

November 2024

'NO-IT' is no IT problem

Becoming operational resilient,
a leadership imperative

Table of contents

	Executive summary	3
1	Introduction	5
2	Talking with business leaders about cybersecurity	6
2.1	Uncertainty about expertise needed	7
2.2	Compliance takes precedence over business value	7
2.3	Risks and investments not aligned	8
2.4	Addressing blind spots in IT outage preparedness	9
3	Findings from the conversations	10
4	The systemic risk of a tick-box culture	13
5	Four principles of operational resilience	18
5.1	Whole system in the room	18
5.2	Operational risks across functions	19
5.3	Risk tolerance and financial impact	20
5.4	Organizing and testing for continuity and recovery	21
	Appendix	24
A	The authors	24
B	Sources	25

Executive summary

This report presents the results of a study conducted among board members and advisory board members from large organizations to assess the current state of cybersecurity in the business sector. The key question driving this research was: “Are we truly in control and prepared for cyber disruptions?”

The study included in-depth interviews with these executives to gain valuable insights into their perspectives, supplemented by extensive desk research and participation in multiple seminars on cybersecurity and upcoming regulations.

Our conversations revealed a unanimous acknowledgment: cyber threats are an unavoidable reality. The risk goes beyond ransomware attacks or sophisticated hacks, it also includes major operational disruptions caused by human or technical errors. Despite this, many organizations continue to view cybersecurity through a narrow, technology focused lens. This fragmented perspective often fails to address the systemic risks posed by today’s complex and evolving threat environment.

Many organizations face increasing regulatory demands relating to digital resilience. While compliance with these regulations is important and beneficial, it became evident from the interviews that focusing solely on compliance can even distract organizations from addressing the underlying risks effectively.

Executives acknowledged a gap in understanding the broader IT impact across their organizations. They rely heavily on experts and confidently delegate responsibility for these matters. However, this raises an important question: is delegation sufficient? We believe it is not.

A critical insight emerged: framing challenges as a “digital resilience” issue reinforces the misconception that they are purely IT problems. In truth, they represent threats to operational resilience in a digital era. The phrase “No-IT is no IT problem” highlights that cyber risks are fundamentally risks to organizational continuity. These are not just technical concerns; they directly impact how businesses operate and thrive in an increasingly digital landscape.

A shift in mindset is necessary. Organizations must view operational resilience as the foundation for implementing measures to ensure business continuity. This shift demands direct ownership from executive leadership, it is not an issue that can be delegated.

True operational resilience is not just about adding more layers of protection, it’s about rethinking how to prepare for and recover from incidents. The reality is, it’s not a question of if your organization will be impacted, but when.

While executives recognize that it's impossible to maintain full control over all risks, this does not relieve them of the responsibility to take control of the aspects they can manage effectively.

This report underscores the importance of adopting an organization wide approach to operational resilience by strengthening digital resilience and cybersecurity. Governance, operations, and risk management strategies need to be reviewed.

To facilitate this, the report outlines four essential guidelines for operational resilience:

The four principles for operational resilience.

Whole system in the room

Build multi-disciplinary teams that address risks collaboratively. Extend these efforts beyond internal teams by involving key partners across the value chain. Unified collaboration strengthens defenses and enhances resilience across the ecosystem.

Operational risk across functions

Evaluate risks from a business operations perspective, emphasizing cross-functional collaboration to gain a comprehensive understanding of vulnerabilities.

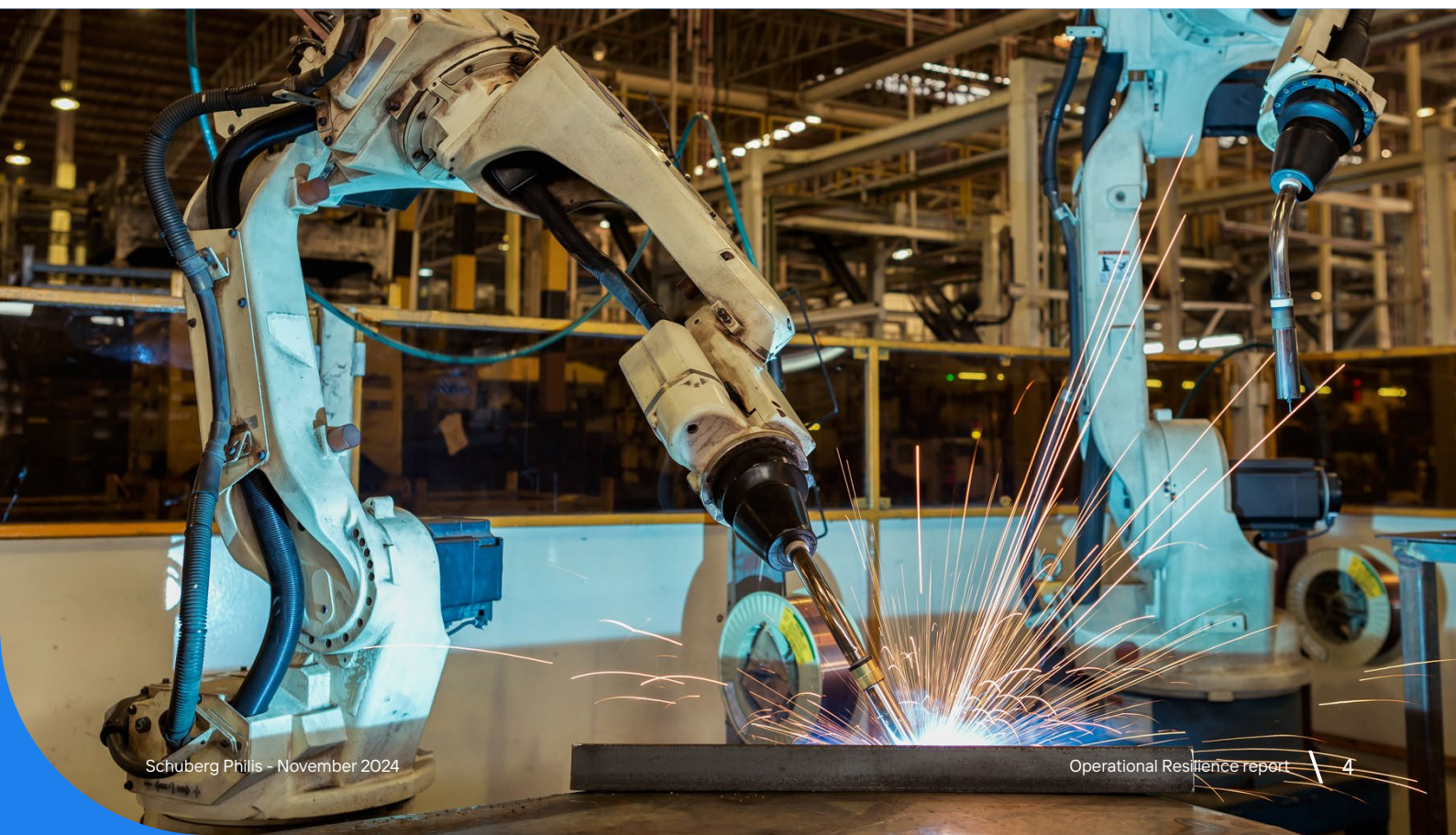
Risk tolerance and financial impact

Recognize that risks and opportunities are interconnected. Focus resilience efforts on the most critical areas, directing resources to protect and recover key assets.

Organizing and testing of continuity and recovery

Develop and rigorously test recovery processes to ensure rapid responses to disruptions, maintaining operational continuity.

Through this report, we aim to promote a collective approach, paving the way for a future proof and resilient society.



Introduction

Cyberthreats such as ransomware attacks, sophisticated hacks, and operational disruptions caused by human error are becoming increasingly frequent and complex. Beyond their immediate impact on organizations, these threats can disrupt essential services, creating ripple effects that extend across society.

This report presents the findings of research conducted among executives from large organizations, aiming to evaluate how prepared businesses are for cyber disruptions. The central question driving this research was: "Is leadership truly in control and ready to handle cyber threats?"

These interviews revealed a critical truth: cyber threats are an unavoidable aspect of doing business. The risks, from ransomware attacks to operational disruptions caused by human error, are not only escalating but also growing in complexity.

As these risks intensify, regulatory demands for digital resilience are also on the rise. While compliance with these regulations is crucial, another important question arises: Does regulatory compliance alone create truly resilient organizations? Through the interviews, we explored how leadership is striving to gain control within their organizations.

The findings in this report are based on a multi-faceted research approach designed to deliver actionable insights:

- 1 In-depth interviews:** Conversations with executive board members from large organizations formed the core of the research. These interviews provided valuable perspectives on the challenges, strategies, and opportunities for enhancing cybersecurity readiness.
- 2 Extensive desk research:** thorough review of existing literature and emerging trends offered a foundational understanding of the broader cybersecurity landscape. This included key developments in regulatory requirements and best practices.
- 3 Seminar participation:** Attendance at multiple cybersecurity seminars added practical insights, particularly regarding upcoming regulations and the common challenges organizations face in adapting to a rapidly evolving threat landscape.

By combining these methods, this report captures both the strategic priorities and operational realities of organizations as they navigate the growing risks posed by cyber threats. The goal is to provide a comprehensive understanding of how executives are addressing these challenges and to identify practical pathways for building greater resilience.

Talking with business leaders about cybersecurity

Most executives express confidence in their organization's security posture and operational resilience. While this confidence reflects their belief in the systems and processes in place, they openly acknowledge the limitations of their own cybersecurity knowledge. They understand that achieving full control in this complex and ever evolving domain is by definition unachievable..

Despite these challenges, executives prioritize cybersecurity within their organizations. Recognizing the importance of specialized expertise, they place significant trust in both internal teams and external experts to guide them through the complexities of the cyber threat landscape. This reliance on collaborative efforts underscores their commitment to maintaining resilience and safeguarding their organizations against potential risks.

Several quotes
from the interviews

"I don't have time and the knowledge to delve into the appropriate level of detail, but I do have capable people for that."

"I have too little knowledge of which processes carry a high risk and, as a result, of the vulnerability of my company."

"If we have to choose between eliminating the certainty of a fine for non-compliance or reducing the actual risk, we choose to eliminate non-compliance."

"The code of good governance does not state that knowledge of technology is necessary."

"I have at least minimal certainty that things are taken care of, but if you ask me how to assess that financially... no idea."

"We already have been hacked, we've learned from it and we're safe now. "

2.1 **Uncertainty about expertise needed**

At the same time, the overwhelming volume of information about the ever-expanding threat landscape creates a degree of uncertainty. While executives generally feel secure, given their access to expert guidance, the question remains whether this access to expertise alone is sufficient. As technology evolves rapidly, even those with strong IT backgrounds acknowledge the limits of their knowledge.

Additionally, new regulations from both EU and national authorities are placing greater responsibility on leadership, prompting concerns on how these risks and regulations might impact future investments and personal liability. This sense of uncertainty became evident during the in-depth interviews we conducted.

By acknowledging the complexity of fully understanding the scope and impact of IT and cyber risks, critical questions can be raised, such as: What expertise is truly needed? Is leadership in control of the organization's crown jewels, critical processes, and operational resilience? How recoverable are these critical processes in the event of a major incident—or, worse, a No-IT scenario? What is the financial (materialized) impact of such an incident?

2.2 **Compliance takes precedence over business value**

Compliance has become a central focus for executives as they navigate through increasingly complex conversations with regulators. To manage this, many organizations rely on color-coded reports from CISOs, flagging risks in red, orange, or green. These color-coded reports guide executive decisions, with the belief that addressing individual controls will reduce overall risk. However, while it checks the compliance boxes, it doesn't always tackle the deeper, underlying risks. As one supervisory board member honestly noted: *"If we have to choose between eliminating the certainty of a fine for non-compliance or reducing the actual risk, we choose to eliminate non-compliance"*. This sentiment highlights the tendency to focus more on complying with basic regulatory requirements than on actually reducing the real cyber risks.

No resistance against the regulatory objective

Executives recognize the need for regulations, they acknowledge the value in safeguarding their organizations. At the same time, there's a strong call for more practical collaboration between regulators and the market. A lack of clear, unified interpretation of regulations leads many organizations to focus on simply doing the minimum to comply.

Regulatory fatigue

'Regulatory fatigue' is a growing concern among executives. The increasing complexity of regulations has led many organizations to adopt a checklist approach to compliance, which may not fully address their actual vulnerabilities. Executives feel the mounting pressure, as compliance officers and CISOs find themselves constantly keeping up with regulations like DORA, NIS2, and upcoming AI standards. As one executive put it: *"We face a heavy load of regulations and audits, and balancing this with innovation and business growth is becoming a real challenge."*

Focus on business continuity

At the executive level, there is a growing need for financial insights around operational risks and the strategies needed to mitigate them. While many leaders are already aware of the importance

of addressing cybersecurity threats, the challenge often lies in demonstrating the clear business value these efforts bring. It's important to close the gap between regulatory compliance and real cybersecurity effectiveness, ensuring that risk management efforts are not only about meeting requirements but also adding value to the business.

By shifting focus from just compliance to business continuity, executives can better understand how their cybersecurity strategies support business continuity, even in the face of major disruptions. The key is to recognize that effective risk management strengthens the organization's ability to keep operations running smoothly, no matter the challenge.

Ultimately, the goal is to ensure that the business is prepared to handle disruptions while minimizing downtime and maintaining trust with customers and stakeholders. By adopting a proactive mindset, executives can create a stronger, more resilient organization that not only meets compliance standards but thrives even when faced with unexpected challenges.

2.3 Risks and investments not aligned

A critical challenge was revealed during our conversations with board level executives: the difficulty of connecting cybersecurity investments directly to their impact on operational risk levels. This disconnect often leaves decision makers without a clear framework for prioritizing resilience initiatives.

Overcoming the perception of cost without value

A recurring theme was the perception that cybersecurity is a cost center, lacking tangible contributions to competitive advantage or business value. While digital transformation has accelerated the adoption of new technologies, it has frequently failed to embed resilience as a foundational element. Many leaders acknowledged struggling to contextualize cyber risks within broader business priorities, which hampers the integration of resilience into strategic decisions.

This challenge becomes particularly acute during mergers and acquisitions, where due diligence often neglects the impact on cyber and operational resilience. This oversight can expose the organization to significant vulnerabilities, weakening its overall security posture post-acquisition.



Addressing the materialized impact of risks

A lack of actionable insights into the materialized impact of cyber and operational risks was consistently pointed out. This gap not only increases hesitation but also undermines confidence in allocating resources effectively. Leaders recognized that economically driven decision making, grounded in a clear understanding of risk scenarios and potential outcomes, is essential to overcome resistance to cybersecurity investments.

Shaping a strategic response

The consensus on the need for meaningful board level discussions to drive alignment between resilience strategies and business objectives is a key outcome of the conversations we had.

Leaders emphasized the importance of answering pivotal questions:

- 1 — Where should resources be allocated to achieve the greatest risk reduction?
- 2 — How can investments in resilience provide measurable returns in operational stability and business continuity?
- 3 — What frameworks are needed to translate technical risks into business language?

2.4 Addressing blind spots in IT outage preparedness

Most executives referred to practices like penetration testing and vulnerability scanning as proof of their cybersecurity readiness. Yet, our conversations revealed a recurring issue: the stark gap between these measures and the frequently neglected risks of No-IT scenarios. When asked about the potential for complete IT outages, it became clear that a critical blind spot persists.

While business continuity plans (BCPs) are widely in place, executives acknowledged that these plans are rarely, if ever, tested against realistic and large-scale scenarios where the entire digital infrastructure is unavailable. The absence of No-IT simulations leaves organizations vulnerable to a gap between theoretical planning and actionable recovery.

Executives were open in recognizing the inevitability of severe incidents, still they expressed considerable uncertainty about their organizations' ability to recover effectively from such disruptions. This lack of confidence underscores a critical need for more rigorous testing and scenario planning, designed not just to identify risks but to stress-test recovery strategies in the most extreme conditions.

Third-party risk

Another pressing concern was the management of third-party risks. Executives frequently highlighted the security vulnerabilities introduced by external partners, noting that many cyber risks originate within the supply chain. However, these risks are amplified by insufficient accountability frameworks, with many organizations unable to pinpoint ownership of risk mitigation responsibilities within their supply chains.

This gap fosters a widespread perception that third-party risks are beyond the control of the organization, further undermining confidence in resilience strategies. Leaders agreed that strengthening collaboration and accountability frameworks within supply chains is essential to reducing this exposure.

Findings from the conversations

Our conversations revealed a unanimous acknowledgment: cyber threats are an unavoidable reality. The risk goes beyond ransomware attacks or sophisticated hacks. It also includes major operational disruptions caused by human or technical error. Despite this, many organizations continue to view cybersecurity through a narrow, technology focused lens.

Operational resilience over compliance

Relying solely on regulatory compliance gives a false sense of security. While meeting standards is important, it often shifts focus away from tackling the real operational risks that can disrupt your business. True resilience isn't about checking boxes, it's about being ready to handle whatever comes your way and keeping the business running when disruptions hit.

Digital Resilience is an operational issue, not just IT

The term "digital resilience" gives the impression that it's just an IT issue. In reality, we're talking about operational resilience in the digital era. Cyber risks impact every part of the business. The phrase "NO-IT is no IT problem" underscores the need for a company-wide approach, where every department plays a role in managing these risks.

Delegation alone is insufficient: leadership must drive operational resilience

The research revealed that many executives place significant reliance on technical experts to manage cybersecurity, often delegating responsibility. Effective operational resilience can't be achieved through delegation alone. Leadership must take direct ownership of cybersecurity, elevating it to a strategic priority within the organisation.

Leadership must take the lead in cybersecurity because it is not just an IT issue, it is a critical risk to business continuity. Cyber threats have the potential to disrupt core business processes and compromise the organisation's most valuable assets, its "crown jewels." Addressing these risks requires a strategic approach driven by leadership, ensuring that resilience is embedded in the organisation's operations.

The term 'digital resilience' gives the impression that it's just an IT issue. In reality, we're talking about operational resilience in the digital era. Cyber risks impact every part of the business.



Operational and digital resilience are frequently overlooked in business decision making

When organizations start with new initiatives, the business case often fails to account for investments in cybersecurity or digital resilience. As a result, these critical costs are added later in the process, disrupting the financial projections and negatively impacting the overall business case.

Similarly, during organizational changes, such as shifts in distribution models or mergers and acquisitions, the impact on operational resilience is often not adequately considered. The key question is: How will these structural changes affect our ability to maintain service continuity in the event of a disruption?

Governance for disruption handling is often unprepared

Research shows that many organizations lack proper governance plans for handling disruptive situations. Have all relevant stakeholders been identified for scenarios like a ransomware attack? Is there a clear mandate for this governance? What principles will guide decision-making during a major disruption? Many organizations have not formalized their preparedness to this extent or tested such scenarios.

Recoverability is considered essential but is rarely tested

Executives view recoverability as a critical aspect of their organizations. However, there is limited data available on how effectively the organization would perform in such situations. Testing to gain this insight is often seen as complex. This challenge becomes even greater when the dependencies and risks associated with third parties are taken into account.

Insights into the impact of potential disruptions are limited

How much damage would a disruption cause? This is a question many organizations struggle to answer due to a lack of data and analytical methods. While models exist for such analysis, their adoption remains very low. Risks are often presented in color-coded reports rather than in a quantified format. Interestingly, organizations that have experienced a major disruption can often estimate the total damage relatively quickly after the event.

Executives view that understanding the material impact of risks would be a valuable factor to include in company valuations.

Final considerations

To build true resilience, organisations must adopt a holistic strategy that transcends departmental and organizational boundaries. By breaking down silos, they can better protect critical processes and ensure alignment with their overall business objectives.

Preparedness is non-negotiable

Cyber disruptions are no longer a distant possibility but an inevitable reality for every organisation. Resilience is not about striving to eliminate all risks, a task that is neither feasible nor practical, but about managing them effectively to maintain business continuity. While complete control over every risk is unattainable, this should not lead to inaction. Leaders must take ownership of the elements they can control, implementing strategies that protect critical operations and prioritising the organisation's ability to recover swiftly from disruptions. Recoverability is not optional, it is the foundation of long-term resilience and organisational success.



The systemic risk of a tick-box culture

The problem: avoiding uncertainty leads to short-sighted behavior.

Uncertainty about the likelihood and impact of risks often drives counterproductive behavior. During our interviews, we observed that many executives, unsure about the scale of potential threats, sought reassurance by focusing on compliance activities: essentially “ticking boxes.” While this creates a superficial sense of control, it raises a deeper concern: what are the long-term implications of this avoidance strategy?

The psychology of avoidance

From a behavioral standpoint, humans naturally shy away from uncertainty and ambiguity. This tendency often results in avoidance rather than confrontation, particularly when risks are complex or difficult to quantify. The *fear-avoidance model*, a concept rooted in psychology, illustrates two pathways:

- 1 — **Adaptive pathway:** If discomfort or pain is seen as manageable, individuals confront it, leading to recovery and growth.
- 2 — **Maladaptive pathway:** If it is perceived as overwhelming, avoidance behaviors take over, creating a cycle of fear and stagnation.

We observed that many executives, unsure about the scale of potential threats, sought reassurance by focusing on compliance activities essentially 'ticking boxes'.

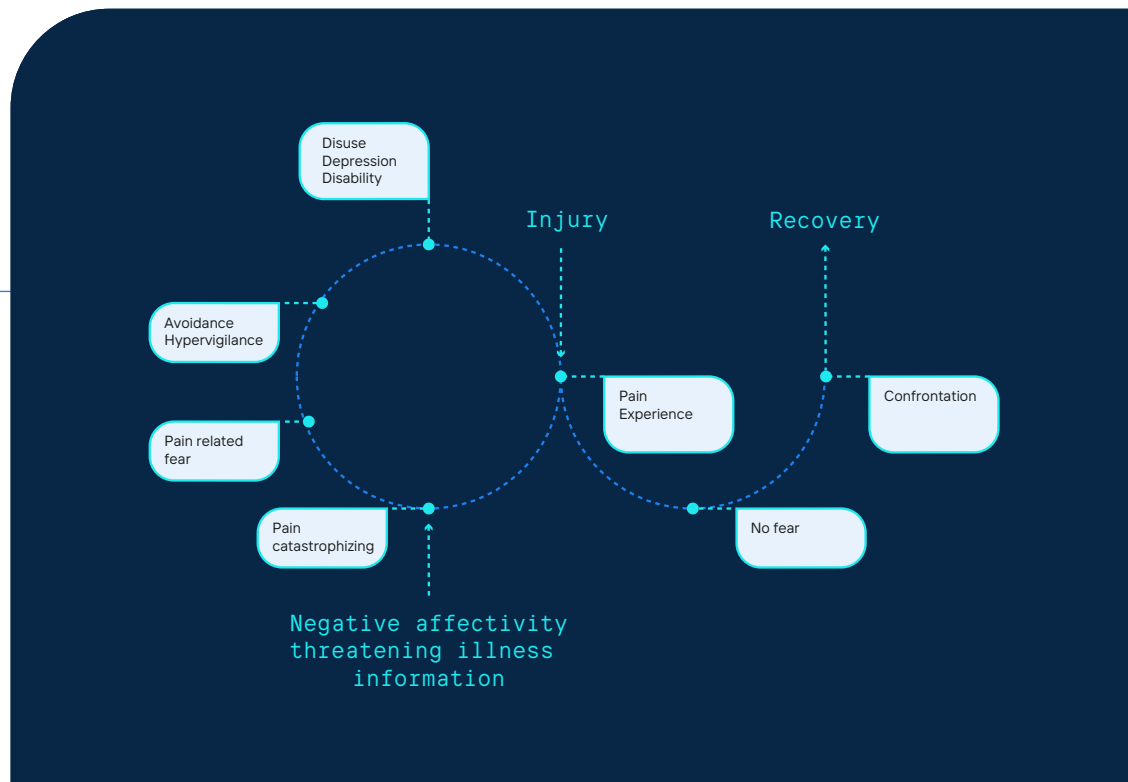
99

The fear avoidance model



Sources:

The fear-avoidance model of pain (J.W.S. Vlaeyen, Journal of Pain, August 2016)



In risk management, this avoidance manifests as an over-reliance on compliance. Leaders may prioritize regulatory adherence, which is measurable and provides immediate reassurance, over addressing the underlying risks that pose real threats to the organization.

Compliance first thinking: a systemic risk to operational resilience

Dialogues with executives revealed a systemic risk in the way organizations approach cybersecurity and operational resilience: a disproportionate focus on compliance first thinking. The pressure to demonstrate “being in control” often drives leaders to prioritize meeting regulatory requirements, as the consequences of non-compliance, such as fines or reputational damage, are immediate and tangible.

However, this compliance driven mindset frequently fails to address the real operational risks organizations face. Instead of enhancing true resilience, it channels resources toward proving the existence of controls, rather than ensuring their actual effectiveness. This creates a dangerous imbalance, where compliance becomes the goal, and operational preparedness takes a back seat.

The systemic prioritization of compliance can perpetuate a false sense of security. While regulatory obligations may be met, they often do little to improve the organization’s overall ability to manage unpredictable and complex risks. This disconnect leaves significant vulnerabilities unaddressed, especially in areas not explicitly covered by compliance frameworks.

Systemic implications

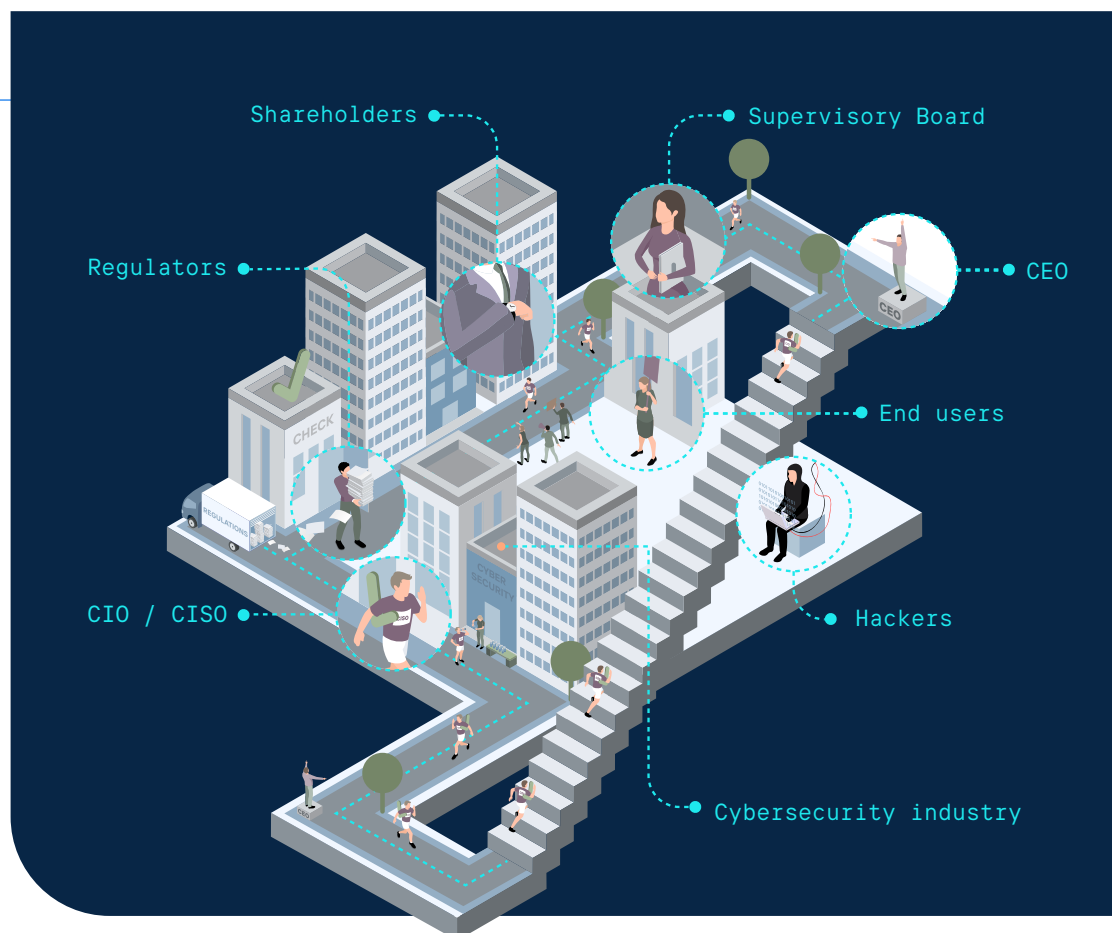
This approach reflects a deeper issue: the tendency to see compliance as a key indicator for resilience. While compliance frameworks are essential for meeting regulatory expectations, they should not define the extent of a risk management strategy. A compliance first focus often creates a systemic blind spot, leaving organizations poorly equipped to handle the dynamic and evolving risks that threaten critical operations.

The diagram below captures the complexity organizations face in managing resilience, shaped by a web of stakeholders whose interests and priorities often collide. Various stakeholders, each with well-intentioned goals, interact in ways that unintentionally reinforce a “box-ticking” mentality. The pressure to demonstrate control, influenced by these overlapping interactions, perpetuates behaviour that prioritizes compliance over true resilience.

Web of stakeholders



Source:
Schuberg Philis,
November 2024



The various stakeholders explained



End users

With the constant news about companies being disrupted by IT failures, such as hacking incidents and system errors which lead to service interruptions, end users are becoming increasingly concerned about the reliability of the services they plan to use.



Supervisory Board

With their extensive knowledge and experience, the Supervisory Board acts as the guiding conscience for the Board of Directors, providing oversight and ensuring alignment with long-term objectives. However, in today's evolving landscape of cyber threats, members are increasingly focused on the organization's resilience.



CEO

The CEO carries the ultimate responsibility for the organization's performance, bearing accountability to the Board of Directors and investors. This includes not only driving growth and achieving strategic objectives but also ensuring that the company operates in a manner that is controlled, secure, and sustainable.

To fulfill this role, the CEO must continually demonstrate effective governance and management practices, often under intense scrutiny. The pressure to "be in control" can lead to an over-reliance on compliance-based approaches, where ticking regulatory boxes is seen as a way to satisfy stakeholders. While this may provide a surface-level assurance, it risks creating a false sense of security if deeper operational vulnerabilities remain unaddressed.



Shareholders

Shareholders place a premium on predictability and stability, expecting the company to achieve its objectives and deliver consistent returns. This predictability drives confidence in the stock's performance and directly impacts the valuation of the company.

However, as the landscape becomes increasingly volatile with rising operational and cyber risks, the ability to demonstrate resilience is emerging as a critical factor in shareholder value. Investors are beginning to scrutinize not just profitability or growth metrics, but the organization's capacity to withstand disruptions and safeguard its operational continuity.



Regulators

Regulators play a pivotal role in fostering a digitally resilient society, where the public can trust in the continuous availability and reliability of essential products and services. Their mission extends beyond merely setting rules, they aim to create a foundation of trust and stability in an increasingly interconnected world.

To achieve this, regulators are introducing and enforcing new laws and standards designed to compel organizations to prioritize resilience. However, this regulatory push also places pressure on companies to adapt swiftly, often requiring significant shifts in strategy and investment.

While compliance with these regulations is essential, the true measure of success lies in an organization's ability to integrate resilience into its core operations. Regulators, therefore, not only set the baseline but also serve as catalysts by enforcing more and more detailed controls. This unintentionally contributes to a tick-in-the-box focus.



CIO/CISO

The CIO and CISO hold the critical responsibility for all IT-related matters within the company, with a primary focus on preventing digital threats and ensuring the security of the organization's digital infrastructure. Their role requires a delicate balance: not only must they manage immediate risks, but they must also build a resilient, future proof IT environment.

In demonstrating their capability and effectiveness to the CEO and the board, the CIO and CISO often face pressure to show control through measurable outcomes, such as compliance with regulatory requirements and the completion of cybersecurity audits. This consequently leads to a focus on "box-ticking", ensuring that all necessary checks are in place to meet the requirements of the regulator and the CEO, rather than addressing broader, more systemic resilience challenges.

While compliance may be necessary, it is not always sufficient to manage the full spectrum of operational risks that digital threats pose.

Ultimately, the CIO and CISO must ensure that the organization is not only compliant but also truly resilient, capable of responding to emerging threats while maintaining business continuity. Their success is measured not only by their ability to meet immediate requirements but also by their capacity to anticipate and address evolving risks in the long term.



Cybersecurity industry

The cybersecurity industry is experiencing rapid growth, driven by escalating societal risks and the rising demand for protective measures. While many solutions focus on mitigating immediate threats, offering organizations an array of safeguards, the industry's emphasis tends to lean heavily on detection and protection. However, these measures, while essential, often fall short of addressing the broader challenge of full-scale operational recoverability. Organizations require more than prevention, they need robust, comprehensive recovery strategies to ensure business continuity during significant operational disruptions.



Hackers

They are becoming increasingly sophisticated and professional in their operations. Not only are they more adept at infiltrating the IT systems of companies and institutions, but their negotiation strategies, which accurately assess what a company or institution can financially endure, are leading to greater success.

Despite the considerable efforts of all stakeholders, the rapid evolution and sophistication of cyber threats seem to outpace the implementation of compliance measures. A sole focus on compliance risks creating a growing disconnect between real world risks and the mitigations compliance frameworks can offer. This approach does little to enhance overall operational resilience, ultimately perpetuating a cycle of vulnerability and insufficient preparedness.

Four principles of operational resilience

Executives understand that achieving complete control over all risks is unrealistic. However, this does not absolve them of the responsibility to manage the risks they can influence effectively. Four principles of operational resilience provide a structured framework to address these manageable aspects, enabling organizations to navigate and mitigate systemic risks more effectively.

5.1 Whole system in the room

To effectively manage risks and plan for recoverability, it is crucial to approach the process with a comprehensive, system-wide perspective. This means bringing together all critical stakeholders, those who hold responsibility and accountability for operations and IT and ensuring that essential knowledge is present in the room. These stakeholders should include both internal leaders and external partners, whether they play a support role or are integral to the value chain's delivery.

By involving the whole system, organizations can gain a holistic understanding of their critical processes and "crown jewels", their most valuable and essential assets or functions. This clarity is key to identifying viable options for recoverability and ensuring that strategies align with the organization's objectives and dependencies.

Ultimately, the goal is to ensure the organization maintains control over its ability to deliver the minimum acceptable level of service or performance during disruptions or crises. This requires a solid analysis of risks, close collaboration among stakeholders, and the development of solutions that reflect the interconnected nature of modern business ecosystems.

To effectively manage risks and plan for recoverability, it is crucial to approach the process with a comprehensive, system-wide perspective.

99

5.2 Operational risks across functions

Resilience starts with understanding which processes are critical to the organization's survival during a crisis. Collaboration between business and IT leaders is critical for mapping risks at the intersection of business workflows and supporting infrastructure. Steps to achieve this include:

Conducting business process walkthroughs to map workflows, customer journeys, data flows, and supporting systems.

Identifying potential failure points and vulnerabilities.

Simulating "No-IT" scenarios to understand how the organization would operate without IT systems and test alternative workflows.

These exercises not only highlight vulnerabilities but also deepen understanding of operational risks, enabling organizations to define maximum tolerable downtime and recovery objectives.

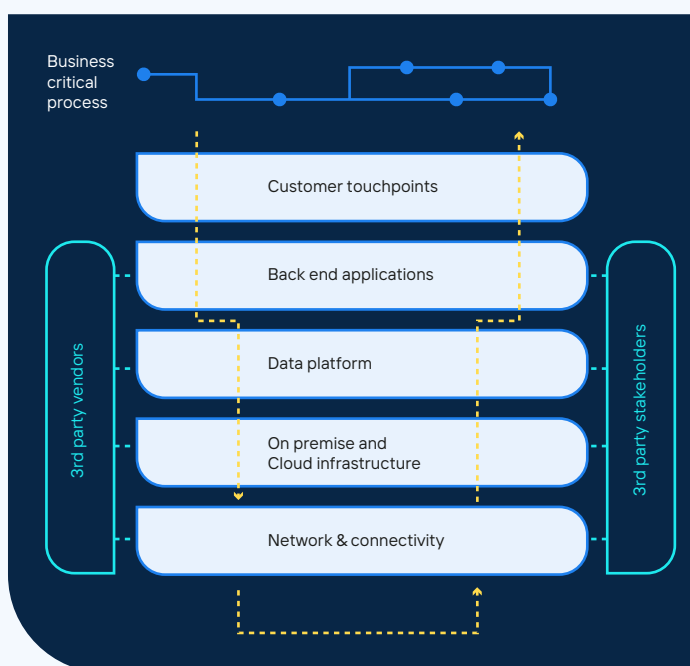
Best practice: Business process walkthrough to identify risks

Defining risk tolerance starts with understanding the organization's most critical processes, those essential to long-term success. Conducting a business process walkthrough provides a comprehensive view of risks by mapping key workflows, including the customer journey, data flows, and supporting technology systems.

By aligning these priorities with organizational goals, leaders can shift to a proactive strategy, transforming risks into opportunities and embedding resilience as a cornerstone of sustainable growth.

This approach highlights interdependencies, bottlenecks, and single points of failure, offering actionable insights to strengthen processes and build redundancy. By identifying vulnerabilities and their potential impacts, organizations can prioritize protecting critical assets and allocate resources more effectively.

Insights from such analyses provide the foundation for enhanced resilience, ensuring that organizations can prevent disruptions or recover swiftly.



5.3

Risk tolerance and financial impact

Effective resilience planning demands strategic clarity on resource allocation and risk tolerance. Organizations must carefully weigh the costs of mitigating risks against the potential financial, operational, and reputational impacts of inaction. This balancing act requires prioritizing efforts across three key dimensions:

Effective
resilience
planning

Business: Drive innovation to stay competitive while ensuring compliance with evolving regulatory requirements.

Operations: Strengthen operational stability by reducing critical incidents and minimizing disruptions.

Reputation: Safeguard customer trust by maintaining secure, reliable systems and avoiding financial losses or regulatory penalties.

By aligning these priorities with organizational goals, leaders can shift to a proactive strategy, transforming risks into opportunities and embedding resilience as a cornerstone of sustainable growth.



Best practice: Mapping risk tolerance and materiality

Pursuing growth and innovation often increases exposure to risk. Balancing ambitious goals with well-defined risk tolerance is critical, especially for business-critical processes. Discussions on risk tolerance should directly connect potential risks to business outcomes, offering leadership a clear perspective on trade-offs.

The **FAIR Institute** promotes a quantified approach to cyber and operational risk management. By expressing loss exposure in financial terms, using a Materiality Assessment Model (MAM) that enables leaders to make informed decisions, balancing risk protection with business objectives. This framework supports compliance while fostering a proactive, risk-based approach to resilience.

Using practical models like FAIR for materiality assessment gives a clear, measurable basis for defining risk tolerance and sets a strong starting point for resilient decision making. The model below represents a combination of MAM and S&P Global Ratings.



Source:
1. An Introduction to the FAIR Materiality Assessment Model. (2023). FAIR Institute Perspectives On Cyber Risk Across Corporates:
2. The Potential Impact Of Cyber Threats Is Growing. (2022, November). S&P Global Ratings.

Information privacy	Proprietary data loss	Cyber extortion	Network Security	Business interruption
Operational, response and recovery costs	Operational, response and recovery costs	Operational, response and recovery costs	Operational, response costs	Operational, response and recovery costs
Fines and judgements	Loss of future revenue	Ransom	Liability	Productivity and loss of future revenue
Liability	Liability	Liability		Liability
Financial fraud	Media content	Hardware bricking	Post breach security improvements	Reputation
Operational and replacement costs	Operational and replacement costs	Operational, response and replacement costs	Operational and response costs	Reputational damage
Liability	Liability			Market and brand value
				Cost of capital and credit rating
				Employee churn

A gap analysis, supported by standardized risk quantification frameworks, helps organizations evaluate strategic vulnerabilities and comply with regulations. This method clarifies where to allocate resources to align resilience efforts with business priorities effectively.

The FAIR Institute

The FAIR Institute is a research-driven not-for-profit organization dedicated to advancing the discipline of cyber and operational risk management through education, standards and collaboration.

The FAIR Institute and Quantified Risk Management

The FAIRTM framework helps boards and business executives understand an organization's loss exposure in financial terms, enabling more informed decision making. The institute encourages collaboration between risk professionals and business leaders to strike the right balance between protecting the organization and facilitating business operations. Unlike compliance focused strategies, FAIR promotes a risk-based approach aligned with international standards, allowing leadership to allocate resources more effectively.

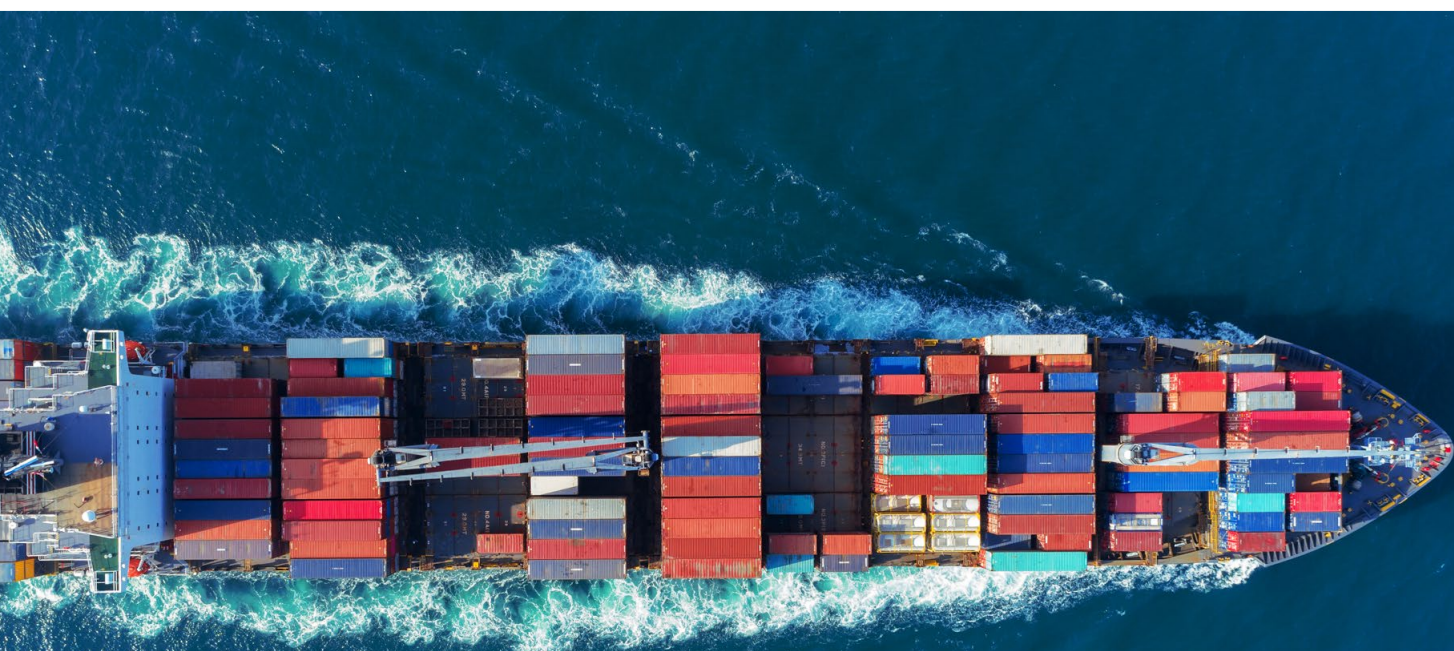
5.4

Organizing and testing for continuity and recovery

Regulations such as DORA and NIS2 are raising the bar for operational resilience, shifting the focus from merely preventing and detecting incidents to ensuring robust business continuity and recovery. With cyberattacks becoming increasingly frequent and sophisticated, the critical question is no longer if an incident will occur, but when. The recurring challenge is: *"Are we prepared to recover quickly and minimize disruption?"*

Culture, governance, and metrics

C-level executives play a pivotal role in embedding operational resilience by driving strategic alignment, accountability, and resource allocation. This includes creating a culture of resilience across the organization and ensuring that resilience priorities integrate seamlessly with technical and operational measures.



The strategic role of testing

Testing is a cornerstone of effective risk and continuity management, particularly for preparing organizations to handle NO-IT scenarios. A dedicated recovery environment, securely isolated to restore and validate compromised systems, allows for effective recovery without disrupting ongoing operations.

Regular testing in such controlled settings is critical to assess whether recovery objectives, including Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO), are achievable. These simulations provide valuable insights into readiness, helping identify gaps and ensuring that processes align with recovery goals.

Key boardroom discussions topics

Key boardroom discussions should address:

- Do we have a clear understanding of what it means to be in control?
- Have we identified our critical assets ("crown jewels") and ensured their protection?
- What about our critical processes, how are they safeguarded?
- How is our operational resilience structured?
- Where do vulnerabilities lie in our third-party partnerships?
- Has our recovery process been tested with measurable KPIs, or is it just a paper exercise?
- Are we simply meeting compliance standards, or have we embedded real resilience?
- Is our governance for recovery well-defined and actively in place?
- Have we set a clear, documented chain of command for handling ransomware incidents?
- Are board members trained in security threats, recovery strategies, and resilience measures, and ready to ask the right questions?

By testing NO-IT disruptions, organizations can identify gaps, enhance preparedness, and build confidence in their capacity to recover effectively when faced with severe incidents. Testing is not just a technical necessity; it is a strategic priority for long-term resilience.



Best practice: Testing through NO-IT scenarios

Recovery planning must address disruptions beyond IT failures, focusing on restoring business operations.

Key questions for NO-IT scenarios:

- What is the minimum acceptable level of service or performance we must maintain?
- Who are the essential personnel needed to sustain operations?
- What minimum information is required to function?
- Which critical applications or services are indispensable?
- What manual processes or physical tools can replace IT-dependent workflows temporarily?
- Are employees trained on alternative workflows and manual processes?
- Can specific processes be temporarily outsourced?
- Are there critical third-party dependencies, and do we know how they would support us during a No-IT event?
- Can audit and compliance proof-gathering be deferred during disruptions?
- Who is responsible for decision-making and coordination in a No-IT scenario, and is this chain of command clearly documented?
- Do we have clear communication strategies and tools that are independent of IT systems?

Key questions No-IT scenarios

Dedicated recovery environments and testing

Testing for No-IT scenarios has become a cornerstone of risk and continuity management. Establishing a secure staging area, an isolated environment for restoring and validating compromised components, ensures recovery without unintended risks to ongoing daily operations.

Regular testing in these environments assesses the organization's ability to recover within RCO (Recovery Centric Objectives) metrics. Such exercises allow teams to evaluate the readiness of their most critical processes, ensuring alignment with recovery goals.

RCO include:

- **Maximum Tolerable Downtime (MTD):** The longest downtime critical operations can endure without irreversible impacts.
- **Recovery Time Objective (RTO):** The maximum duration systems or functions can remain offline.
- **Recovery Point Objective (RPO):** The maximum acceptable data loss period after a failure.
- **Recovery Time Frame (RTF):** The total period required to restore services to full functionality.

Investing in resilience

Operational resilience demands continuous investment in tools, processes, and strategies to safeguard essential business functions. By strengthening collaboration between business and IT leaders and adopting proactive measures like RCO, organizations can build a resilient foundation. The approach allows for a dual strategy for resilience:

- 1 **Temporary emergency measures:** Immediate actions to reduce the impact of "No-IT" scenarios, ensuring essential operations can continue despite system outages.
- 2 **Structural enhancements:** Longer-term investments to address underlying vulnerabilities, strengthen operational systems, and eliminate reliance on temporary solutions. A detailed analysis of vulnerabilities and risks must translate into transformative, structural changes within your organization's core systems. In some cases, this entails a complete re-platforming of critical components to secure recoverability and continuity in the face of crises.



The authors

We would like to express our sincere gratitude to all the executives who participated in this study for their valuable contributions and insights. Your openness in sharing perspectives and experiences has been instrumental in shaping the findings of this report. The depth of your engagement has provided a comprehensive understanding of the critical challenges and strategic priorities facing organizations in the realm of cybersecurity and operational resilience. As leaders committed to driving progress and mitigating risk, your input is invaluable in helping shape the future of resilience within the business sector. Thank you for your time, expertise, and dedication to advancing the conversation around cybersecurity and its impact on business continuity.



Annemieke
Deering



Erik
Hoving



Ivo
Roefs



Jeroen
Borst



Jorrit
Molkenboer



Tom
den Hartog

Sources

Alvarez, P. S&P Global Ratings. (2023, August).

Cyber Risk Insights: IT Asset Management Is Central To Cyber Security.

<https://www.spglobal.com/ratings/en/research/articles/230815-cyber-risk-insights-it-asset-management-is-central-to-cyber-security-12819307>

Blaesing, N., Stauffenecker, J., PwC, & Harvard Business Review Analytic Services. (2021).

The Necessity of Cyber Risk Quantification.

Pulse Survey.

<https://hbr.org/resources/pdfs/comm/pwc/TheNecessityofCyberRiskQuantification.pdf>

Dezeure, F., Moerel Prof. L., Webster, Dr. G. SSRN Electronic Journal. (2024, February).

Improving the World's Cyber Resilience, at Scale.

Implementing Baseline Security by Default.

https://www.researchgate.net/publication/378213351_Improving_the_world's_cyber_resilience_at_scale_Implementing_baseline_security_by_default

Dezeure, F., Moerel Prof. L., Webster, Dr. G. Eurocontrol. (2022, March).

Reporting Cyber Risk to Boards.

<https://www.eurocontrol.int/sites/default/files/2022-03/reporting-cyber-risk-to-boards-be.pdf>

FAIR Institute. (2021).

An Introduction to the FAIR Controls Analytics Model (FAIR-CAMTM).

https://higherlogicdownload.s3.amazonaws.com/ISACA/9c800c88-34d8-4fca-8bd2-5d46fd639822/UploadedImages/Introduction_to_the_FAIR_Controls_Analytics_Model_FAIR-CAM_.pdf

FAIR Institute. (2023).

An Introduction to the FAIR Materiality Assessment Model (FAIR-MAMTM).

In FAIR Materiality Assessment Model (FAIR-MAMTM) (pp. 1–6).

<https://1616664.fs1.hubspotusercontent-na1.net/hubfs/1616664/An%20Introduction%20to%20the%20FAIR%20Materiality%20Assessment%20Model.pdf>

Gibbons, S. (2024, January).

Service Blueprints: Definition.

Nielsen Norman Group.

<https://www.nngroup.com/articles/service-blueprints-definition/>

Grant, H., & Goldhamer, T. (2021, November).

Our Brains Were Not Built for This Much Uncertainty.

Harvard Business Review.

<https://hbr.org/2021/09/our-brains-were-not-built-for-this-much-uncertainty>

Habib, M., Altberg, M.P., Ratnam, R., Merani, V.H.

(2022, November).

Perspectives On Cyber Risk Across Corporates: The Potential Impact Of Cyber Threats Is Growing. S&P Global Ratings.

<https://www.spglobal.com/ratings/en/research/articles/221107-perspectives-on-cyber-risk-across-corporates-the-potential-impact-of-cyber-threats-is-growing-12530941>

Jones, J., FAIR Institute, & RiskLens. (z.d.).

An Executive's Guide to Cyber Risk Economics.

In An Executive's Guide to Cyber Risk Economics.

https://www.risklens.com/hubfs/uploads/2019/04/RiskLens-eBook_An-Executives-Guide-to-Cyber-Risk-Economics.pdf

Pearlson, K., & Hetner, C. (2022, November).

Is Your Board Prepared for New Cybersecurity Regulations?
Harvard Business Review.

<https://hbr.org/2022/11/is-your-board-prepared-for-new-cybersecurity-regulations>

Polizu, C. S&P Global Ratings. (2020, October).

Cyber Risk In A New Era: Recent Cyber Events And Impact On Company Financials.

<https://www.spglobal.com/assets/documents/ratings/research/100047000.pdf>

Psychopedia. (z.d.).

Fear Avoidance Model.

https://www.physio-pedia.com/Fear_Avoidance_Model

SAFE. (2023).

CISO's PLAYBOOK FOR SEC CYBER RISK COMPLIANCE [Report].

<https://pages.safe.security/rs/691-VHU-261/images/ciso-playbook-for-sec-cyber-risk-compliance.pdf>

Shostack, G. L. (2014, August).

Designing services that deliver.
Harvard Business Review.

<https://hbr.org/1984/01/designing-services-that-deliver>

S&P Global Ratings. (2023, October).

C-Suite Must Walk The Cyber Talk.

<https://www.spglobal.com/ratings/en/research/articles/231017-c-suite-must-walk-the-cyber-talk-12878364>

The Harvard Law School Forum on Corporate Governance. (2021, June).

Principles for Board Governance of Cyber Risk.

The Harvard Law School Forum On Corporate Governance.

<https://corpgov.law.harvard.edu/2021/06/10/principles-for-board-governance-of-cyber-risk/>

Vlaeyen, J. W., Crombez, G., & Linton, S. J. (2016).

The fear-avoidance model of pain. *Pain*, 157(8), 1588–1589.

<https://doi.org/10.1097/j.pain.0000000000000574>

Zeijlemaker, S. (2023, June).

4 Areas of Cyber Risk That Boards Need to Address.

Harvard Business Review.

<https://hbr.org/2023/06/4-areas-of-cyber-risk-that-boards-need-to-address>

Zucker, R., & Rowell, D. (2023, January).

6 Strategies for Leading Through Uncertainty.

Harvard Business Review.

<https://hbr.org/2021/04/6-strategies-for-leading-through-uncertainty>