

How Jungheinrich's CISO Demonstrated ROSI in Under 8 Weeks

with Deloitte Germany and the Squalify's CRQ Platform.

Table of Contents

1	Executive Summary	 2
2	Engagement Objective	 4
3	Collaboration Overview	 6
4	Cyber Risk Quantification Process	 8
5	Results	 12
6	Key Contributors	 14

Disclaimer: The figures in this case study are for illustrative purposes only and do not represent actual business results in order to maintain client confidentiality.

“This communication contains general information only, and none of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

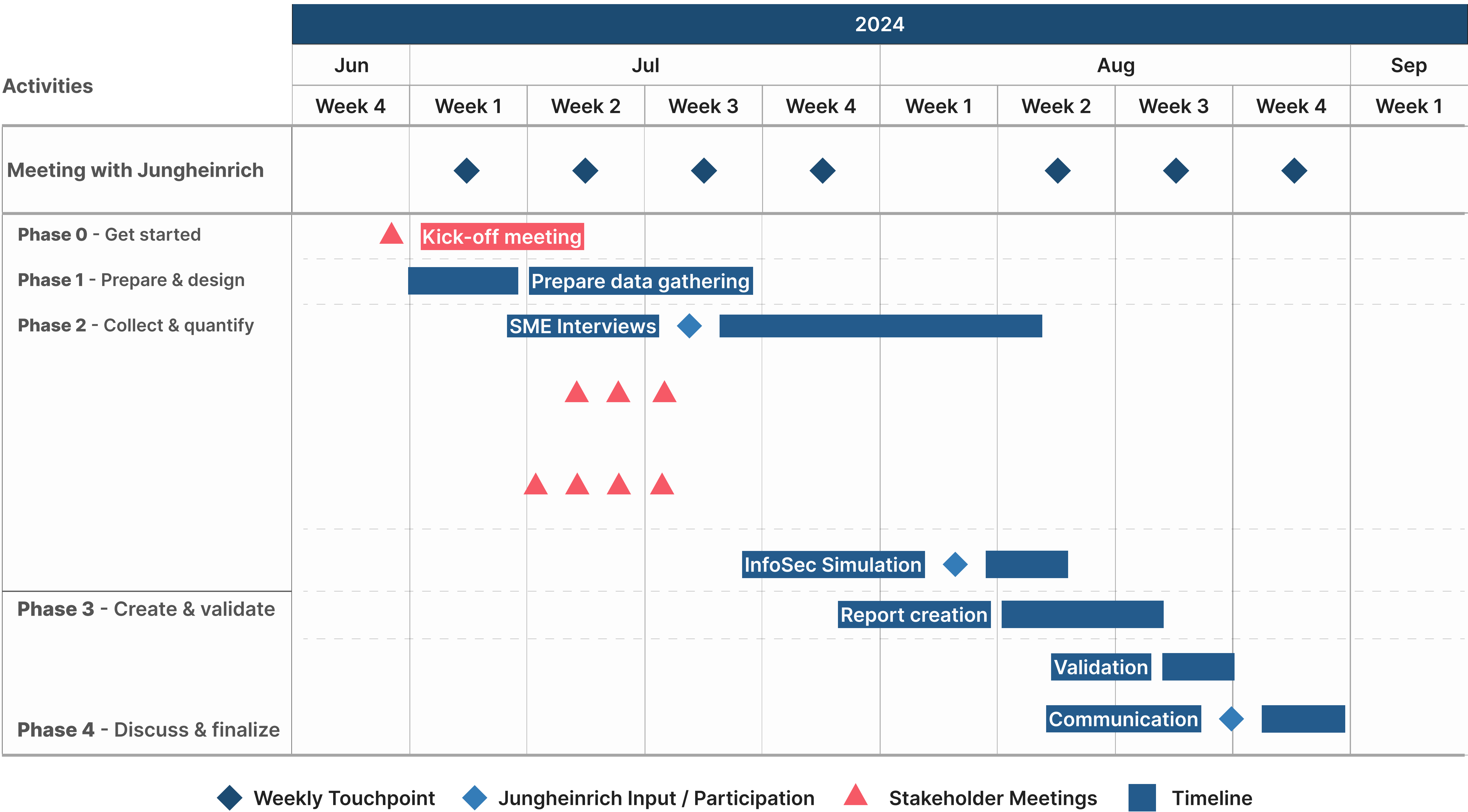
No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.”

Executive Summary

Jungheinrich, a global leader in intralogistics, recognized the importance of quantifying the company's cyber risk in order to make informed cybersecurity investment decisions. With global cybercrime costs projected to increase by 15% annually, Jungheinrich needed a way to verify its return on security investment (ROSI) and gain clear visibility into its evolving threat landscape.

Illustrative Data Only: Not Actual Business Figures

Timeline for Top-Down Cyber Risk Quantification



CRQ Timeline with Key Milestones: The timeline outlines the critical phases and activities of the CRQ process, including stakeholder meetings, weekly touchpoints, and data preparation.

Working with Squalify and Deloitte, Jungheinrich successfully completed a comprehensive Cyber Risk Quantification (CRQ) in under 8 weeks. Jungheinrich validated its information security improvement opportunities through this quantification process, evaluated its security investment strategies, and integrated cyber risk values into its broader Enterprise Risk Management (ERM) system.

Results

- ✓ Jungheinrich has a complete picture of how the threat landscape, information security maturity, and risk exposure have changed from last year to today.
- ✓ Jungheinrich can now validate the ROI of past and future cybersecurity investments and make informed decisions about cybersecurity investment priorities.
- ✓ With greater visibility into cyber risks, Jungheinrich can strategically align cybersecurity initiatives with business objectives to better contribute to long-term operational resilience.
- ✓ Jungheinrich can now present risk data to the Executive Board and the entire organization in meaningful and easy-to-understand monetary terms, including insights into the recurrence period of cyber losses across various scenarios.



Thanks to the superior value of Squalify's CRQ solution, I can track improvements in our cybersecurity investments and make sure we're investing in the right initiatives to reduce our cyber risk!

Dr. Tim Sattler

CISO at Jungheinrich AG | Director, Board of Directors at ISACA

Engagement Objective

About Jungheinrich

Jungheinrich AG is one of the world's leading manufacturers of material handling equipment and intralogistics solutions. With more than 21,000 employees, the company is represented in over 120 countries. The company is a key driver of innovation through automation and digitalization, offering solutions that optimize logistics processes and increase supply chain efficiency. Jungheinrich is headquartered in Hamburg, Germany.

Prior CRQ Engagement (2022)

In 2022, Jungheinrich partnered with Squalify for an initial cyber risk quantification (CRQ). This initial engagement allowed Jungheinrich to better identify and prioritize vulnerabilities by providing an external view of the company's risk profile, complementing the internal results of the cyber risk assessment.

By 2024, with an evolving cyber threat landscape and changing risk exposure, Jungheinrich recognized the need for updated risk quantification and ongoing cyber risk monitoring to ensure the continued effectiveness of its cybersecurity strategy. Together with Squalify and Deloitte, Jungheinrich supplemented their operational cybersecurity risk assessment with top-down financial impact values and integrated CRQ insights into their enterprise risk management (ERM) system.

Engagement Objective (2024)

Given the changing threat landscape, the company's risk exposure and evolving business model, Jungheinrich needed to:

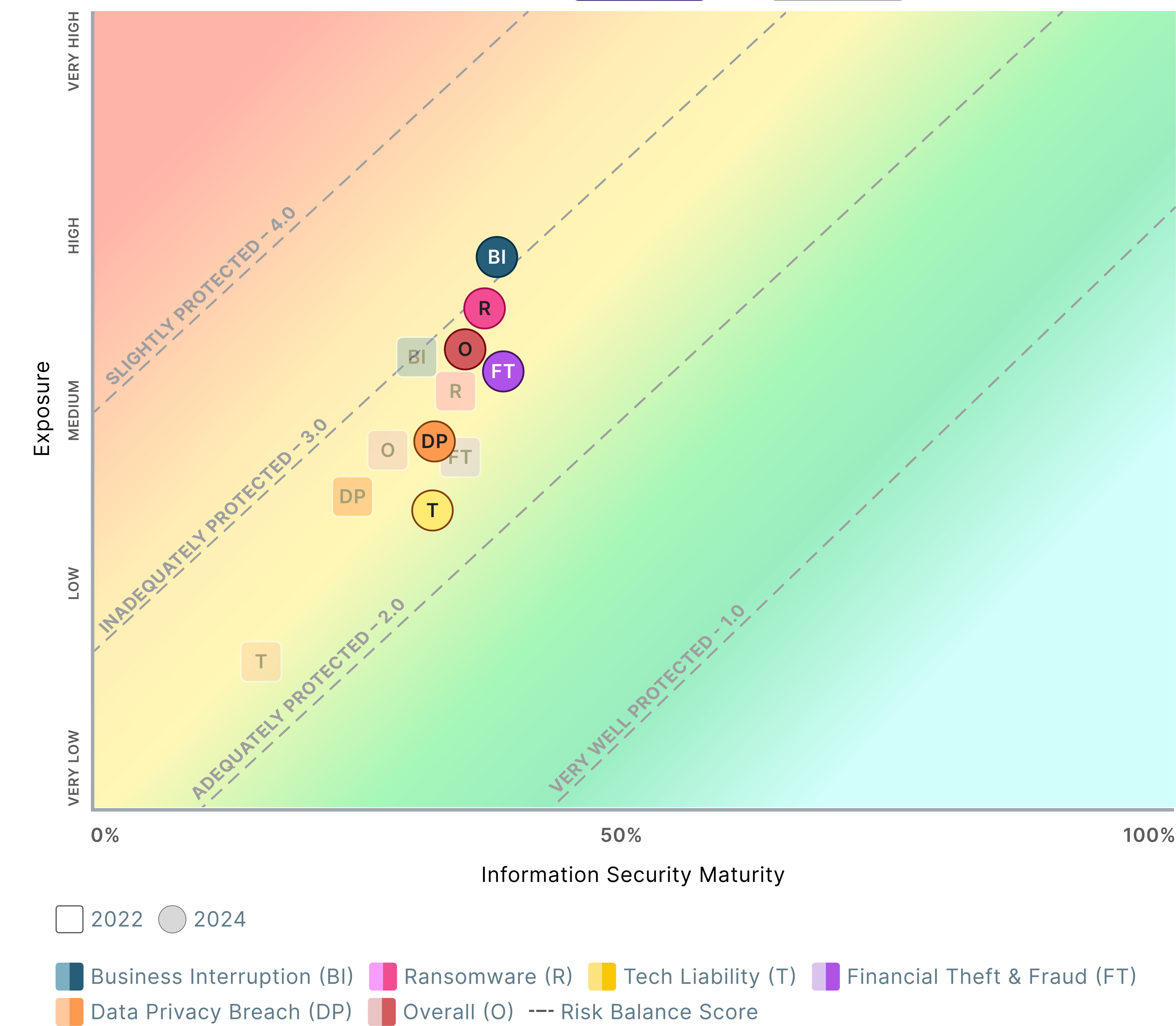
- ✓ Understand overall changes in their cyber risk profile from 2022 to 2024.
- ✓ Assess the impact of product automation on the overall cyber risk profile.
- ✓ Quantify the effectiveness of their security investment programs.
- ✓ Prioritize security initiatives according to their largest risk mitigation potential.
- ✓ Ensure that security investments are aligned with business objectives and are explainable to the executive board.

The engagement objectives were threefold:

- ✓ Demonstrate the value of security investments through measurable returns.
- ✓ Maintain continuous oversight of their evolving cyber risk profile.
- ✓ Implement a scalable process to conduct CRQ analyses annually.

Illustrative Data Only: Not Actual Business Figures

Risk Balance: 2022 vs 2024



Comparison of 2022 (semi-transparent) and 2024 (solid) risk positions, highlighting changes in exposure and information security maturity across key risk components.

Collaboration Overview

About Squalify

Squalify's CRQ platform enabled Jungheinrich to quantify and validate its security investments, providing complete visibility of its cyber risk profile and the financial cyber impact in today's threat landscape. By assessing how Jungheinrich's security programs contribute to risk mitigation efforts, Squalify provided the foundation for more effective strategic decision-making.



CRQ bridges the gap between cybersecurity and the Boardroom. Translating cyber risk into clear business terms is key to increasing transparency and strategic alignment between cyber leaders and the board.

Asdrúbal Pichardo

CEO at Squalify

Deloitte's Role

Deloitte played a pivotal role in synthesizing and validating insights from Jungheinrich's finance, production, and R&D teams to gather the necessary information and assess the company's cybersecurity maturity.

Leveraging their consulting expertise, Deloitte ensured that the CRQ output metrics were fully aligned with Jungheinrich's strategic objectives and supported informed decision-making as Jungheinrich's cybersecurity evolved.

As an experienced practitioner of Squalify's CRQ methodology, Deloitte is Squalify's preferred partner for project delivery, reinforcing their expertise and leadership in this area.



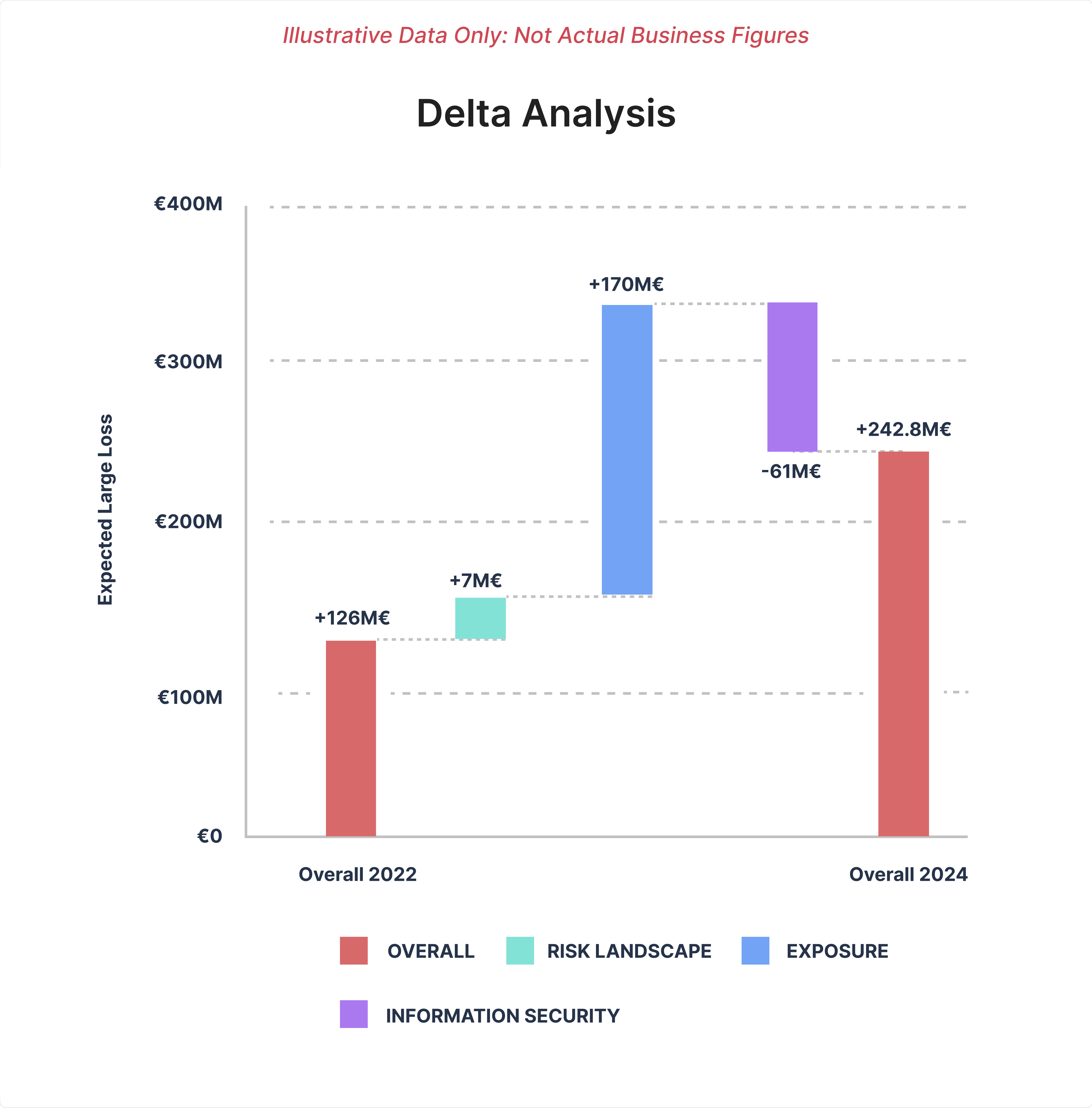
CRQ provides a detailed picture of an organization's risk position. The quantitative values in financial terms are intuitive and can be compared with other types of risk - which are assessed using financial metrics.

Volker Burgers

Partner and Offering Lead Cyber Strategy & Transformation at Deloitte Germany

Cyber Risk Quantification Process

Jungheinrich partnered with Squalify and Deloitte. Together, they implemented a streamlined CRQ process that enabled Jungheinrich to focus on a high-level strategic CRQ overview, providing required input information and evaluating the quantification output as a basis for their strategic decision-making.



The analysis shows changes in expected large losses primarily due to increases in risk exposures, partially offset by improvements in information security.

1. Scoping and Data Gathering

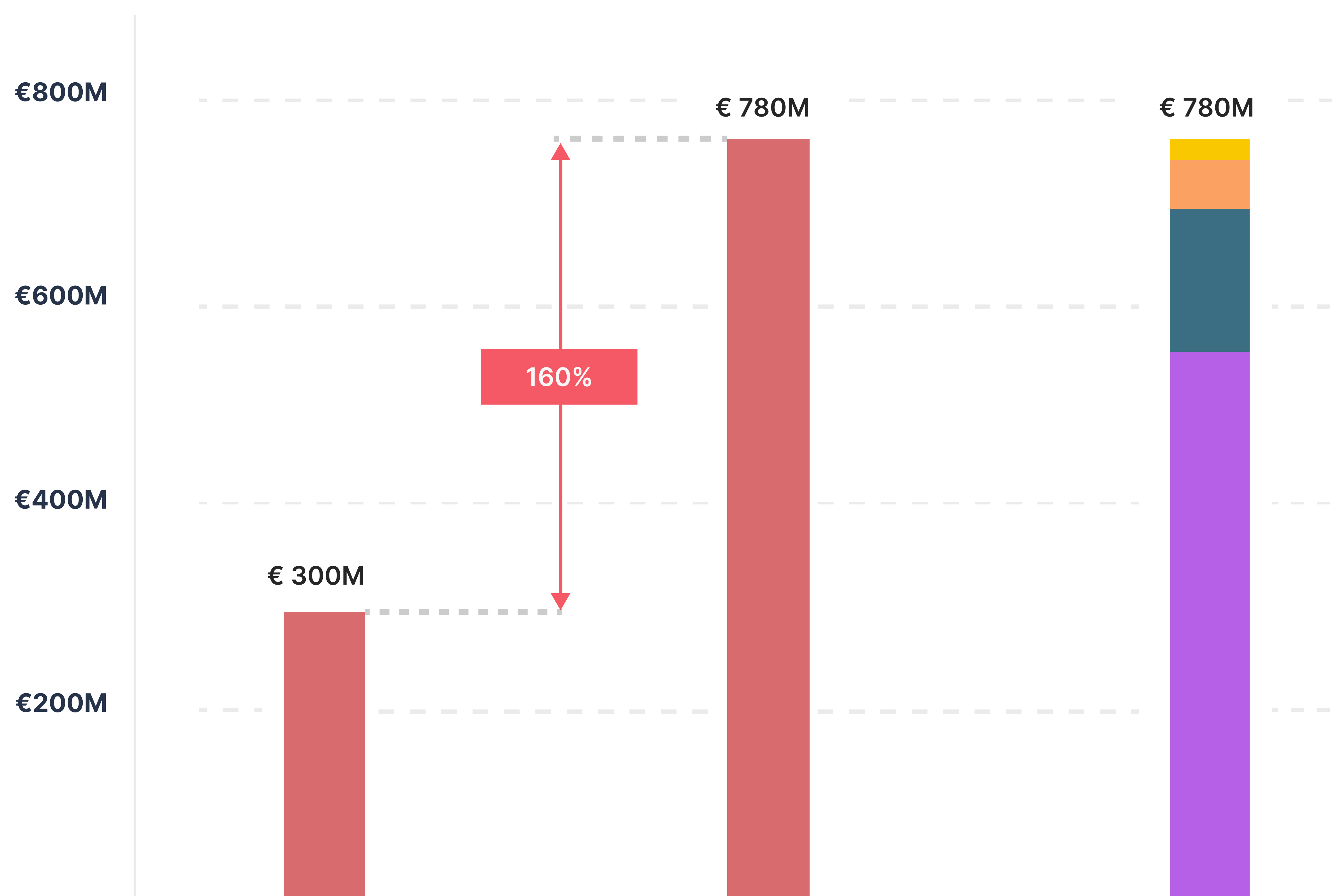
At first, the team worked together to define the primary objective: to gain visibility into Jungheinrich's current cyber risk profile and validate the return on security investments. Also, the stakeholders provided essential data on business processes and financial perspectives to quantify cyber scenarios.

2. Quantification and Insights

After gathering the necessary input data from interviews, internal reports, and previous assessments and feeding it into Squalify's CRQ platform, the team modeled various risk scenarios to evaluate the effectiveness of Jungheinrich's security program.

Illustrative Data Only: Not Actual Business Figures

Worst Case Loss Components



The analysis shows an increase in worst-case loss components from 2022 to 2024. Financial Theft & Fraud is the largest contributor, while Tech E&O appears as a new loss component not present in the 2022 analysis

By leveraging historical cyber loss data with over 1 million data points from 100,000 companies across 130+ industries, the platform provides reliable and quantifiable insights alongside industry benchmarks. This data-backed approach provided measurable insights into how cybersecurity efforts impact Jungheinrich's overall risk profile.

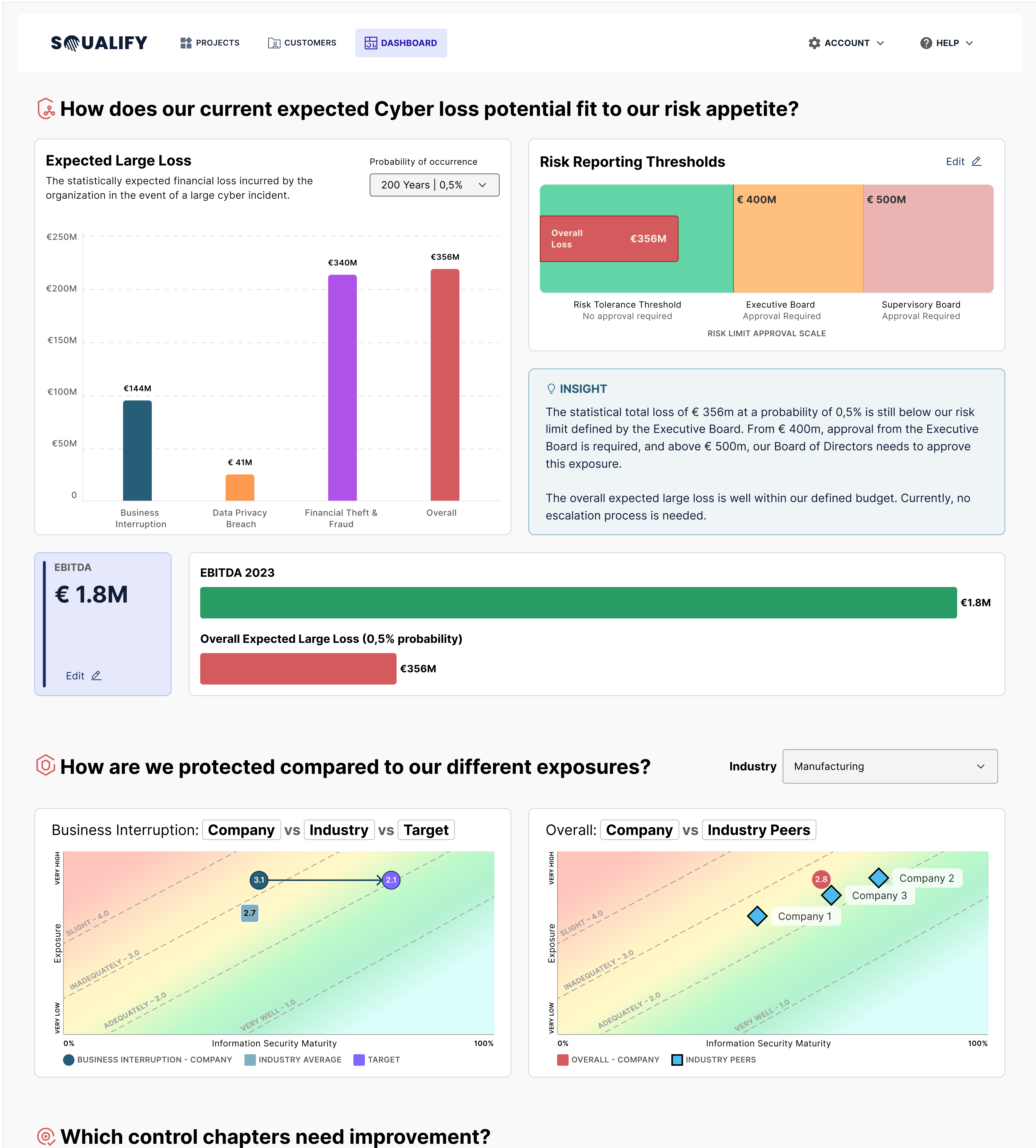
By linking financial metrics to Jungheinrich's cyber risk, the team validated the tangible benefits of their security programs and further strengthened the alignment between cybersecurity efforts and business objectives.

3. Board Reporting and ERM Integration

Finally, the strategic insights derived from the quantification were successfully presented to the Jungheinrich board. In collaboration with the Deloitte project team, Jungheinrich's CISO, Dr. Tim Sattler, transparently communicated the need for increased investment in cybersecurity. Together, they addressed all questions from board members directly and provided strategic recommendations for cybersecurity investments.

Jungheinrich's CISO, Dr. Tim Sattler, confirmed that, following the presentation, they had integrated the CRQ risk scores into the company's regular board updates and ERM system. This ensures ongoing monitoring and integration of cyber risk data into their broader risk management framework.

Illustrative Data Only: Not Actual Business Figures



Squalify board report provides an overview of expected cyber loss potential, risk thresholds, and exposure benchmarks.

Results

Key findings included:

- ✓ **Change in Cyber Risk:** Jungheinrich gained full visibility into how their threat landscape and risk exposure evolved between 2022 and 2024.
- ✓ **Validated ROSI:** Quantified insights confirmed a positive return on security investments and the effectiveness of cybersecurity efforts in improving the organization's overall cyber risk profile. In addition, the quantification allowed Jungheinrich to prioritize security programs according to their individual ROSI.
- ✓ **Strategic Alignment:** Financially driven CRQ insights enabled Jungheinrich to assess its cybersecurity alignment with the business goal of increasing automated products. This enables continued business growth and operational efficiency in a resilient environment.
- ✓ **Boardroom-Ready Insights:** Squalify's expert-led, data-driven approach, , executed and presented by Deloitte's cyber experts, enabled Dr. Tim Sattler to present risk data to his board in meaningful and easy-to-understand financial terms. This created a strong narrative for ongoing cybersecurity investments, secured board-level buy-in, and integrated risk insights into the company's ERM system.



Squalify's CRQ solution delivered superior insights that have enabled me to provide full transparency to our Executive Board on our cyber exposure. Now, I can have a straightforward dialogue with the right business language and confirm the strategic direction of our Cybersecurity program.

Dr. Tim Sattler

CISO at Jungheinrich AG | Director, Board of Directors at ISACA

Make Your Cyber Risk Quantification Board-Ready

Are you ready to take control of your cyber risk? Like Jungheinrich, your organization can validate the return on security investments, align cybersecurity programs with long-term business goals, and gain board support for cybersecurity initiatives.

[Book Meeting](#)

Key Contributors



Jungheinrich AG is one of the world's leading manufacturers of material handling equipment and intralogistics solutions. With more than 21,000 employees, the company is represented in over 120 countries. Jungheinrich is headquartered in Hamburg, Germany.



Dr. Tim Sattler

CISO at Jungheinrich AG | Director, Board of Directors at ISACA



Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Legal advisory services in Germany are provided by Deloitte Legal. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 457,000 people worldwide make an impact that matters at www.deloitte.com/de.



Volker Burgers

Partner and Offering Lead Cyber Strategy & Transformation at Deloitte Germany



Lennart Hornauer

Senior Manager Enterprise Security



Stefan Feiniler

Senior Consultant Cyber Strategy & Transformation



The Squalify CRQ platform empowers board-level discussions with cyber risk quantification. By uncovering financial loss metrics and key risk drivers, Squalify supports business leaders in developing effective cybersecurity strategies. Squalify is headquartered in Munich, Germany, and is a wholly owned subsidiary of Munich Re, the world's leading cyber reinsurer.



Asdrúbal Pichardo

CEO



Hermann Kramer

Founder & Chief Strategy Officer



Theresa Barsy

Senior Cyber Risk Consultant

Learn more at

www.squalify.io

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/de/UeberUns to learn more.”



Squalify - Cyber Risk Quantification for the Boardroom
www.squalify.io