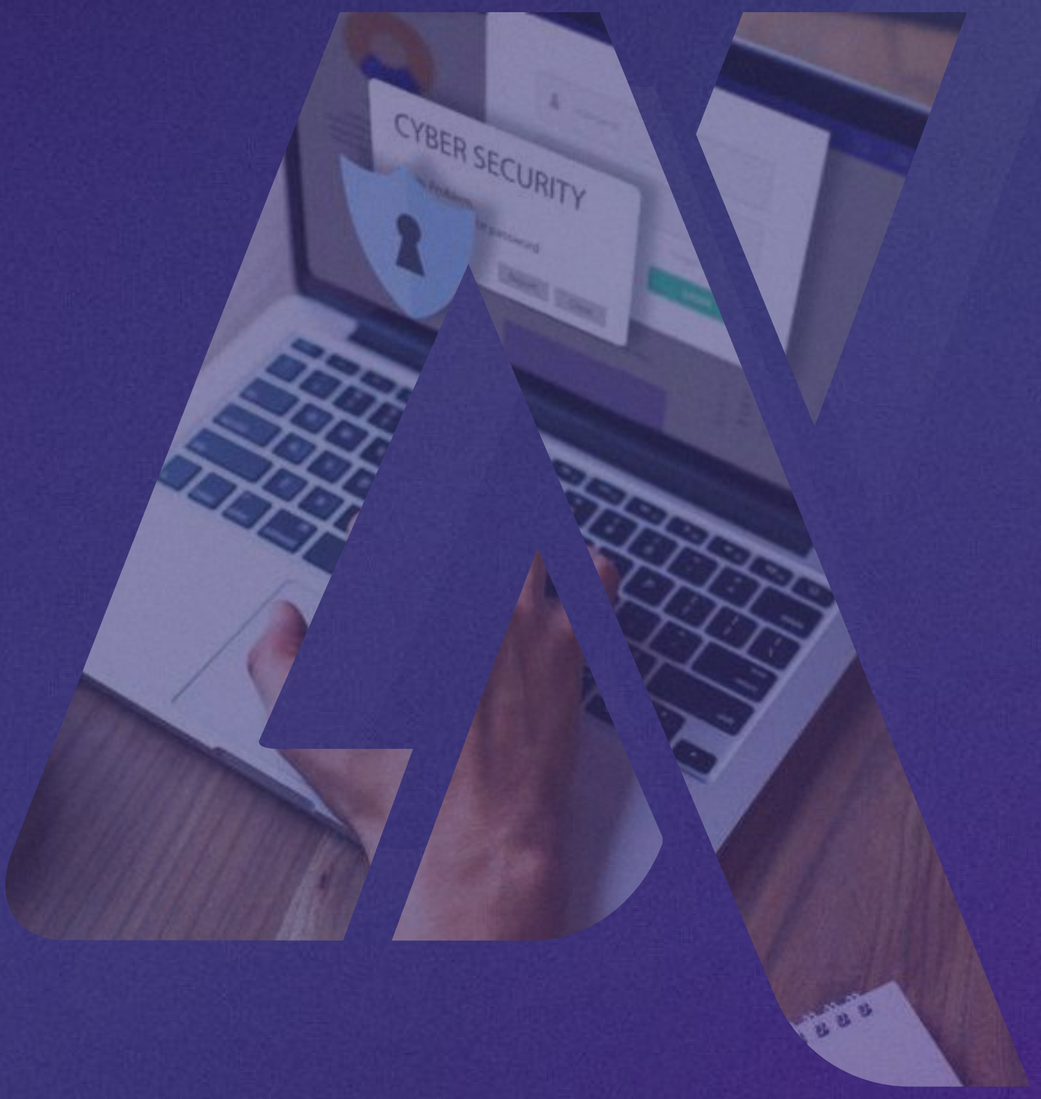


Alfahive

Automate cyber risk assessment and quantification for Retail, Consumer Goods and Hospitality organizations

Alfahive’s cyber risk automation platform - RiskNest^{tm}

About Alfahive

We are on a mission to revolutionize cyber risk management for retail, consumer goods and hospitality organizations. Our cyber risk automation platform automates assessment, quantification and control prioritization resulting in significant efficiency gains and cost savings for risk managers. Our platform enables organizations to save time and money by making data-driven risk decisions.

Introduction

Purpose of the white paper

In this white paper, we offer a revolutionary solution to the challenges faced by retail, consumer goods and hospitality organizations in their cyber risk management and quantification journey. You will gain valuable insights into the limitations of current options, and discover how our innovative approach, based on industry-specific and data-driven models, can provide significant advantages. By reading on, you will learn how our platform can help you automate your cyber risk assessment and quantification needs, resulting in significant cost savings and efficiency gains.

Introduction to Alfahive cyber risk automation platform

At Alfahive, we understand that effective cyber risk quantification starts with a deep understanding of banking and financial services business processes and your unique operations. Our platform is specifically tailored for banking and financial services organizations using the following key capabilities:

- Pre-built library of cyber risk scenarios specifically designed for retail, consumer goods and hospitality.
- High-quality loss event costs data from over half a million cyber loss events with pre-curated cohorts just for retail, consumer goods and hospitality.
- Trained machine learning models to identify relevant attack sequences and controls.
- A unified controls framework with multiple security control standards common to retail, consumer goods and hospitality.
- Built-in APIs to integrate with and gather control assessment status from GRC platforms as well as results from automated pen testing and attack surface management systems.
- Patent-pending, cyber incident susceptibility model, includes an inside-out and outside-in, comprehensive, susceptibility score.
- Automatically quantified and ranked security control improvements.

Our platform can help you assess risks faster and quantify them more accurately with a unique susceptibility model, customized industry data, and our customer success experience. This can save your risk manager time and boost productivity by eliminating the need for manual efforts.

The current state of cyber risk management and quantification

Overview and shortcomings of current market and solutions

The current market for cyber risk management solutions offers a dizzying array of solutions which generally fall into two categories: qualitative ranking and manually created quantification reports.

Qualitative ranking approaches

The qualitative approach to managing security risk is based on reporting the security status on a red, amber, and green or rating the security risks based on a predefined scale like 1-10 or 1-100. While this approach may be useful to understand the basics of cyber security risks, it lacks the necessary granularity and specific information needed for competitive retail businesses to make efficient decisions to spend time and money. These also lack the context of the business operations of a retailer and lead to an inability to communicate decisions to business stakeholders and involve them in decision-making.

Manually created quantification reports

On the other hand, more mature retail, consumer goods and hospitality use consulting partners to build quantification models. It requires manually creating risk taxonomies, identifying threat actors, curating threat intelligence, and developing threat event frequency and susceptibility models. This approach is expensive, time-consuming, and heavily reliant on the skills of the consulting organization, leading to a lack of standardization and peer benchmarking.

Limitations and challenges with existing solutions

The current approaches to cyber risk management have several limitations and challenges for retail, consumer goods and hospitality organizations. Qualitative ranking approaches lack the necessary granularity and specific information for efficient decisions to deploy the limited time and money a retailer has. On the other hand, manually created quantification reports are expensive, time-consuming, and heavily reliant on the skills of the consulting organization. This approach lacks standardization and peer benchmarking, leading to questions about the reliability of the reports. As such, there is a need for a more efficient, accurate, and standardized approach to cyber risk management that can address the limitations and challenges of current approaches.

Our cyber risk automation platform

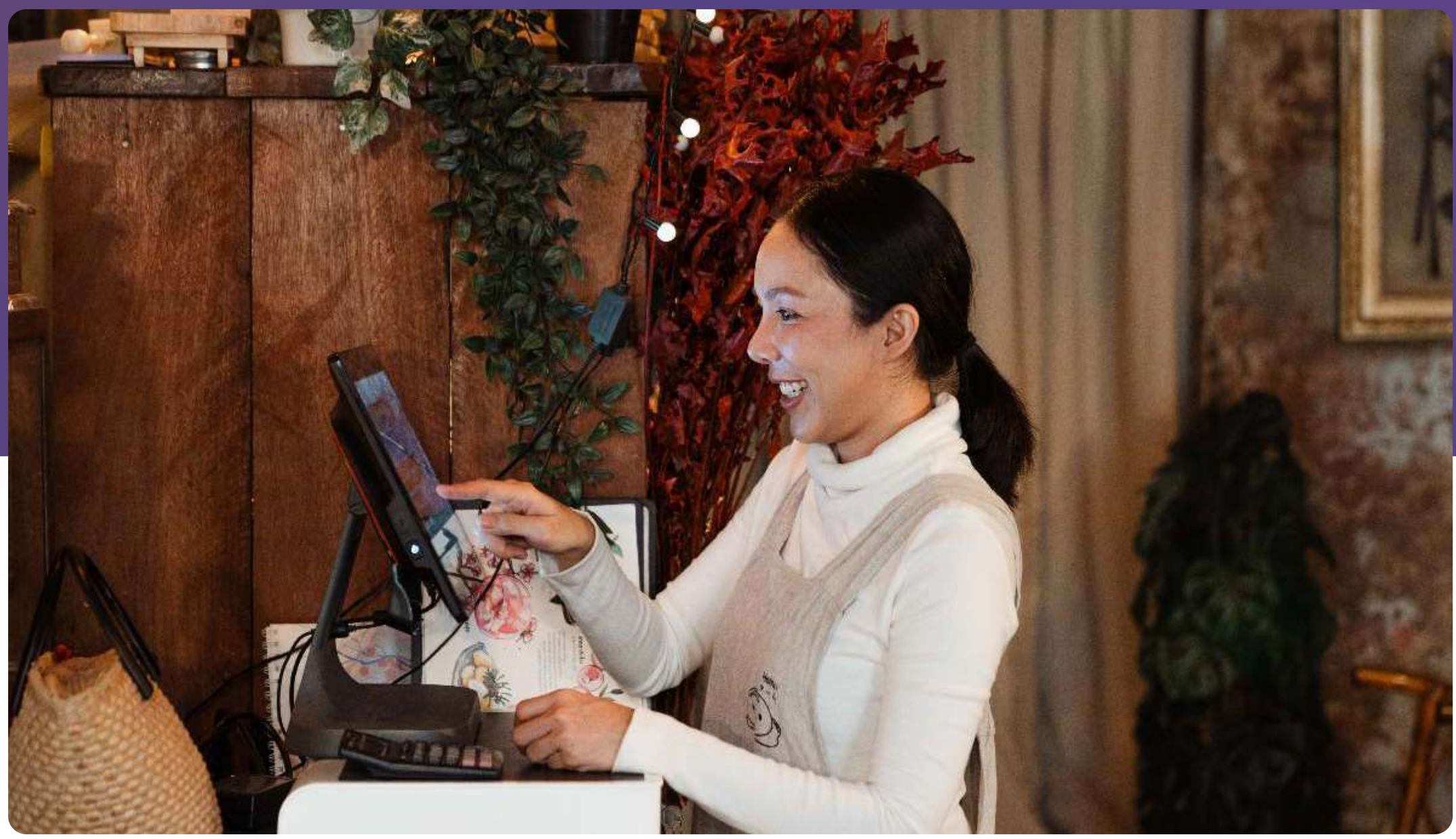
At Alfahive, we have developed a unique, industry-specific, data-driven approach to cyber risk automation. Our cyber risk SaaS platform has three key automation capabilities: Automated assessment, Automated quantification, and Automated recommendation plan.

Automated assessment includes pre-configured relevant control frameworks for retail, consumer goods and hospitality organizations and an automated workflow to assess internal projects and third parties. A typical retail, consumer goods and hospitality organization have several hundred ongoing digital projects and third parties to be onboarded every year across the entire breadth of the business. Our platform automates the ongoing and continuous assessment of controls across all these varying needs.

Automated quantification models are tailored to specific industries and are designed to identify cyber risks and generate a quantification of the cyber risk in terms of both financial exposure and the probability of an impact using OPEN-FAIR cyber risk quantification methodology and Monte-Carlo simulation. The platform has pre-populated data on threats, losses and control prioritization. The machine learning models are already trained based on the threat landscape of a specific industry and country cohort. It is a multi-tenant platform based on Microsoft Azure, and it uses state-of-the-art technology and security measures

The third component of our platform is the recommendation engine, which automates the security control prioritization based on the reduction in risks. This approach is designed to maximize the return on the security capital and do more. By focusing on risk reduction, our recommendation engine helps organizations achieve a higher return on their security investments. Our solution is unique in the market, and it helps organizations to understand, measure, communicate and, ultimately, make data-informed decisions that drive cyber resilience. It is compatible with multiple control standards like NIST CSF, ISO27001, CIS CSC, PCI DSS, SOC2 etc to take inputs from the customer based on what works best for them.

Moreover, we have worked closely with Industry ISAC members to define the risk taxonomy and business functions for individual industries. This has allowed us to tailor our platform to the specific needs of each industry, ensuring that our models are as accurate and effective as possible. By training our machine learning models based on loss event data, we have developed a highly sophisticated approach to cyber risk quantification. The following part of the whitepaper outlines the key details of the business functions and risk scenario for a retail, consumer goods and hospitality organization.



Retail business functions

The Alfahive research team has pre-configured the following business functions in the Alfahive platform and the same can be modified further based on the individual retailer’s business model:

- **Online channels:** E-Commerce platforms, digital marketing, brand online presence, Online customer service
- **Store operations:** POS system, inventory management system, workforce management, CRM system
- **Supply chain:** ERP (Procurement, inventory, demand, Order fulfilment), warehouse management system, transportation management system, supplier relationship management
- **Product development:** Applicable to consumer goods organizations or retailers with private labels. It includes product research and development systems.
- **B2B Sales:** Applicable to consumer goods organizations. This function includes distribution management systems and B2B sales systems
- **Manufacturing operations:** Applicable to consumer goods organizations and retailers owning the manufacturing for the private label brands.
- **Corporate functions (HR, legal):** The systems and processes used to manage human resources, including employee training, background checks, and incident response procedures.
- **Information Technology (IT):** Responsible for maintaining the systems and infrastructure to support its operations, dev/Ops, desktops, devices etc
- **Acquisitions:** All the acquisition entities

Cyber risk scenarios for Retail, Consumer Goods and Hospitality organizations

The Alfahive research team collaborated with members of the RH-ISAC community to study the commonly used risk taxonomy in the Retail, Consumer Goods and Hospitality industry. We used cause-and-effect modelling to identify the most important converge and published a set of automated retail risk scenarios.

These cyber risk scenarios are easily adapted to suit the uniqueness of each individual organization.

- **Data breaches.** Customer personal information, payment card data, transaction information, employee information, supplier information, intellectual property etc.
- **Ransomware.** Malware that encrypts a victim's files and demands payment for the decryption key.
- **Business continuity**. Disruptions to an organizational infrastructure that can prevent customers from accessing their accounts and cause a loss of revenue.
- **Fraud.** BOT abuse to the online channel, ATO of loyalty program, online fraud.
- **Third-party risks.** Third-party risks refer to the potential threats and vulnerabilities that an organization may face because of its relationships and interactions with external parties such as vendors, suppliers, and service providers.

Alfahive research

The Alfahive research team (also known as our “RiskSquad”) has researched the typical loss questions for both primary losses and secondary losses based on inputs from various industries' research and loss history databases.

- How many are the total customers?
- How many customers are estimated to be affected by the breach?
- What is the estimated cost of any lost customers? (Customer acquisition cost)
- What is the estimated revenue loss due to the breach? Revenue/customer.
- What is the cost of incident response and recovery?
- What is the cost of any legal fees associated with the breach?
- What is the cost of any loss of intellectual property?
- What is the impact on the organization’s ability to comply with regulations and standards?

Depending on the scenario and the client’s business operations, other questions are added by the Alfahive research team to the platform.

Case study

A large private equity organization

Challenge

A large private equity organization had significant challenges in assessing the cyber security of its portfolio companies. The process was time-consuming and required significant resources, making it difficult to conduct regular assessments and identify potential cyber risks in a timely manner. Additionally, the organization was concerned about the potential impact of cyber incidents on the portfolio companies in terms of regulatory fines and reputational damage.

Solution

To address these challenges, the organization turned to Alfahive's cyber risk management platform for a pilot. The platform uses a unique, industry-specific, data-driven approach to automate the assessment and quantification of cyber risk for all portfolio companies. The platform utilizes pre-built data and patent-pending machine learning technology to create a unique approach to cyber risk assessment and quantification.

Results

By using the platform, the organization was able to significantly reduce the time and resources required for regular cyber risk assessments. Additionally, the platform provided a clear understanding of the cyber risks facing the portfolio company, including the potential financial exposure and probability of an impact, which helped make more informed decisions about risk management. The platform also provided the organization with a clear understanding of the specific security controls needed to mitigate the identified risks.

Overall, the Alfahive platform helps private equity organization to better protect their portfolio companies from cyber threats, minimize their risks from cyber incidents, and build cyber resilience.

Case study

A large retail organization for the third-party risk quantification

Challenge

A large retail organization faced significant challenges in assessing the cyber security of its third-party vendors. The process was manual and relied on excel spreadsheets, making it time-consuming and resource intensive. Additionally, with hundreds of third parties to be assessed each year, the organization struggled to maintain consistency in its assessments and to identify potential risks in a timely manner.

Solution

To address these challenges, the organization turned to Alfahive's cyber risk management platform. The platform uses a unique, industry-specific, data-driven approach to automate the assessment and quantification of cyber risk for all third-party vendors. The platform utilizes pre-built data and patent-pending machine learning technology to create a unique approach to cyber risk management.

Result

By using the platform, the organization was able to significantly reduce the time and resources required for regular cyber risk assessments of third-party vendors. Additionally, the platform provided a clear understanding of the cyber risks facing the third-party vendors, including the potential financial exposure and probability of an impact, which helped the organization make more informed.

The platform also provided the organization with a clear understanding of the specific security controls needed to mitigate the identified risks and helped the organization to stay compliant with the regulatory requirements, it enables communicating the risk status and security controls to the third-party vendors in a common language.

Case study

A major bank to assess and quantify the cyber risks and make capital adequacy decisions (in partnership with a Big-4 consulting partner)

Challenge

A major bank faced significant challenges in assessing and quantifying the cyber risks to their organization, which was crucial in making capital adequacy decisions. The bank had a large, complex IT environment with a wide range of systems and applications, making it difficult to identify and prioritize cyber risks. Additionally, the bank needed to comply with regulatory requirements and maintain a high level of security to protect against cyber threats.

Solution

To address these challenges, the bank partnered with a Big-4 consulting firm and turned to Alfahive's cyber risk automation platform for a pilot. The platform uses a unique, industry-specific, data-driven approach to automate the assessment and quantification of cyber risk for the bank. The platform utilizes pre-built data and patent-pending machine learning technology to create a unique approach to cyber risk management.

By using the platform, the bank was able to gain a clear understanding of the cyber risks facing the organization, including the potential financial exposure and probability of an impact on the pilot scenario. This helped the bank make more informed decisions about risk management and capital adequacy.

In partnership with the Big-4 consulting firm, Alfahive was able to provide the bank with a comprehensive solution for cyber risk quantification. The consulting firm's expertise in the banking industry and regulatory requirements was combined with Alfahive's industry-specific, data-driven approach to cyber risk quantification. Together, we were able to provide the bank with a clear understanding of the cyber risks facing the organization and the specific security controls needed to mitigate those risks.

Result

The platform's ability to provide trustworthy and explainable quantification numbers in the context of the bank's business functions was particularly valuable. The bank is working to roll out the platform's data-driven approach to identify and prioritize risks and to make informed decisions about risk management and capital adequacy. Business and technology stakeholders are able to easily understand the financial exposure and probability of an impact of cyber risks in dollar terms as provided by the platform.

Benefits of our solution

How Alfahive solves the limitations and challenges of current solutions

Alfahive's cyber risk automation platform overcomes the limitations and challenges of existing cyber risk management and quantification solutions by offering pre-curated and researched risk scenarios customized for specific industries. By automating cyber risk assessment and quantification, our platform enables retail organizations to make efficient risk decisions to save time and money.

Additionally, our platform automatically provides a clear understanding of the specific security controls needed to mitigate the identified risks, which helps to enhance the return on security investments and ensure the full utilization of all assets invested in security. Our platform also provides a common language for business and technology stakeholders to communicate in, which helps in the decision-making process. Our approach is unique in the market, and it helps organizations to understand, measure, communicate and, ultimately, make data-informed decisions that drive business resilience.

Quantifiable benefits

- **Recapture many hours of productivity.**
  By automating the assessments and moving away from manual, often excel-based, and resource-intensive approaches, our platform **reduces the cyber risk assessment effort by over 50%.**

- **Leverage risk quantification in a fraction of the time.**
  Our platform has pre-built data specific to the industry and geography, and it has already trained machine learning models, leading to a **10X faster time to value.**

This means that the typical risk quantification program that takes approximately 8-12 months can be completed in about 4-8 weeks with minimal training and consulting resources.

- **Gain efficiencies.**
  Our platform's ability to make data-driven decisions on control improvement prioritization and linking risk operations to security operations helps to uncover opportunities to do more with less. This results in an estimated approx. **20% higher return on security investment,** which is significant in today's competitive and ever-changing business environment.

Implementation

The implementation process for the Alfahive platform is designed to maximize value creation for our customers. It begins with a value discovery phase, where we work with the customer to select a business function and a risk scenario to prove our value in approx. 2-4 weeks.

Once the value of the platform is confirmed and agreed upon by the customer, we move forward with the rollout of the platform. The rollout plan is aligned with the business priorities and digital roadmap of the organization to ensure that value is created early in the process.

	Lite	Full	Global
Capabilities	Single lite control assessments orchestrated to third parties by our platform	Control assessments risk quantification scenarios single site deployment	Control assessments risk quantification scenarios. Multi-site deployment
For	Private equity firms third party assessments	Large organizations with complex business and nested ecosystem of partners	Large organizations. global presence, multiple lines of business.

Our global consulting partners

Alfahive works in partnership with 5 of the top 10 global cyber consulting organizations as well as select regional partners for local country-specific needs. These relationships allow Alfahive to reach many organizations on a global scale. We follow a collaborative approach that combines our Cyber Risk Automation product (SaaS), industry data, research team, and Cyber Risk Quantification (CRQ) expertise, with the services and industry depth of our consulting partners.

Our consulting partners bring in-depth domain knowledge of the retail industry. This is a multi-disciplinary approach, bringing experts from different fields, including cybersecurity, risk management, compliance, and information technology.

Together, we meet the specific needs of each retailer, ensuring that our combined delivery achieves your risk management outcomes.

The Alfahive team

Alfahive has a team of highly trained and experienced professionals who specialize in cyber risk quantification and management. The team is well-versed in the latest cybersecurity technologies. We have a deep understanding of the regulatory environment and compliance burdens that banks face, which allows us to provide our customers with guidance and precision.

Conclusion

In conclusion, the Alfahive cyber risk automation platform has been instrumental in helping retail, consumer goods and hospitality organizations assess and quantify their risks with speed and quality. Using pre-curated and researched risk scenarios tailored for the retail industry, the platform has significantly reduced the time and resources required for regular cyber risk assessments, while providing a clear understanding of the cyber risks facing the organization, including the potential financial exposure and probability of an impact. Moreover, the platform has enabled organizations to make efficient risk management decisions.

Overall, the platform has helped organizations build cyber resilience, stay compliant with regulatory requirements, and communicate risk status and security controls in a common language. The data-driven approach to identifying and prioritizing risks and the ability to provide trustworthy and explainable quantification numbers in the context of the organization's business functions make the Alfahive platform an asset to any organization seeking to automate cyber risk assessment and quantification effectively.

Schedule a pilot with us today and see the value.

We invite forward-looking organizations to engage in a proof of value pilot to demonstrate the time and cost savings our platform can drive for risk managers.

See how you can:

- Save time and money by automating cyber risk assessment and quantification.
- Understand, measure, communicate, and make data-informed capital allocation decisions.
- Maximise the return on security investments by improving the utilization of the security assets.
- Begin to innovate your risk management processes for the future.
- Influence your organization to see risk and compliance as a strategic enabler.