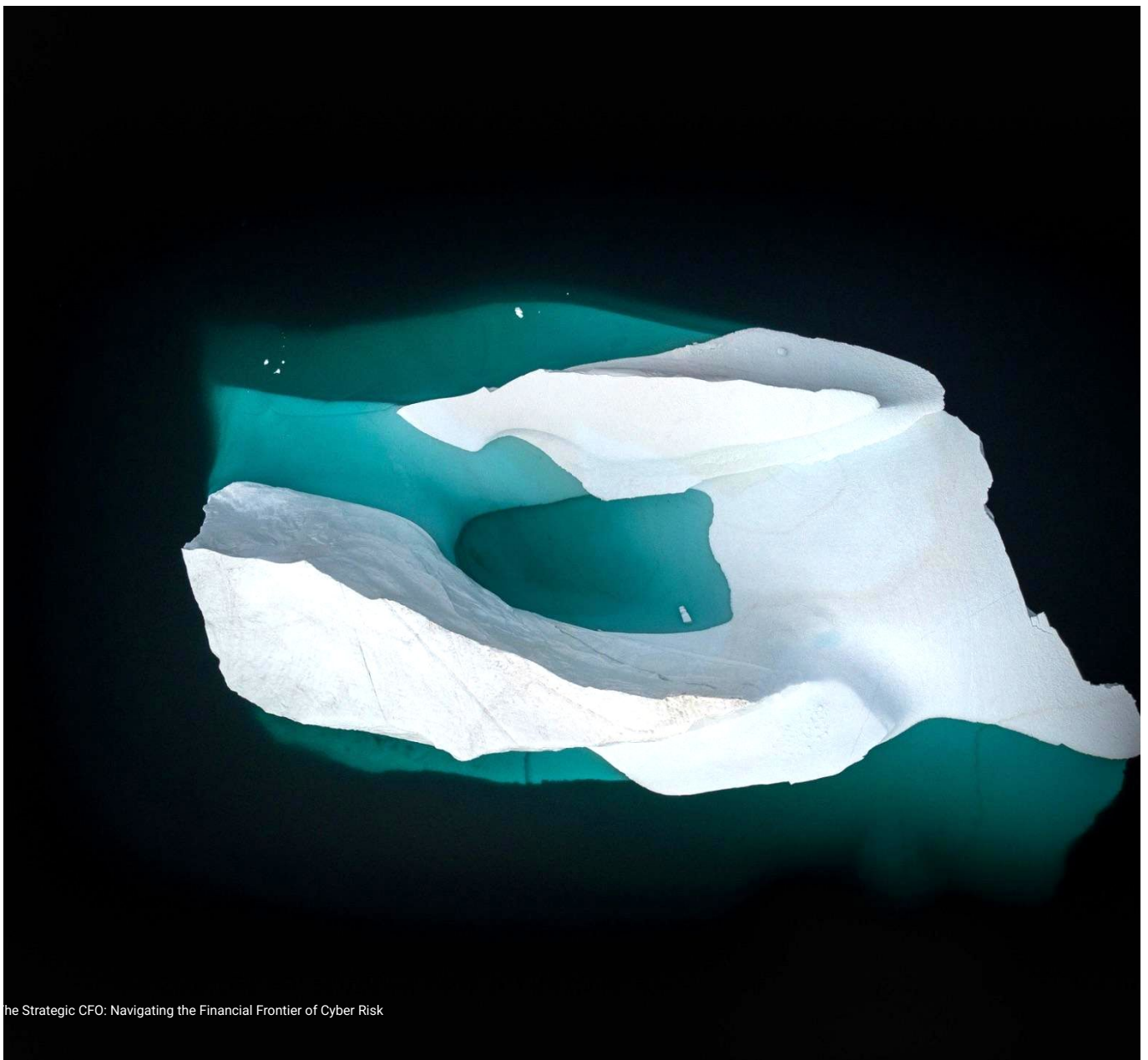


This situation leaves the CFO and the board questioning whether **security investments truly protect** the business or if they face a **lose-lose scenario**: investing in a costly "AI-enhanced SOC*" only to eventually pay a ransom anyway.

Of course, depending on the type of cyber incident, the cost will not be the same. A corporate website unavailable for a day or a marketplace unavailable for one hour will have significantly different impacts.

Regardless of the type of cyber event and considering that in the end there is **always financial cost** associated with it (whether it is to remediate, recover, compensate or pay fines) the CFO should be at the forefront of cyber risk management.

* Security Operation Center





The evolution of cyber threat

Cyber Risk is ranked number one of the **top 10 risks** by many major insurance* or risk expert organizations**, and is expected to stay in the **top 3** for the next few years.

Though there are **no official** and **reliable statistics** to grasp the evolving number of cyber incidents over the years, experts*** agree on the **increasing trend**. Furthermore, despite the cyber sphere always evolving, we can identify **four trends** that organizations should be mindful of:

▲ **Hybrid warfare**

The shift toward a "**war economy**" creates a suitable **landscape** for cyberattacks. By targeting **critical infrastructures** and companies in specific areas like energy, defense and logistics, competitors of Western countries are increasingly trying to **destabilize** the European **economy** and **undermine** the trust of their population in their **institutions**.

▲ **Technological innovation**

AI-powered cyberattacks have drawn some attention in the last years due to capacity to **impersonate executives**, ease the recognition phase before an attack or through reducing time to craft new malwares. The **AI-threat** will be met by the **Quantum threat** that will come in the next **five years**.

But even if these new technologies are gaining some traction, **statistics** show that **phishing** and **unpatched vulnerabilities** are still the **main entry-points** leveraged by attackers.

This specific trend highlights that the **span of expertise** that organizations need to address is **widening**, putting **teams** under **tension**.

Source:

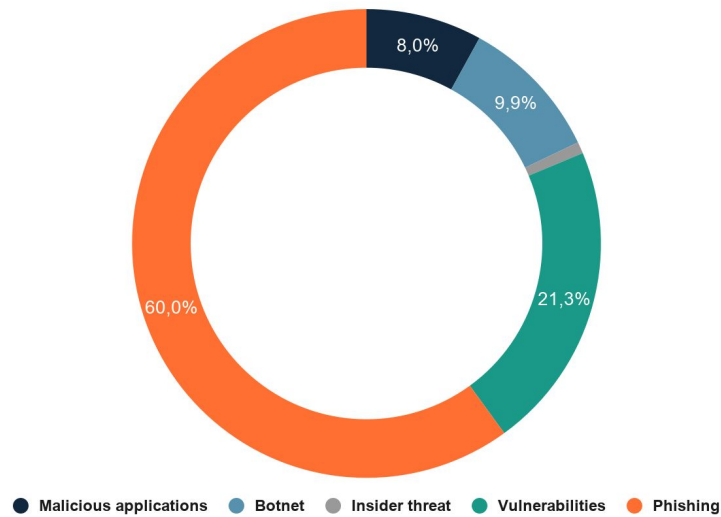
* Allianz Risk Barometer 2026

** Protivi Unlocking opportunity - Executive perspectives on top risks and opportunities - 2026

*** Check Point - Cyber Security Report 2026



Exhibit 3 - Most identified initial infection vector*



▲ Supply Chain fragility

As **major companies** have increased their cyber maturity, they have become **harder targets** for attackers. Hackers, state-backed or just financially motivated, are increasingly targeting their **supply chain**. **Direct suppliers** (Tier 1) or **indirect suppliers** (tier 2 or 3) are likely to be smaller, with a more **limited budget** and set of **skills**. So they can be used by attackers to destabilize a major companies:

- △ By leveraging the **IT interconnections** with their customers to be used as **entry point** to the major company's information system;
- △ By **disrupting** the supplier's activity and therefore, disrupting their major customer's value chain.

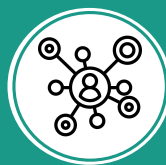
Smaller supplier are generally facing:



Lower budget
capacity for
cybersecurity



Limited in-house
skills or ability to
access external
support



Lower maturity of
the workforce on
cybersecurity
topics



Limited or
contract-based
cyber
management of
their own supply
chain

Source: * ENISA Threat Landscape 2025



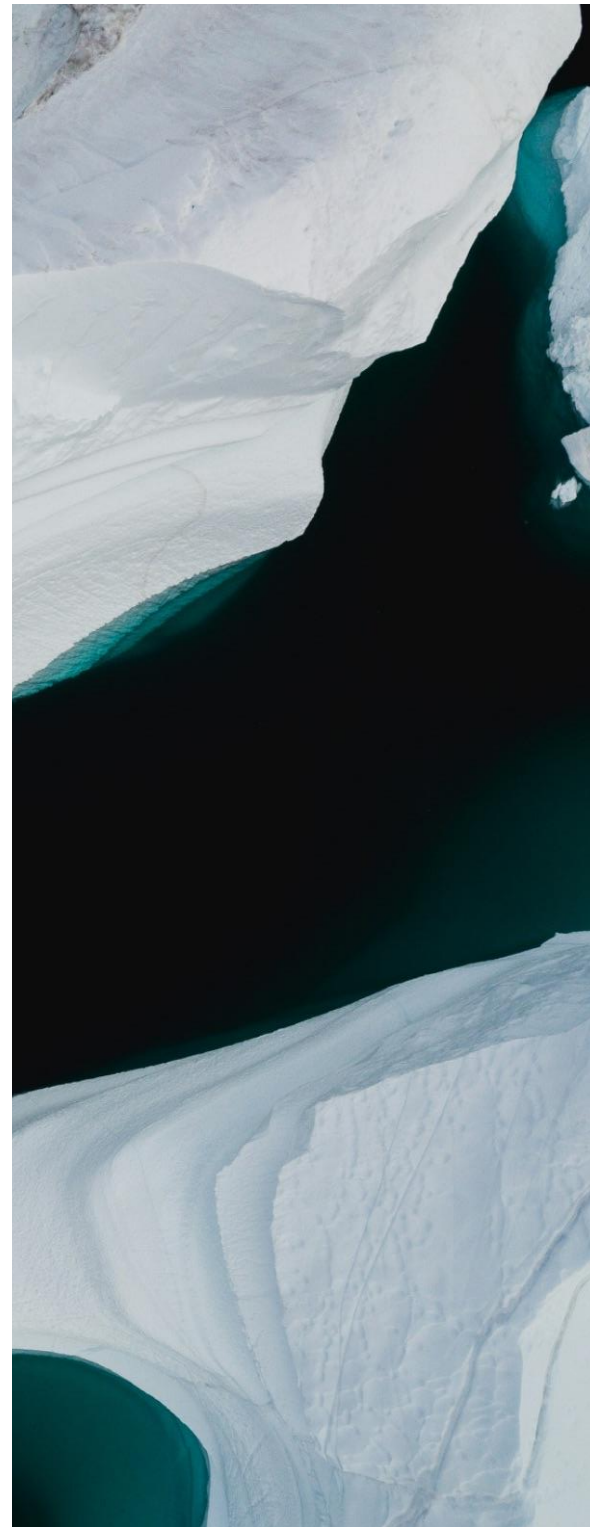
▲ Threat actor ecosystem evolution

The **landscape** of threat actors has **evolved** towards a "**division of labor**" approach or specialization. Some groups are **specialized** in gaining **initial access** into an organization and then selling it on the **black market**. Others are specialized in crafting specific tools or malware, while the final links of the value chain are groups specialized in **ransom laundering**.

In addition, the **fast-evolving** technological landscape allows hackers to perform "**skills leapfrogging**" and directly target companies even with very limited technical expertise through "**ransomware-as-a-Service**" type of tools.

In 2022, the hacker group **Conti** faced a massive leak of internal communications, showing that it was structured almost like a regular organization, with HR-like discussions on bonus, holidays, performance reviews, etc.

The creation of such an **ecosystem** shows that **cyber crime** is getting **more professional** and difficult to **dismantle**, enhancing the threat level for organizations.



Value chain of the cyber threat ecosystem



Initial
Access Broker



Malware
developers



Ransomware
operators



Supply Chain
specialists



Money
laundering

Focus: Quantum threat will need a multi-year investment

While every company is assessing the use of Artificial Intelligence, **Quantum computing** has made significant breakthroughs. Based on **quantum physics**, it will allow the processing of certain complex problems **exponentially faster** than with classical computers.

Though the benefits would be tremendous, the Quantum Revolution would also bring its misuses. For IT, the **Quantum Threat** mainly concerns **cryptography** and would materialize as follows:

▲ **Asymmetric encryption obsolescence**

Asymmetric encryption, currently used for **securing connection** to websites (HTTPS), ensuring the **authenticity** and **integrity** of **digital signatures**, Public Key Infrastructures (PKI), digital activities or software, would become **easy to break**.

The consequences would be that online activities based on trust like online payment, money transfers or banking activities could **not be trusted anymore**.

▲ **Harvest now, decrypt later**

Encryption actually protects data, even if stolen, by making it **unreadable**. But Quantum Computing will allow users to decrypt previously stolen data. This horizon of possibilities encourages hackers to harvest encrypted data with the hope of **decrypting it later**. Military information, strategic data, industrial secrets or healthcare data could be easily decrypted in a few years.

▲ **Digital certificate unreliability**

Currently, **software integrity** is proven through the usage of **Digital Certificate**. Should this certificate be altered, the software would **not be trustworthy anymore**.

This basically means that a company that were to apply an update, for example, on its CRM or ERP, could be applying a counterfeit and therefore **enable hackers** to **access** their system easily. The same would apply to connected objects, vehicles, etc.

Quantum computers are still in the **development phase** and could only be afforded by certain countries, but institutions expect materialization of this threat, called "**Q-Day**", by **2030**.

Large companies or organizations are beginning to launch **Post-Quantum Cryptography** projects, but these company-wide **migrations** will need **time** and will come with **multi-year investments**.

The UK National Cyber Security Center suggests that this migration should be **completed** by **2035**.

Considering the **business implications** and the need of **long-term financial resources**, the CFO should leverage **Cyber Risk Quantification** in order to **prioritize** the **assets** to migrate and **build** a clear **roadmap** that will ensure **cost-effectiveness** and **business value**.

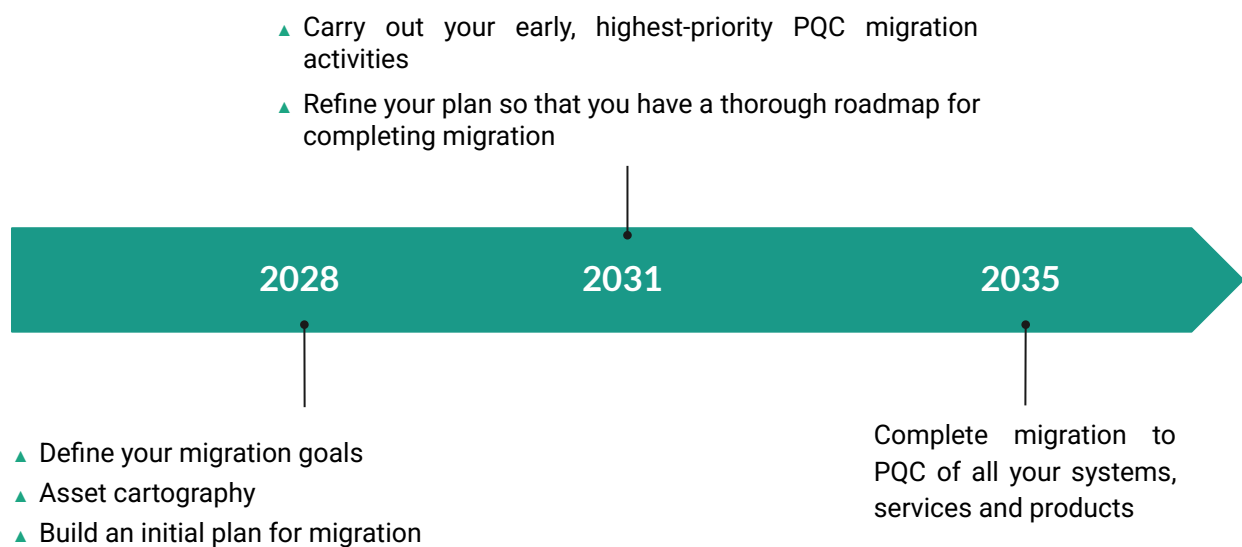


Exhibit 4: Timeline for migration to Post-Quantum Cryptography*

Source: * NCSC Annual Review 2025 - Migrating to post-quantum cryptography - 2025



The financial breakdown of a cyberattack

The **different phases** of a **response** to a **cyberattack** are well documented throughout various frameworks. From a **financial standpoint**, even if all organizations have their specificities, we can identify **common patterns**.

Phase 0: Initial compromise

This phase, where the **attacker gets inside** the information system, can last for months. They can be **dormant**, can try to get further access through **privilege escalation** (getting more rights) or **lateral movement** (move to other systems) or they can slowly exfiltrate data.

At this point, there is **no financial impact**, except if the attacker aims to leverage **false invoices** to receive undue payments (which could last years before being identified).

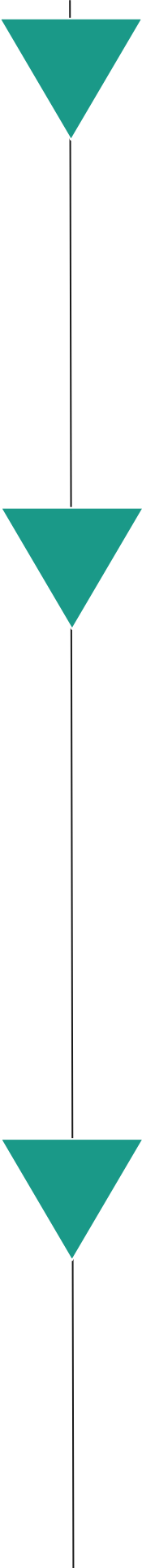
Phase 1: Detection & identification

When the **attack begins**, actions can unfold very quickly with progressively all **systems** becoming **unavailable** and all the teams unable to communicate. Or it can come slowly, through **customers, partners** or **employees** complaining they can't access certain services anymore.

At this stage whether this is a **regular IT-incident** or an **attack** and the extent of the disruption can be unclear and needs to be **assessed**. Depending on the cyber maturity of the company, detection can take **hours** or **days**.

Depending on the organization's business, the financial impacts can start right away: **cash inflows** and **order processing** are **affected**.

An online shop will instantly lose cash through payment loss whereas a less-digitized factory will be impacted later.



Phase 2: Containment

The containment of the attack aims to **prevent** it from **spreading** further. Having in-house Incident response skills is usually seen in larger organizations. Smaller ones will certainly need **external resources**. Companies with **cyber insurance** can often benefit from **technical support**.

From a **financial perspective**, this is when **cash** will start to be **impacted** by requesting **external support**.

Phase 3: Crisis management & communication

At this point, the business **responses** get organized and **management** takes **decisions** through **Business Continuity** or **Disaster Recovery**.

Should further external support be needed, impact on **cash** would continue and since **communication** to customers, partners, authorities will be decided by management, **news** of the **attack** will likely be **public**. Therefore, **publicly traded** companies can face a **negative impact** on **stock price**.

Companies with a **low treasury** might be forced to **find credit solutions** that, based on the confidence in their **financial health** and **recovery capacity**, might be more or less **costly**.

Phase 4: Eradication

Like the containment phase, Eradication is **critical** and will determine the **ability** to start the **recovery**. The incident response team needs to make sure that the **threat** has been **eliminated** and will not persist through **hidden backdoors** that would allow hackers to **continue** the **attack**.

From a **financial** point of view, **cash inflows** is still **unavailable** or limited while **cash outflows** continues to sustain incident response.



Phase 5: Recovery

Depending on the organization's **ability** to **eradicate** the **threat**, to recreate a **safe IT environment**, to leverage **backups**, etc, recovery can last for **days** or for **months** and will likely need **purchasing** new IT **capacities** (servers, licences, new solution to replace legacy or customized solutions, etc).

Here, **two financial points** must be considered: **Available cash** to sustain the crisis (OPEX and unforeseen CAPEX) and **turnover loss** that will impact cash later on. Depending on the organization, several levers exist: **cash outflows delay**, **credit-line** or cyber **insurance** advance payment (depending on capacity to pay the **deductible**) etc.

Some companies take the decision to **pay** the requested **ransom**, sometimes by using the services of **negotiators** to **diminish** the **amount** asked.

Phase 6: Post-incident

Once the **IT recovery** allows the **business** to **restart**, the **financial impacts** **continue** for **months** if not **years**.

cash inflows can **resume** but **cash outflows** **persist**, ordering / selling can restart even in degraded mode. **Longer impacts** will have to be considered: **Turnover**, **EBIT**, **Insurance premiums**, etc.

But the **second wave** can be **penalties**, customer discounts, regulatory **finances**, etc. Following a cyberattack, usually, **investments** are needed to secure or adjust the information system.





Focus: CDK Global, a systemic impact on the US automotive industry

On June 18, 2024, **CDK Global**, a major US provider of **Dealer Management Systems** and **ERP** solutions for **car dealerships**, was hit by a **ransomware** attack reportedly attributed to BlackSuit.

CDK Global's systems support **critical** dealership **operations**: vehicle sales, financing, inventory management, parts ordering, repairs, payroll, accounting, CRM and reporting.

Two days after the incident began, the company reportedly paid a **\$25 million ransom**. Around **15,000 dealerships** were disrupted, with many remaining heavily impacted for approximately **three weeks**.

▲ The direct costs on CDK Global

The direct costs for CDK Global likely include incident response, crisis management, forensic investigation, system restoration, infrastructure rebuilding, legal support, customer communication, reputational damage, and potentially the reported \$25 million ransom, if confirmed.

▲ The indirect economic cost for CDK Global

The attack also created **longer-term consequences** as

- △ **Customer dissatisfaction** and potential customer **churn** as some dealerships were forced to consider alternative providers or backup solutions
- △ **Reputational** damage, especially as CDK Global publishes annual cybersecurity research for the automotive sector
- △ **Lawsuits** and arbitration proceedings: several lawsuits have been initiated including a **collective action** in Canada linked to the data breach or to the crippling impact for car dealerships. Companies specialized in collision repairs, not direct customers of CDK Global, also filed a lawsuit raising questions on the **depth of liability** on the supply chain.
- △ **Market awareness** of excessive **dependency** on a single **critical** technology **provider**

▲ Impact on customers

For dealerships, the attack was not just an IT outage. It disrupted **core business operations**.

Many dealerships were **unable** to properly track **contracts**, manage vehicle **inventory**, order **parts**, process **repairs**, manage payroll, complete financing, reconcile accounting data or access customer records.

Some dealerships reverted to **paper-based processes** to continue operating. However, “going back to paper” is **not free**. It creates **hidden costs** as

- ▲ Double entry once systems are restored
- ▲ Increased risk of errors in contracts, payroll, inventory and financing
- ▲ Manual backlog processing
- ▲ Loss of real-time visibility on margins, commissions and vehicle availability
- ▲ Slower sales cycles
- ▲ Additional staffing and overtime costs

Kinley Automotive Group, for example, claimed it lost around **\$600,000** during the disruption period.

▲ Impact on the US automotive sector

CDK Global's **dominant position** created a **systemic effect**. The disruption did not only affect one company; it affected an entire **ecosystem**.

Anderson Economic Group* estimated the total cost of the consequences of the attack at **\$1.02 billion** in **direct losses** for franchised dealerships over the **three-week disruption** period.

▲ Insurance figures

In its 2024 report, **At-Bay**** included a focus on this attack. The report highlighted:

- △ **+43% increase** in **claims** related to indirect ransomware attacks, largely attributable to CDK Global
- △ **\$241,000 average cost** for impacted policyholders
- △ the **frequency** of **indirect** ransomware **claims** increased from **46** in **2023** to **66** in **2024**, including **42** linked to **CDK Global**

This incident also raised an important **insurance issue**: **dependent business interruption**.

Many affected companies were not attacked directly. Their losses came from the unavailability of a critical supplier. In other words, **having cyber insurance is not enough**. Companies need to verify whether their policy **actually covers** losses caused by a cyberattack affecting a key supplier.

Source: * AEG - Dealer Losses Due to CDK Cyberattack Reach \$1.02 Billion - July 2024
** At-Bay The 2024 InsurSec Report: Ransomware Edition



The iceberg analogy of financial impacts

The **financial impact** of a cyberattack can easily be **underestimated** by organizations by only looking at the **immediate impacts**, just like an iceberg.

We can identify three main parts to this iceberg: the pinnacle (emerged part), the waterline (presumed part) and the keel (submerged part).

The pinnacle: impacts on cash and stock-price

Impact on cash

As described, cash is the first financial asset to get impacted by **blocking** the **inflow** and creating **unforeseen outflow**.

From an inflow perspective, in the event of a cyberattack, assuming the actions that triggers **invoicing** of **customers** are **blocked**, having a clear **cash management strategy** will define how long the company can last without external help. Among all possibilities, some points to consider:

Days Sales Outstanding (DSO)

Negotiating with customers to **collect payments faster** will define if the company can still count on cash flowing in to **sustain** the **exceptional CAPEX**. **Reducing** the **DSO** is often among the first actions to consider during a crisis but could be **limited** by the lack or **limited access** to **IT** tools like CRM or invoicing.

Days Payable Outstanding (DPO)

Increasing payment delay is certainly a logical action but could create other trouble: **negatively** impacting **fragile suppliers**, creating a **bullwhip effect** that would adversely affect the company later, result in **contractual penalties**, etc. Some suppliers could also **fear** a **bankruptcy** and **refuse payment delays** or worse, request **upfront** payment.

Days Inventory Outstanding (DIO)

Due to **impossibility** to **deliver** products, goods blocked in **inventory** will result in longer **cash immobilisation**. For companies selling perishable goods or goods with a **volatile cost** (raw material), this might also result in a **dead loss**.



From the **outflow perspective**, **exceptional expenses** will be required in order to recover to a normal situation, for example:

▲ **Consulting**

Incident response team	Crisis management	Legal counsel
In the absence of a cyber insurance, or technical support, bringing the specific expertise to investigate and remediate the crisis will be necessary. Consulting companies are specialised in Incident Response and able to work 24/7 .	Even if a crisis management cell is in place, having an external support to coordinate the actions or communication internally or externally could be helpful.	Many factors could lead to the need of legal counsel during a cyberattack: negotiation with suppliers to avoid penalties , relations with authorities regarding specific regulations, preparing for possible claims from customers, but also, in the case of a cyberattack being enabled by a third party, considering legal actions against this third-party .

- ▲ **Hardware:** business continuity could mean buying new **laptops** for specific teams, or new **servers** but also for industrial cyberattacks, replacing **industrial assets**.
- ▲ **Licences:** purchasing temporary **licences** to get access to certain **IT tools** can **increase** the **recovery time**. In some cases, subscribing to maintenance services (ex: for ERP) would require **immediate payment**.

In all these cases, having a **contract** in place for **emergency support** (consulting, hardware or software) could help identify the specific type of **skills** needed, and **avoid** the last minute **negotiations** that can result in paying the **highest price**.

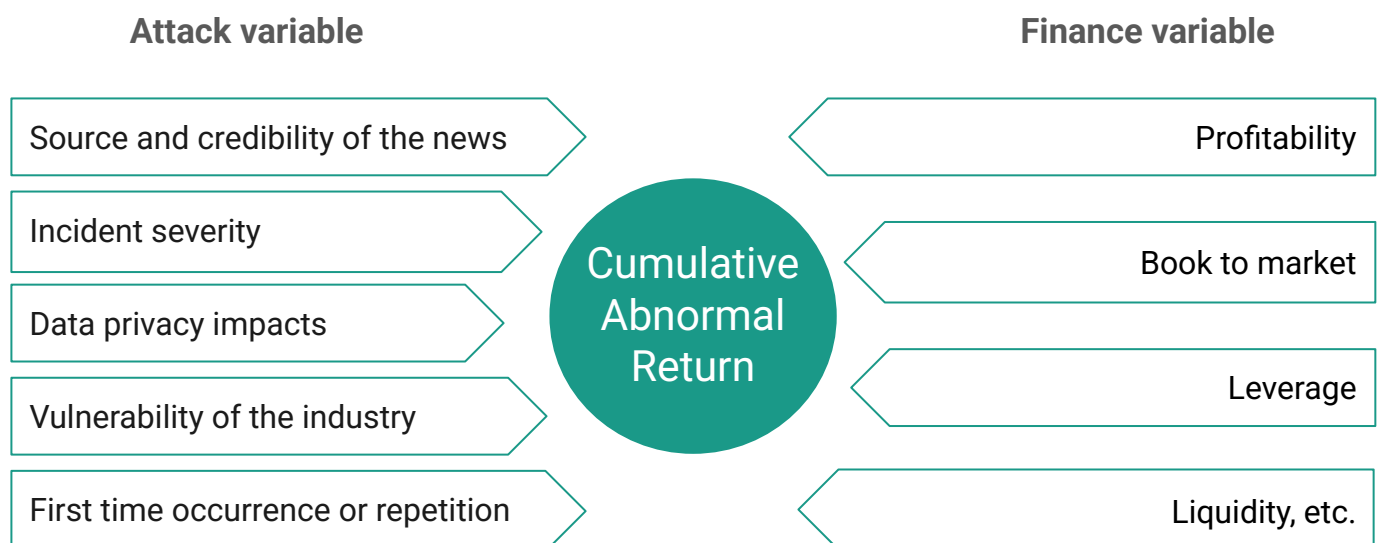


Impact on stock price

For **publicly listed** companies, **adverse events** might have an impact on **stock prices**. Studies* have shown that the main **variables** will concern the **attack** itself but also the **company's financial situation**.

Depending on all these factors, the market's response shows an **average loss** of 0.15% **Cumulative Abnormal Return (CAR)** on the **day** of the **announcement** and up to 0.36% of CAR in the **5 days** following the announcement.

This study suggests that **markets react negatively** in the **short term**.



A second study** suggests that in a **one-year period**, companies that are victims of a major cyberattack **under-performs** by **8,1%** against the expected results and by **14%** over **2 years**.

The **immediate negative reaction** following an announcement underlines the importance of having a **clear** and **effectively** managed **crisis communication** in order to avoid uncontrolled and/or **misleading communication** (or worse, letting the **hackers communicate** and leverage the fear of negative brand impact).

Source: * The dynamics of Stock Market Responses following the Cyber-Attacks news: Evidence from event Study - Dewan Muktadir-Al-Mukit & Md Hakim Ali - 2025
** The impact of information security events to the stock market: A systemic literature review - Spanios & Angelis - 2025



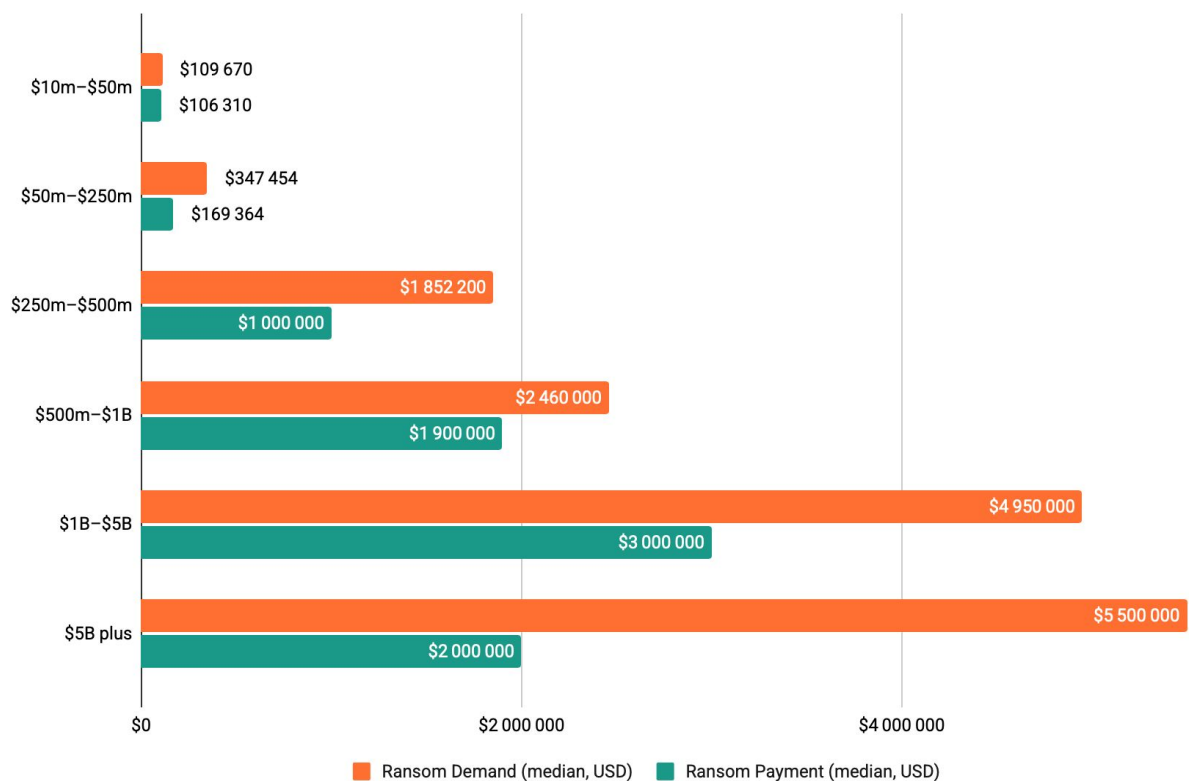
Focus: Insights on Ransom payments

A growing number of companies implement **“no payment” policies**, but in a dire situation, organizations can be tempted to **reduce** the **disruption** time by paying the ransom.

If this question can create **strong debates**, the fact that a significant amount of companies decides to pay (between **36%** and **49%** based on different reports), means the questions cannot be dismissed so easily.

From a strict **financial perspective**, the **cost** of weeks of **impaired activity** is likely to be **higher** than the **ransom**. The average ransom in **2025** was estimated to be **1.3M\$**. Furthermore, some **cyber insurances** cover **ransom** payments and **negotiations**.

Exhibit 7 : Ransom demand vs ransom payment split by company annual revenue*



Source: * Sophos - The state of ransomware - 2025

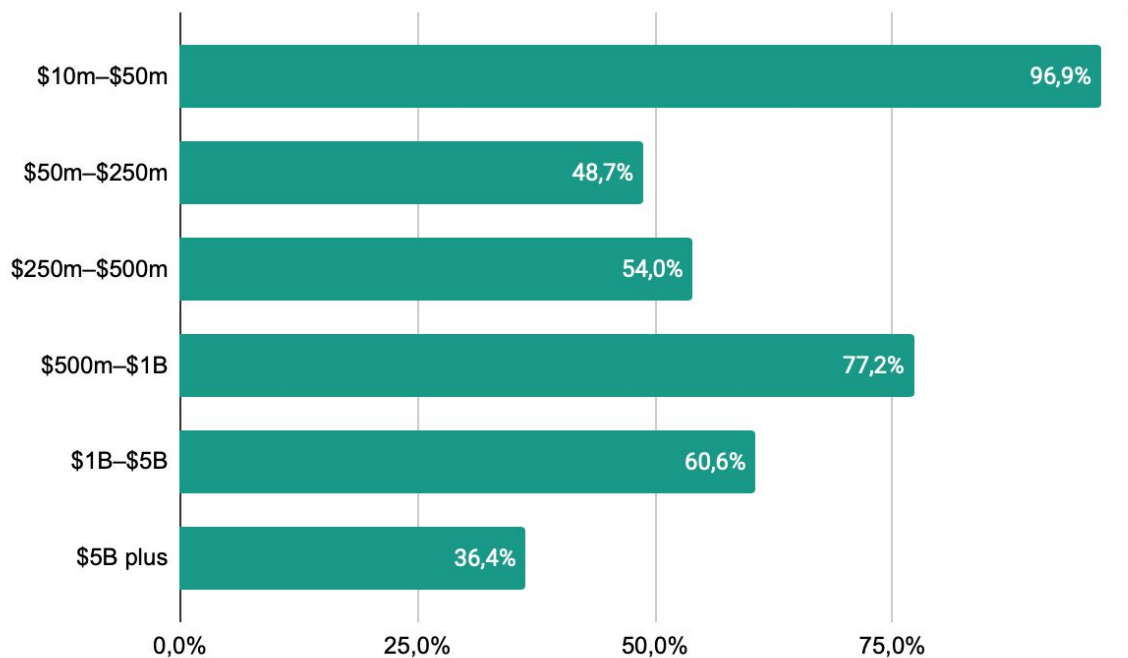


Exhibit 8 : Payment as % of the ransom demand*

Putting aside the financial question, paying a ransom **generates new risks** that need to be kept in mind:

- ▲ Paying doesn't mean the data will be **handed over**. The decryption can be slow or only allow partial recovery;
- ▲ Paying doesn't mean your data will **be erased** afterwards and could still be used, published or **sold** to another party;
- ▲ Paying a ransom is **generally legal** but organizations should keep in mind that attackers are **criminal organizations** and that paying ransom could, under certain circumstances, be seen under certain circumstances as a **direct funding**. The risk that a European company could be **prosecuted** in **another country** for this motive **cannot be ruled out**.

Source: * Based on Sophos - The state of ransomware - 2025



◆ The waterline: impact on EBIT and M&A

Impact on EBIT

Following a business disruption, EBIT will face a “**pincer movement**” due to:

▲ Revenue destruction

Turnover loss is a direct result of a **business disruption**. This situation is especially true for companies operating in **dynamic markets** where customers can easily turn to competitors, possibly leading to a sub-consequence: **customer churn**.

▲ Increasing operational charges

As mentioned, the incident management, recovery and catch-up will generate **extra costs** that could be **temporary** or **lasting**, should there be, for example, legal proceedings requiring counseling.

Even though contracts are now integrating cyberattacks as **force majeure** clauses, **contractual penalties** can be added to the equation. Depending on the nature of the business, it can be a **revenue loss** or **OPEX increase**, but nevertheless, impacting **EBIT**.

Additionally, a “**productivity tax**” could be added to the EBIT impact. Following the business disruption, all **employees** will likely **focus** on **remediation** and treating the backlog **instead** of pursuing **growth** and reaching initial business objectives.

On **monolithic markets**, this **EBIT impact** might be **shorter** over time whereas in **dynamic markets**, the impact on revenue due to **customer loss** could have a lasting impact on EBIT.

This **depth of financial impact** is often **overlooked** in **risk assessments** but is paramount for **recovery**.





Impact on M&A

Cybersecurity and data protection have become **scrutinized topics** in **Mergers & Acquisition (M&A)**, certain companies conducting now **cyber-due diligences**.

For companies in the process of being acquired, any **perturbation** can **influence** the outcome of the **transaction** even after the signature.

The case of **Asco** is quite instructive. In May **2018**, **Spirit Aero** announced a deal to buy Asco, a Belgian aircraft parts supplier for **650M\$** in **cash**. A formal approval by the **European Commission** was delivered in **March 2019**.

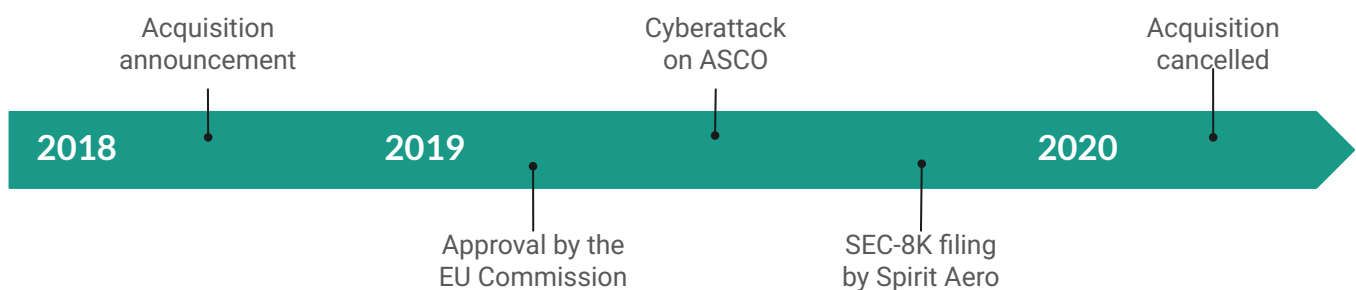
In **June 2019**, **Asco** was hit by a **ransomware**, leading to a complete **production stoppage** on several manufacturing sites. Around 1000 employees had to stop their activity. The complete recovery was only possible by **mid-July**. The cost of **IT remediation** is estimated to be **20M€**.

In **July 2019**, Spirit Aero extended the deadline to terminate the deal if closing conditions weren't met, required all information on the cyberattack and requested **150M\$** in **damage**, increasing **escrow** by **40M\$**, reaching then **80M\$***.

In **September 2020**, Spirit Aero **ended** the **deal**. Asco was later acquired by Montana Aerospace for an undisclosed amount.

Analysts have pointed out that Spirit Aero was also facing complicated financial and market-related circumstances that might have motivated them to cancel the deal. Nevertheless, the **financial impacts** generated by the **cyberattack** have been **significant** enough to **jeopardize** the acquisition and adversely impacted Asco's **finance** and **market value**.

Exhibit 5: ASCO Industry - Spirit Aero deal - Timeline



Source: * Aronberg Goldgehn - Business Law Alert - Mergers & Acquisitions: Cybersecurity traps for the Seller & Buyer - 2020



The keel: the invisible but long lasting costs

Impact on credit and debt cost

An organization suffering from an **unexpected** and **impactful event** will likely have to face a **third wave** of **financial impacts**. Studies* have shown that after a cyberattack:

- ▲ companies could face **higher loan spreads** (up to 30 points)
- ▲ access to **credit** could be more **restrictive**

Organizations with a **higher credit risk profile** prior to the cyberattack could face additional difficulties to access credit.

Of course, should the organization be in need of an **emergency loan** to complete or supplement the treasury, **higher rates** could be applied by financial actors.

These restrictions could also **adversely impact** the **investment capacities** and contribute to **limiting** the **ability** to flatten the backlog of activity due to business disruption.

Impact on premiums for cyber insurances

After a **volatile period**, where surging ransomware attacks forced cyber insurances to **hike prices** and **tighten coverage**, increased corporate cybersecurity spending has successfully reduced claim severity, restoring cyber insurer profitability and shifting the market back toward **buyer-friendly rates** and broader terms.

Reports also emphasize the fact that insurers are now applying **stricter requirements** to *"obtain or keep their insurance coverage**"*.

But following a cyberattack, **premiums** could be **increased**. For example, by first **cancelling** out the **market-wide rate decrease** the company would have otherwise benefited from, and then by applying an **additional risk premium** on top.

Source: * Cybersecurity Risk and the cost of debt - Amy G. Sheneman - 2021
 ** Demystifying Cyber Insurance: Today's Trends & Tomorrow's Challenges - FERMA - 2025



Impact of Fines

Since 2018, with GDPR coming into force, several new regulations like NIS 2, SEC cybersecurity disclosure rules or CRA* are now imposing **security requirements** on companies subject of **fines**.

Organizations have since been progressively considering **cybersecurity** through the **compliance lens**, fearing up to **4%** of worldwide turnover fines.

If indeed European data protection agencies imposed **1.2 billion euros** in fines in **2025**, statistics show that they **rarely exceed 1%** of global turnover. Furthermore, in comparison to the number of data breaches notified, the **number of fines** is **modest**.

From a **financial standpoint**, the duration of **investigations** allow time to **provision** for this risk (between 12 and 24 months in France for example).

This provision for **loss contingency** will appear as **non-operating expenses**, decreasing the **net income** and adversely affecting the **cash flow**.

Exhibit 6: Number of data breach notification and fines between May 2018 and January 2026**



CRA* Cyber Resilience Act

Source: * Based on GDPR fines and data breach survey - DLA Piper 2026 and GDPR Enforcement Tracker by CMS Law Tax Future



Focus: Insolvency following a cyberattack

In cybersecurity there is an **urban legend** "One in two businesses facing a cyberattack will go bankrupt within six months". This figure is repeated as a mantra but is not accurate, and furthermore, **misleading**.

Small and medium companies are usually more **vulnerable** to cyberattacks because they generally **lack** the **budget** or the **skills** to keep up with the **evolving cyber threat**. They are more targeted by hackers understanding this situation and assuming they would be more prone to pay a ransom.

While if many **SMEs** facing a **cyberattack** will bear the **stigmas** for a long time, only few are going **out of business** due to cyberattacks. There are some publicly known examples of the companies going out of business due to cyberattacks (**Fosana***, **KNP**** or **Stoli*****), yet in all these dramatic cases, the cyberattack was just the **last blow** to **already fragile companies**.

The types of impacts from a cyberattack vary from a company to another, but it always creates **unforeseen extra costs** to address:



Business
disruption



IT
Rebuilding



Human
Resources



Insurances



Customer
satisfaction



Legal

From a **financial standpoint**, this implies **direct** and **lasting impacts** on **EBIT** (Earning Before Interest and Taxes) **and consequently on cash**. If a company is already in a complicated financial situation with **low cash** and **limited** capacity to **leverage** debt or other funding sources, a cyberattack might be the **last nail** in the **coffin**.

Source: * A ransomware attack pushed the german napkin firm fasana into insolvency - Security Affairs - 2025
 ** The Knights of Old cyber-attack – a salutary lesson for all businesses - Clear Insurance Management - 2025
 *** Vodka maker Stoli's US companies file for bankruptcy after cyberattack - Reuters - 2024



Knowing the financial exposure to master cyber risks

Cyber risk is a business risk. The current geopolitical environment and threat evolution increases cyber risk pressure on companies. Just like any other risk, **understanding** the **potential cost** allows companies to **adequately provision** for this risk or to **mitigate** by **reducing** its **likelihood** or **impact**.

Understanding the financial exposure to cyber risks **allows the board** to:

- ▲ **Accurately position the cyber risks in regard to other risks**

Currently, most risk frameworks offer a heat map with *low / Medium / High / Very High* financial threshold that **doesn't help C-level** executives to **take** enlightened **decisions** because the financial assessment is rarely accurate. These heat maps give (at best) a **frozen picture** of the financial impacts.

But what a **CFO** needs is way more **complex data**: impact on **cash**, **EBIT**, **duration** to **financially recover**, etc.

- ▲ **Allow enlightened decision regarding mitigation**

These **inputs** will **drive** the **mitigation strategy** and the **budget** linked to it, not only for cyber or IT-solutions, but also for **business continuity** or **operational workarounds**.

As an example, a manufacturing company could decide to invest in additional buffer stocks to avoid an operational shutdown during the IT recovery. But this **buffer stock** is a **financial immobilization** that could be **depreciated** should it not be stocked properly, generating risks by itself. So knowing the **cost-avoidance** that this buffer stock could bring is a **key decision driver**.

As another example, a company wishing to postpone an obsolete system replacement, could decide that to mitigate the risk, it could **provision cash** in order to **increase** its **capacity** to cope in the event of a disruption.

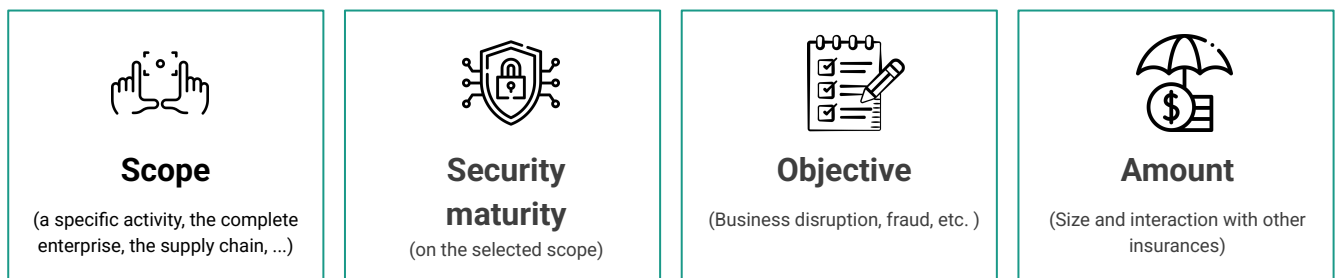


▲ Adjust the cyber insurance coverage

Cyber insurance is a **mitigation** measure that can provide **two main benefits**: **shorten** the **crisis** period by providing external support (when present in the contract) and **reduce** the **financial impact** if defined properly.

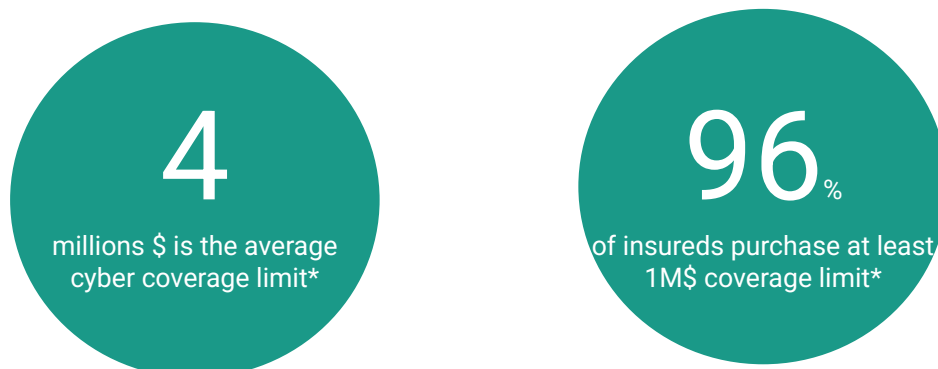
For this last point, some points to consider:

- △ **Sizing** the right level of **coverage** is the first challenge and requires understanding the following:



- △ The main **pitfalls** are **underestimating coverage** needs, overlooking policy **exclusions** or misjudging the financial **value** of the **crisis support**;
- △ Even if the coverage is well defined, the cyber insurance **market** is **volatile** and might be **unable** to **provide** the **needed amount** (pushing companies to leverage **captives** and control the cost and structure of their cyber risk financing).

But cyber insurance is not a **silver bullet**, even companies like **Marks & Spencer**, with a significant **100M£ coverage**, could not be completely covered, therefore, **further investment** was needed.



Source: * AWS Outage: Market Impacts and Coverage Implications - AMWINS - 2025



They can also be hard to **trigger properly**:

- △ Whenever a cyber incident happens, the **window to declare** it to the insurer is **limited**. In the first hours or days of the incident, it is hard to know if the **overall cost** will **exceed** the **deductibles**;
- △ Having **several scenarios** of loss with **in-house figures**, even if it doesn't match with the exact scope of the attack will still give an **overall estimation** of the worst case cost.

Once the insurance is triggered, depending on the **magnitude** of the event, there is a possibility that the cyber insurance may be able to **reinstate** the **initial coverage** and therefore be a **one-time safety net**;

- △ There have been discussions about **systemic events**, an attack that would **massively impair** a common supplier of **thousands** of **companies**. Currently the market would not be able to face such an event and governments would have to take **Covid-like** measures like for **Jaguar Land Rover's supply chain**.

▲ **Define where to invest cybersecurity budget first**

Knowing their financial exposure to cyber risk will also allow organizations to **answer the hard question: where will money actually secure the business?**

In an **economically complicated landscape**, some organizations have to be **conservative** with their **budgets**. It is often complicated for CFOs and other board members to really **understand** if the **investments** requested will **effectively mitigate risks**. Traditionally, CISOs presented security risks in terms of vulnerabilities, monitoring or certification opportunities. Over the last few years, there has been a shift in the conversations, bringing them to speak about **business impacts**. When explaining that there is a high possibility to face a minor disruption of the customer service, C-level members globally **picture** the **financial impact** but not with **enough precision** to understand that the budget to extend the SOC capacity would be worth it.

In addition, **understanding** the **cost** of the **cyber incident** is important, but presenting the **remediation plan** and an estimation of its **financial benefits** could help the board to make an **investment decision**.



Focus: Marks & Spencer, one year of profit erased

Marks & Spencer suffered a **major cyberattack** in April 2025. The intrusion was detected over the Easter weekend and **disrupted operations** for weeks.

M&S had to suspend parts of its **online orders** for **6 weeks** and **click and collect** for **15 weeks** leading to a significant loss in **operating profit reflecting on Half Year 2026 results**. Though the cyber **insurance** covered the losses up to **100M£**, the direct cost and the shortfall **exceeded** this **coverage**.

Overall, it was one of the most significant recent cyber incidents affecting a UK retailer.

Exhibit 9 Marks & Spencer financial impact of the cyberattack

KPI	Half Year 2025* (Issued 6 nov 2024)	Half Year 2026** (Issued 5 nov 2025)	Full Year 2025 (Issued 29 March 2025)
Direct cost	-	-£136M	-
Shortfall (sales)	-	-£324M	-
Insurance	-	£100M	-
Turnover	£6.5b	£7.9b	£13.7b
Operating profit	£462.7M	£251.4M	£990.3M
Profit before Taxes (PBT)	£413.1M	£184.1M	£890M
Free Cash Flow from operations	£16.3M	£193M	£474.3M
Food adjusted operating margin	5.1%	2%	5.2%
Fashion, Home & beauty adjusted operating margin	12%	2.7%	11.2%

Source: * Marks and Spencer Group Plc - Half Year Results for the 26 Weeks Ended 28 September 2024
 ** Marks and Spencer Group Plc - Interim Half Year Results for the 26 Weeks Ended 27 September 2025



Measuring the value of cyber investments

"Security is not usually an investment that provides profit but loss prevention"

Security as a normal state of work, is **difficult** to **financially assess**. You can value the cost of insecurity but the opposite is usually complex. This peculiar situation makes it **difficult** for information security professionals to **request budget increases** (or to avoid budget cuts).

Over time, different methods deriving from traditional ROI or with **different approaches** have been used to financially **quantify** the **benefits** of **"being secure"**.

Bellow are some of the indicators used to assess the worth of cybersecurity investments:

Indicator	Used for	Approach	Inputs	Outputs
Cost-Benefit Analysis (CBA)	Strategic "Go/No-Go" decisions for projects.	Total Benefits - Total Costs	Estimated gains, implementation costs, and maintenance.	A net financial value or ratio.
Return on Security Investment (ROSI)*	Justifying a specific security tool by measuring the risk it avoids.	(Monetary Loss Reduction - Cost of Control) / Cost of Control	Threat rates, incident costs, and the solution's price.	A percentage (%) of return on the spend.
Annualized Loss Expectancy / Single Loss Expectancy (ALE/SLE)**	Quantifying the average expected annual loss for specific threats.	ALE = SLE x Annual Rate Occurrence	Asset value, exposure factor, and frequency (ARO).	Expected annual loss in currency.
Cyber Value at Risk (CVaR)***	Communicating catastrophic enterprise risk to the Board.	Monte Carlo simulations	Revenue, assets, exposures (\$), and security controls.	Currency value of a "1-in-20 event".

Exhibit 10 - Examples of indicators used to value cybersecurity investments

Source: * Introduction to Return on Security Investment - ENISA - 2012

** Augmented Risk Analysis - Bella, Bistarelli, Peretti & Riccobene - Electronic Notes in Theoretical Computer Science - 2007

*** Cyber Value-at-Risk (Cyber VaR) - Marsh Risk Consulting - 2017



Depending on the organization, these indicators can **provide** the **expected outcome**. But some will need a **higher level** of **maturity** or be more adapted to **larger companies**.

Alternatively, **Cyber Risk Quantification (CRQ)** will allow organizations to understand the **financial exposure** by assigning currency value to cyber risk and **prioritize budget** allocation.

For CRQ, two main methodologies exist:

▲ **FAIR (Factor Analysis of Information Risk)**

FAIR works by decomposing risk into measurable factors. It moves away from subjective labels (like "Medium Risk") and instead **asks two fundamental questions**:

- △ **Frequency**: How often will a loss event happen
- △ **Magnitude**: How much will it cost when it does

The methodology uses a **taxonomy** (a specialized hierarchy) to break these questions down further. For example, **frequency** is determined by **how often** a threat agent attacks and **how vulnerable** your defenses are. **Magnitude** is determined by both the immediate "**primary**" **costs** and the "**secondary**" **costs** like legal fees or reputation damage.

FAIR accounts for **uncertainty** using **Probability Distributions**. To address the complex question of probability, FAIR uses **Monte Carlo simulations**. The model runs thousands of "**what-if**" **scenarios** based on ranges you provide (For example, "*This could happen between 1 and 5 times a year*").

The result is usually expressed as an **Annual Loss Expectancy (ALE)**

$$\text{ALE} = \text{Expected Frequency} \times \text{Average Loss Magnitude}$$

This allows organizations to see their risk as a bell curve of probable outcomes rather than a single, static guess.

FAIR needs **quality data inputs** to correctly assess the risks and will require **resources** in **time** and **people** but will prove quite **effective** for **justifying budgets** and changing the way cyber risks are presented to executives.



▲ SPICE (Scenario Planning for Identifying Cyber Exposure)

SPICE is a **risk-based** and **business-centric** methodology developed and used within **Airbus Group** since **2016** to quantify the financial impact of catastrophic cyber events on its business operations.

This methodology **shifts** the **focus** from purely technical vulnerabilities to **tangible business consequences**.

SPICE is a two-phase methodology:

- △ **Identify** with business representatives their **most feared events** and **quantify** the **cost** of the consequences to provide an **initial scenario**;
- △ **Identify** with business representatives the **relevant mitigations** and **quantify** the **mitigated** scenario.

The process relies on a "**triple validation**" principle:



Business leaders identify
"most feared events"



Cybersecurity experts
confirm technical feasibility



Financial controllers
calculate the actual costs

The **financial figures** of potential losses are measured in **EBIT** and **Free Cash Flow (FCF)** over a **recovery period** of up to six years.

This specific approach offers **depth** to understand the financial exposure and recovery time.

Based on **internal financial figures** rather than **market benchmarks**, it allows management to have a **contextualized** understanding of the business consequences and their cost over years.

This **straightforward** methodology, doesn't need specific inputs but will need **engagement** of both **business** and **finance leaders** to deliver **valuable insights**.

These quantified **before-after scenarios** allow management to take **informed decisions** regarding investments in cybersecurity projects.



Key takeaways

The era of treating cybersecurity as a "**black box**" of technical **expenses** is over. As this paper has demonstrated, **cyber risk** is not an IT problem—it is a **sophisticated financial variable** that directly affects **liquidity, profitability**, and long-term enterprise **value**.

For the **Strategic CFO**, the challenge is no longer just about defending the perimeter, but about **mastering** the **financial narrative** of **resilience** by moving away from qualitative "heat maps" and embracing **Cyber Risk Quantification (CRQ)**.

The path forward for 2026 and beyond requires three decisive shifts:

1. **Integrating Cyber into Financial Planning:** Treat cyber investment not as a sunk cost, but as a strategic hedge against **EBIT volatility**.
2. **Leveraging Cyber Risk Quantification:** Knowing the cyber exposure will not only allow organizations to effectively assess the **value** of **investments** but also **unlock** new **capacities** for finance leaders in **strategic conversations** with **Executives** and peers.
3. **Quantifying the "Submerged" Costs:** Accounting for the long-term "keel" of the iceberg—credit spreads, insurance premiums, and M&A valuation—is essential for true **risk transparency**.

In an economy where **digital** infrastructure is the **backbone** of all **revenue streams**, the **ability** to **quantify** and **manage** cyber risk is becoming a **competitive advantage**.

Those who lead this transition will not only **protect** their **balance sheets**, they will build the **capacity** to **overcome** uncertainty and to thrive in an **increasingly volatile** global **context**.





About Utgard

Utgard Cyber Risk Consulting is an **independent** Swiss-based consulting firm helping companies to **navigate** the cyber **threat** landscape.

By leveraging an **extensive experience** in multicultural environments, Utgard has been able to serve different sized companies and various **industries** (aerospace, banking, biotechnology, luxury, logistics, etc.)

Whether through **cyber risk quantification**, risk management, program management or **supply chain** cybersecurity, Utgard has only **one goal**: **protect** its **customer' business** and make cybersecurity a **business enabler**.





Utgard

Cyber Risk Consulting

Utgard Cyber Risk Consulting - May 2026
© All rights reserved.
www.utgard.pro