SAFE

Top 5 Priorities for Today's CISO

Executive Summary

Top 5 Priorities for Today's CISOs

There's never been a better time to be a Chief Information Security Officer.
Yes, we know the counter arguments: nation state actors more active and better funded than ever, shortages in the cybersecurity workforce, AI powering threats we can't even anticipate.

But here's the optimist case for CISOs: We now see a way clear to cracking cyber risk management, meaning we can rationally plan cyber defenses to take our best possible shot at controlling loss exposure – and move confidently through a hostile cyber risk landscape.

In this report, we spotlight five priorities for CISOs and other cybersecurity and cyber risk leaders to confidently achieve a proactive cyber risk management program:

1. **Quantify Cyber Risks in Financial Terms**
2. **Achieve Continuous, Real-Time Risk Visibility**
3. **Enhance Third Party Risk Management**
4. **Integrate AI-driven Automation into Cybersecurity**
5. **Lead from Risk Management to Resilience**

1

QUANTIFY CYBER RISKS IN FINANCIAL TERMS

Quantify Cyber Risks in Financial Terms

With quantification, “it was easier for our stakeholders to feel concerned about cyber risk because they started understanding what it means for the business.”

Cedric De Carvalho
Head of Group Cyber Risk and Advisory
Luxury Goods Retailer Richemont (FAIR Inst. event)

Why It Matters

It’s a simple yet disruptive concept, that cybersecurity risk must be communicated to business decision makers not in technical terms but terms they can understand and act on: What would a cyber incident cost us? How likely is one to happen? How less likely would one be for how much investment?

Disruptive, because for too long status-quo security teams have produced risk reports as subjective red-yellow-green ratings, or check-the-box tallies against technical compliance frameworks with no relation to the real needs of the business.

It’s the difference between proactive and reactive cyber risk management

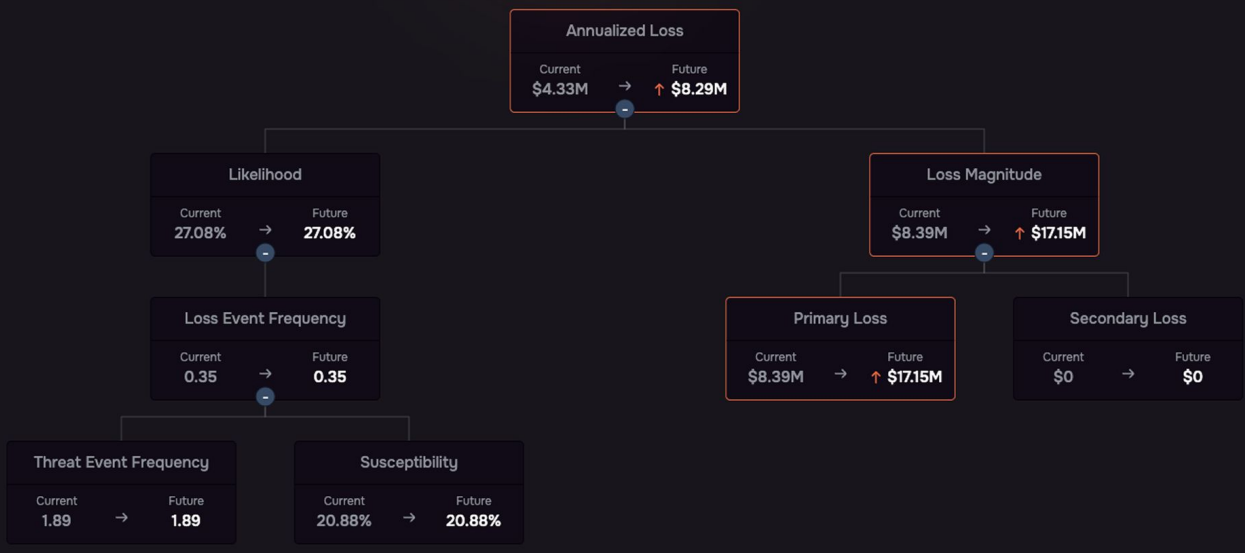
How to Achieve It

Choose the right model. Get the right tools. The FAIR™ model ensures credibility and consistency and importantly defensibility for risk analysis – FAIR is an open standard recommended by authorities such as the NIST CSF. The SAFE One platform automates every aspect of FAIR analysis, presented in the transparent terms of cost and likelihood that non-technical decision makers understand.

Actionable Insight

Cyber risk quantification enables a fundamental management activity in the cyber realm that’s simply not reliably possible without it: Prioritizing among projects, based on return for investment for risk reduction.

What Is FAIR™?



Transparency in risk analysis:
The FAIR model uncovers and quantifies all the factors that roll up to overall cyber risk.

By quantifying the factors that make up Likelihood and Loss Magnitude in a cyber incident, FAIR gives business decision-makers an accurate picture of cyber risk. FAIR has been recognized by the US National Institute of Standards and Technology as a standard for cyber risk assessment. Learn more about FAIR, meet FAIR experts and practitioners through the FAIR Institute. Join the Institute now, free to qualified professionals and students.

2

ACHIEVE CONTINUOUS, REAL-TIME RISK VISIBILITY

Achieve Continuous, Real-time Risk Visibility

> "When you have 200 security capabilities running across over 100 tools, you have a lot of data silos. When we started talking to SAFE, we started to realize the opportunity to unify that, to get that visualization that allows us to get to the right decisions at the right time"
>
> **Mike Elmore**
> **CISO**
> **GSK (SAFE event)**

Why It Matters

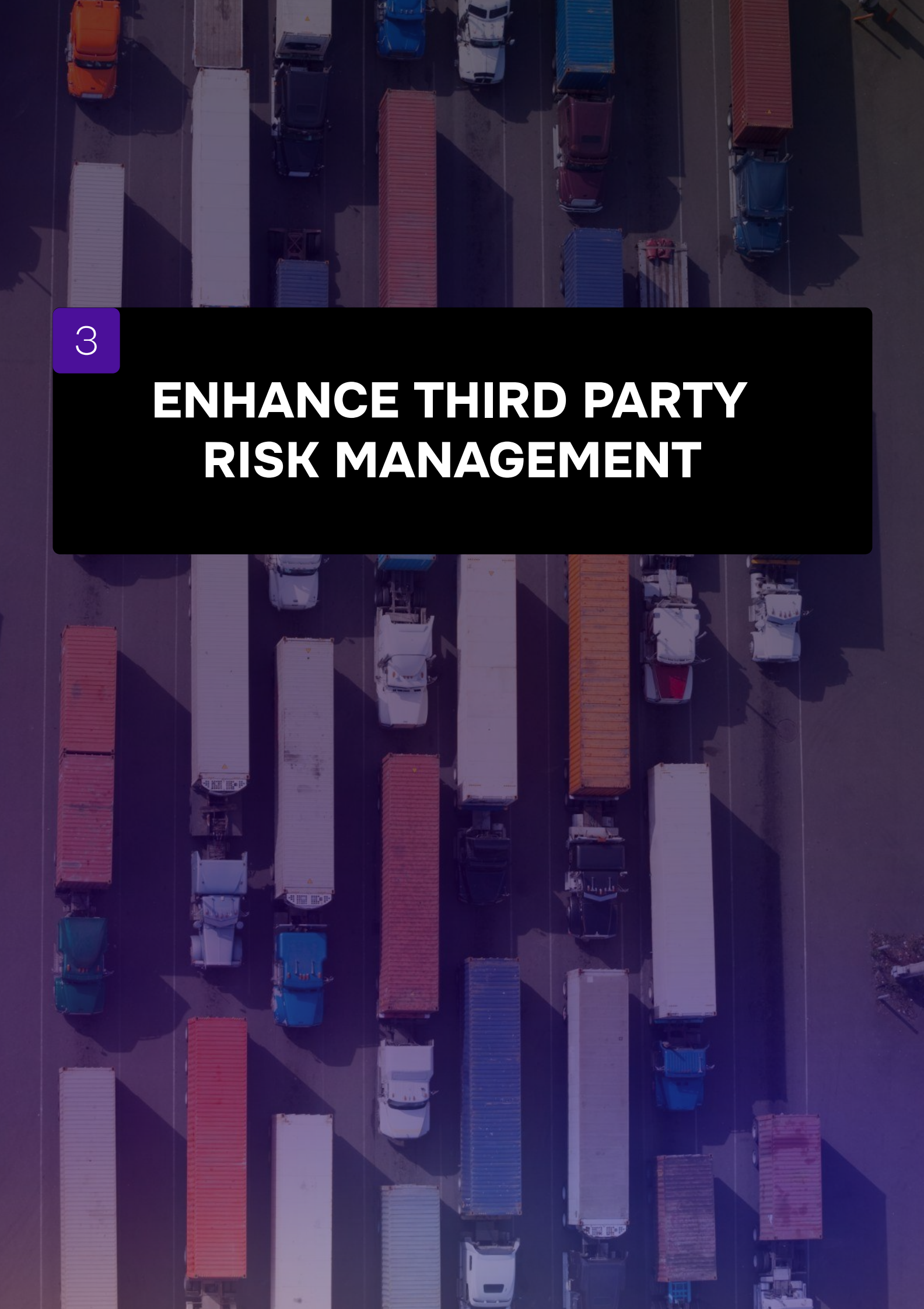
Cyber risk reporting must be quantitative. Now here's the rocket fuel. Risk reporting must be quantitative and continuous to stay ahead of today's threats – Microsoft reported 30 billion phishing attempts against its customers in 2024. But continuous reporting generates noise in security tooling; security alert fatigue is a well-known syndrome. Risk assessment must also be continuous, a constant read on ongoing and emerging risks, prioritized by their financial impact so humans can "make the right decision at the right times.".

How to Achieve It

Through integrations with the major security tools, the SAFE One platform ingests the latest security findings then conducts FAIR analysis on the spot. AI then takes over to generate real-time reporting. The result: meaningful alerts that show not just new threats or vulnerabilities but their probable impact in dollars. The SAFE platform also assesses the readiness and capabilities of the organization's cybersecurity controls at any time for the most accurate read on the enterprise's susceptibility to attacks.

Actionable Insight

As cybersecurity regulations grow tighter, so does the need to quickly quantify risk to determine if a security incident will have a material financial impact on the organization – elevating cybersecurity to a leadership position in a crisis.



3

ENHANCE THIRD PARTY RISK MANAGEMENT

Enhance Third Party Risk Management

> "What is the one thing that all our vendors who have had data breaches have in common? They all passed our third party-risk assessment!"
>
> **Sarah Sullivan**
> **Director IS&T Security Performance**
> **Thomas Jefferson University Hospitals (FAIR Inst. event)**

Why It Matters

Third party risk management (TPRM) is broken. It's an open secret, best known to the attackers who have pegged it as the soft underbelly of cybersecurity. But third party risk can equally come from errors by vendors like CrowdStrike who released a flawed security application that was deeply intertwined with Windows systems, leading to global system outages.
The standard tools of TPRM, such as questionnaires filled out by the third parties or outside-in scans of the third party's internet-facing controls (and no others). are too late and too limited to be effective, and badly in need of a complete rethink

How to Achieve It

In a TPRM Program Blueprint White Paper, SAFE presented five actionable steps for any organization to transform a third-party risk program into an effective risk-reduction tool.

1. Work closely with vendors on a set of priority" security requirements that third-parties need to manage first.
2. Work with your third parties to improve their cybersecurity posture, such as reducing rote compliance tasks with AI.
3. Implement zero trust and other internal controls to minimize access of third parties on your network.
4. Tier your third parties based on risk as defined by loss exposure in financial terms.
5. Expect your third party risk management to only grow - go with security vendors offering flat or fixed prices

Actionable Insight

Don't overshoot - in reality, it's a limited set of controls that protect you from third parties SAFE's Risk Radar report revealed the most exploited third-party controls and attack methods:

10 Most exploited Third-Party controls

1. Data Loss Prevention (DLP)
2. Network Segmentation
3. Network Firewall
4. Hardened Operating System
5. Data at Rest Encryption
6. User Access Control
7. Secured Software
8. Multi-factor Authentication
9. Endpoint Protection
10. People

5 Most exploited ATT&CK Techniques

1. T1020 - Automated Exfiltration
2. T1190 - Exploit Public-Facing Application
3. T1486 - Data Encrypted for Impact
4. T1489 - Service Stop
5. T1566 - Phishing

4

INTEGRATE AI-DRIVEN AUTOMATION IN CYBERSECURITY

Integrate AI-driven Automation in Cybersecurity

> "The [big] opportunity with AI is in using it to fundamentally reinvent [third-party risk management], making it more resilient and aligned with the new risk environment."
>
> **2025 EY Global Third-Party Risk Management Survey**

Why It Matters

Swinging a double edged sword - in the dark. That's artificial intelligence in these early days of widespread adoption of GenAI, LLMs, machine learning and AI agents. The promise of AI in cybersecurity is dazzling:

- Proactively analyzing patterns to predict behavior of attackers..
- Scalable, able to respond to high-volume attacks beyond human capabilities.
- Adaptive/resilient – Agentic AI will learn from past cyber incidents.
- Timesaving, attention-focusing for humans. The promise for cyber risk managers is freedom from rote work and bottlenecks in workflow.

Embedding deeply also raises new frontiers of insider risk: confidential data leaked by employees feeding an LLM or an error in logic leading agentic AI to mis-read malicious traffic as benign.

How to Achieve It

Effective introduction of AI into cybersecurity starts with careful planning.

- Understand the cybersecurity business context. Map your critical assets and business processes; understand where AI could hurt or help, for instance by solving for bottlenecks.
- Quantify the cybersecurity risk. The FAIR Institute has developed the FAIR-AIR approach to help prioritize among AI-generated risks for financial impact.
- Employ AI agents to onboard and assess risk for third parties at large scale and high speed.
- Implement robust cybersecurity controls. Once you have prioritized, implement controls that specifically address those scenarios.

Actionable Insight

Third-party risk management will be at the cutting edge for introduction of AI into enterprise risk management. AI agents, purpose-built to autonomously perform specialized tasks in the vendor management lifecycle, will streamline previously manual tasks and reduce human error. The result will be faster onboarding, prioritized risk decisions, real-time visibility into vendor posture, and continuous monitoring.

Automating Every Step of the Vendor Risk Management Lifecycle with Agentic AI

Using an AI system should be a virtually hands-free experience. The agents "know" what they have to do and perform their tasks singly and in collaboration with beyond-human speed. But developing agentic AI is another story. It starts with painstaking documentation of all the steps the agents will have to perform from onboarding through continuous monitoring to offboarding. Once built, the agents must be rigorously and repeatedly testing to make sure they are producing reliable and useful data – no room for AI "hallucinations."

Once you realize you're under attack, "the biggest thing you have to control is the panic...It's about how do you very quickly translate the tidbits of information that you get and get that back to the appropriate people...You may have to translate technical information into business impact up to your leadership teams...We had to shut down the email system because the attackers were monitoring our conversations...We did not communicate to the board or leadership before we shut it down. It was time sensitive, so I took the approach that I'll beg for forgiveness later."

Watch the SAFE CISO Confidential Interview

Randy Herold
CISO
(speaking about an experience at a previous job) **Manpower Group**

5

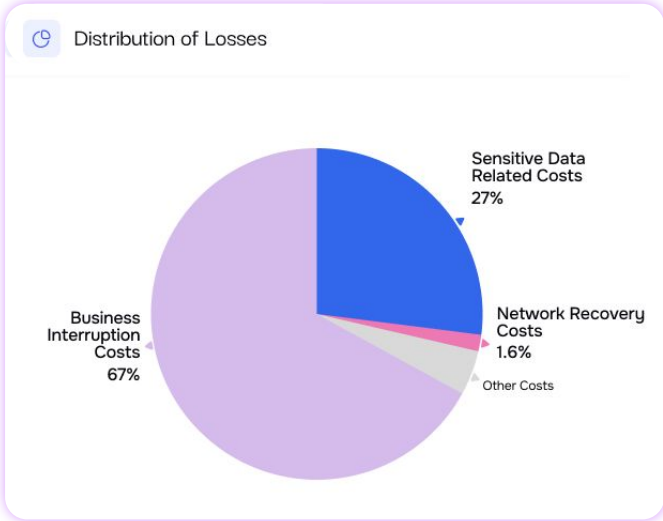
LEAD FROM RISK MANAGEMENT TO RESILIENCE

Lead from Risk Management to Resilience

> "If we look at the world as a bunch of servers and assets, then we continue to be technologists and we are losing sight of the real picture: We have business processes...the resiliency side of the equation. As a profession, we need to get way better at managing risk and resiliency."
>
> **Erik Decker**
> **CISO**
> **Intermountain Health**

Why It Matters

The most recent Risk Radar quarterly report from SAFE uncovered the surprising fact that two-thirds of the cyber-event losses in the study were in business interruption costs, not the data breaches that receive the bulk of the coverage in the news media. Think of the heart-stopping incident described by Randy Herold in the video above and it becomes clear that for a CISO, recovery is actually seamless with prevention and response.



In fact, resilience is the sum of the preceding five priorities - plus an extra factor, leadership by the CISO to fully align cybersecurity with the business.

How to Achieve It

Before the inevitable cyber crisis hits, CISOs should take the initiative on these high-level steps, working with the Board risk committee, business continuity team, IT management, legal and other players that must be kept in the decision loop.

1. Identify mission-critical assets and business processes..
2. Clarify the "risk threshold" the point beyond which the organization must take urgent action to protect those assets or processes, as defined by technical metrics (downtime) or financial impact (lost revenue).
3. Create risk scenarios that clarify the probable ways a cyber loss event might play out and the controls in place (or weak or missing) that would deflect the threat or mitigate the loss. Fix the control gaps, codify the manual for incident response.
4. Run tabletops, simulations, risk assessments to keep up preparedness.

SAFE

SAFE is the leader in AI-powered, continuous cyber risk management. SAFE empowers CISOs to become indispensable partners to the business, by enabling real-time quantification, prioritization, and mitigation of cyber risks, to support digital growth initiatives and ensure organizational resilience in the face of evolving threats.

Contact Us for a Live Demo

CATEGORY LEADER IN CRQ

FORRESTER CRQ WAVE Q3, 2023

LEADER IN THIRD PARTY RISK MANAGEMENT

LIMINAL LINK INDEX™ REPORT, 2025

CYBER INSURTECH OF THE YEAR 2025

INSURTECH, 2025

RESEARCH SPONSOR

MITRE ATT&CK, TOP CONTRIBUTOR

www.safe.security | getintouch@safe.security