2025 State of Cyber Risk Management

From Compliance to Competitive Advantage: The Quantified Value of Cybersecurity

June 26, 2025

The **2025 State of Cyber Risk Management Report** examines how leading organizations are adapting their cyber risk programs to meet increasing business, regulatory, and operational demands. Based on a global survey of 402 cyber risk leaders and practitioners, the report offers a data-driven examination of the practices, technologies, and outcomes shaping the future of the discipline.

From quantification and automation to executive governance and third-party oversight, this report highlights the strategies mature organizations use to reduce uncertainty, drive alignment, and turn cyber risk into a source of business resilience.

Table of Contents

Executive Summary

Conducted in May and June 2025 by the **FAIR Institute** with sponsorship from GuidePoint Security and Safe Security, the ***2025 State of Cyber Risk Management*** research provides a data-driven perspective on how mature organizations are addressing this challenge and where CRM is headed next.

Based on the responses from **402 CRM professionals around the globe**, this report provides the following **key takeaways**:

- → **CRM is fueling business results.** Top outcomes include improved alignment with the business, greater risk reduction, and optimized cybersecurity spending.
- → **Those with mature CRM programs are more proactive and business-aligned.** High-maturity organizations are more likely to have board-approved risk tolerances, quantify risk in financial terms, embed CRM across business functions, and have a more proactive cybersecurity posture.
- → **Factor Analysis of Information Risk (FAIR) and cyber risk quantification (CRQ) are gaining momentum.** Nearly 45% of organizations use or plan to use FAIR. Among adopters, 90% report success.
- → **Technology-focused C-suite decision makers benefit most.** CTOs, CIOs, and CISOs, along with Chief Risk Officers, are the primary consumers of cyber risk information, utilizing it to inform their strategy, investments, and resource allocation.
- → **Automation and AI are delivering scale and impact.** Seventy-two percent of organizations have mostly or completely automated their CRM systems, and 48% are utilizing AI for CRM. Both CRM automation and the use of AI are strongly correlated with maturity and improved outcomes.
- → **Data is foundational.** Organizations use a wide variety of telemetry, threat, and compliance data to inform their decisions. Those who can operationalize this data gain a clearer and more defensible picture of their risk exposure.
- → **Demand for CRM is growing, particularly among those with mature programs.** Nearly all (95%) respondents said internal demand for CRM is growing. Among those reporting high or very high CRM maturity, 23% indicate that demand will increase significantly.
- → **The board sets expectations for risk management but is not sufficiently engaged.** Nearly all respondents have defined risk appetite and tolerance levels that are formally approved by the boards; however, boards consume cyber risk information in less than half of the participating organizations.
- → **Challenges and gaps remain.** Cultural resistance, lack of executive support, and gaps in governance and metrics persist even among more advanced organizations.

This report reflects a maturing discipline, one that is evolving quickly to meet business demands. As CRM continues to integrate with enterprise strategy, those who lead with quantification, automation, and data will be best positioned to reduce uncertainty, enable smarter decisions, and build digital trust.

Our Research Methodology

The *2025 State of Cyber Risk Management* study was designed to explore how organizations with established cyber risk management (CRM) programs are evolving their practices, adopting new technologies, and aligning with business priorities. The research was developed and fielded by the FAIR Institute in collaboration with Hanover Research.

The study focused exclusively on professionals directly involved in CRM execution, including CISOs, risk managers, cyber risk analysts, and related roles. To ensure meaningful insights, respondents who reported "We have no cyber risk management capabilities" were disqualified. All respondents were required to pass a simple knowledge screener that asked, "Which of the following is the primary purpose of conducting a cyber risk assessment in an organization?" (Correct answer: "To evaluate the potential likelihood and impact of cyber-related losses.")

As a result of our qualification criteria, our respondents reflect a higher level of maturity and knowledge about CRM than we would expect from a general population of cybersecurity professionals and organizations. This was by design.

A total of **402 qualified responses** were collected in May and June 2025. Of these, 17 responses were obtained through a survey promotion to FAIR Institute members, while the remaining responses were sourced from a targeted panel managed by Hanover Research. Unless otherwise noted, the data cited throughout this report reflect a sample size of 402 (i.e., n=402).

The sample was global and cross-industry, capturing perspectives from organizations of varying sizes, sectors, and geographic regions.

The survey instrument included over 30 questions across six thematic areas:

- Cyber Risk Measurement, Maturity, & Adoption
- Challenges & Pain Points
- Integration & Automation
- Risk-Informed Decision Making & Outcomes
- CRM Strategy & Outlook

This rigorous design ensured that the insights presented in the report reflect the practices and perspectives of organizations that are actively managing cyber risk and leading the discipline forward.

The Evolution of Cyber Risk Management

Cyber risk management (CRM) is the process of *identifying*, *assessing*, *measuring*, and *responding*[1] to cyber risks. Like all risk management disciplines, CRM deals with uncertainty and probabilities. Cyber risks are a function of *probable loss events* and *probable loss magnitudes*. They depend on the likelihood that threat actors will attempt to cause a loss, your susceptibility to those threats, and the likely business impact should a loss event occur.

So, with all this uncertainty, why bother with CRM? The answer, as evidenced by this report, is that understanding cyber risk improves business outcomes. Assessing loss event scenarios and evaluating your risk factors, such as threat levels, the effectiveness of your controls, your ability to respond in a timely manner, and the adequacy of your insurance coverage, helps you make informed decisions and be a better cybersecurity leader.

CRM was rarely captured in literature a little over two decades ago. Now, CRM has since evolved into a **formalized discipline defined and codified** in numerous industry standards and regulatory frameworks, including ISO/IEC 27005, the NIST Cybersecurity Framework, the SEC Cybersecurity Disclosure Rule, and the EU Digital Operational Resilience Act. Sometimes referred to as *cybersecurity risk management*[2] or *information security risk management*[3], CRM is increasingly regarded as an element of due care under prevailing case law in many jurisdictions.

Yet the risk management demands put upon cybersecurity leaders are evolving faster than the standards and regulations that mandate their CRM programs. **CRM must deliver cost-effective risk reduction in a world of rapid change**. Hence, the question cybersecurity leaders must ask is how to manage cyber risk *cost-effectively*, at *scale*, and *at the pace of their business*. Our research explores this question.

Our data highlights *an important shift*: **organizations are moving beyond traditionally static and qualitative CRM approaches to more continuous, business-aligned programs featuring cyber risk quantification (CRQ)**. The more mature programs utilize automation, including AI, telemetry, and process integration, to enhance their operations. And they are better at driving business outcomes, such as greater risk reduction, optimized cybersecurity spending and budget justification, and improved credibility of the cybersecurity team and trust of internal business partners.

[1] Responding to cyber risks, or risk response, is sometimes called *risk treatment*.

[2] Per NIST Interagency Report (IR) 8286.

[3] Per ISO/IEC 27005:2022.

Those with CRM Programs Show Moderate or Better Maturity

To understand the practices, systems, data, outcomes, gaps, and challenges of individuals with CRM programs, we screened survey respondents for specific characteristics. These included familiarity with their organization's CRM practices, their job function (role) and department being pertinent to CRM, as well as other factors described in the section above, "Our Research Methodology." We disqualified any who reported that they had *no CRM capabilities*.

Therefore, our sample represents organizations that likely have established CRM programs. None of our respondents reported low maturity, as shown in the following table:

Survey Question: *How mature would you rate your organization's cyber risk management capabilities overall?*

Maturity Level	% of Total
Low maturity (i.e., we are in the early stages of our program or have not matured much from our starting point)	0%
Moderate maturity (i.e., we have a regular cadence for CRM processes and are regularly delivering value to our department or company)	26%
High maturity (i.e., we have a regular cadence for CRM processes, have developed advanced reporting and analytics, and are delivering significant value to our department and our company)	31%
Very high maturity (i.e., our CRM program is an integral part of how we plan, operate, and transform our company's technologies)	43%

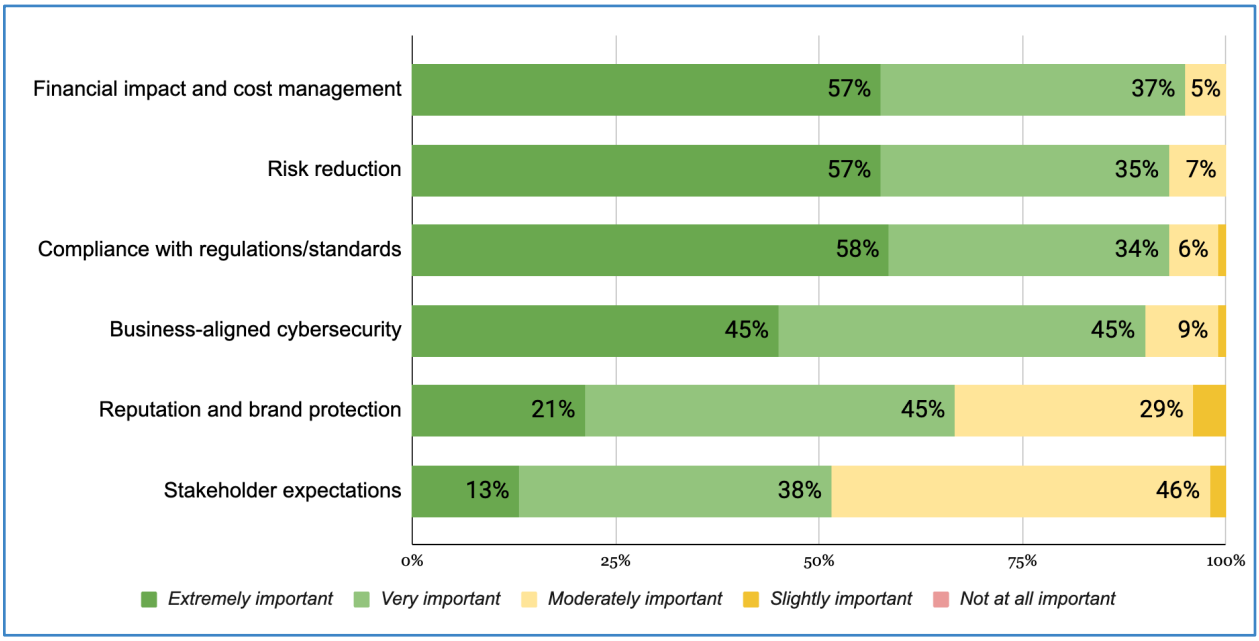
The higher level of maturity reflected in our data is encouraging but should not be misinterpreted as the state of CRM maturity in the general population. Indeed, CRM maturity itself is not the headline of this report. Instead, we often use this data to segment other factors in the report and show where maturity correlates with different metrics.

Throughout this report, we often refer to those respondents reporting "moderate maturity" as "**lower maturity**" and those with "high maturity" or "very high maturity" as "**higher maturity**" for ease of comprehension. In some cases, we will refer to each maturity level separately.

Cyber Risk Leaders Prioritize Business-Aligned Outcomes

CRM is tied to business priorities. When asked which outcomes matter most, respondents identified **financial impact and cost management, risk reduction**, and **compliance with regulations/standards** as their top three priorities. **Business-aligned cybersecurity** was also highly rated. This underscores that CRM isn't just a technical process; it's a strategic discipline that helps organizations drive business performance and resilience.

Survey Question: *How important are the following drivers of cyber risk management at your organization?*



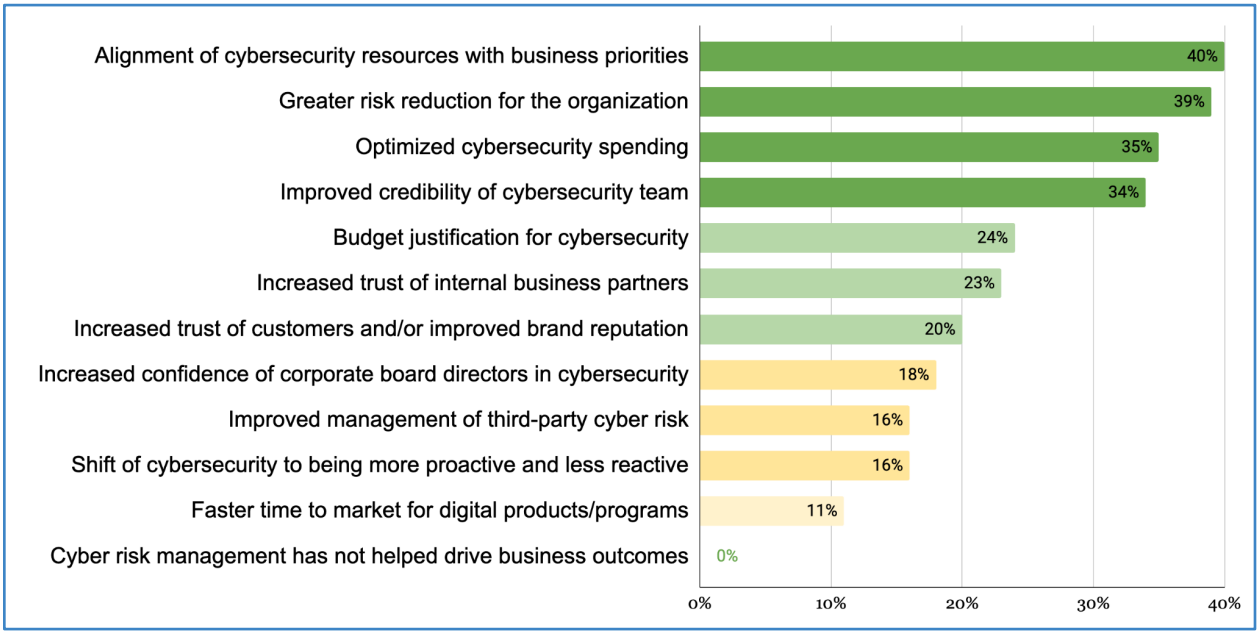
As boards and executives increasingly demand risk transparency in business terms, organizations that can translate cyber risk into financial impact are gaining a strategic advantage. They are better able to align cybersecurity investments with business priorities, optimize resource allocation, and respond confidently to emerging threats and regulatory expectations, outcomes that are more important in today's more turbulent economic conditions.

> "CISOs increasingly must think about enabling the business while protecting it. Cyber risk management, particularly when quantified based on FAIR, offers an effective mechanism for grounding our risk decisions in business outcomes."
>
> — Mary Elizabeth Faulkner, Chief Information Security Officer/ VP of IT Operations, Thrivent, and FAIR Institute Board Director

Cyber Risk Management Creates Value

CRM is delivering clear business value. Rather than operating in isolation, our data show that CRM is helping organizations achieve outcomes that align directly with their enterprise goals of risk reduction, strategic alignment, and budget optimization. CRM is no longer just a compliance mandate.

Survey Question: *What business outcomes has cyber risk management been most helpful in driving at your organization? Select up to three (3).*



We also found that CRM maturity matters, but even moderate maturity delivers outcomes. Respondents reporting higher CRM maturity were significantly more likely to report the following among their top three business outcomes compared to those with lower maturity ratings.

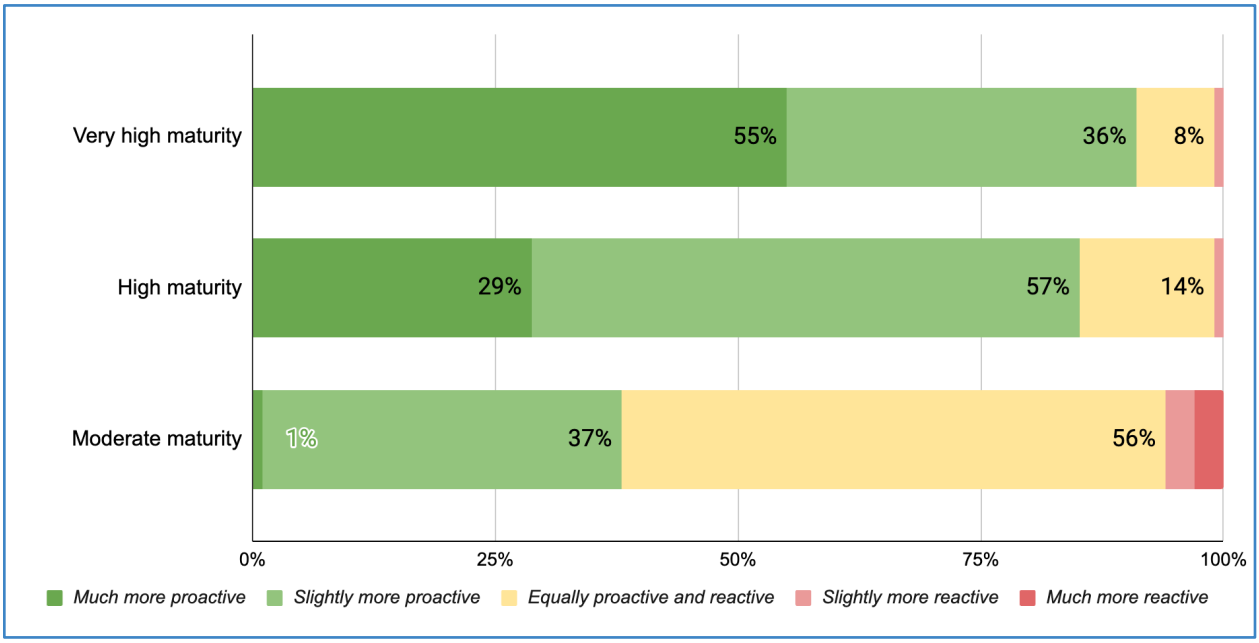
Survey Question: *What business outcomes has cyber risk management been most helpful in driving at your organization? Select up to three (3). [Segmented by CRM maturity level.]*

Business Outcome	% Selecting Among Top Three	
	Lower Maturity	Higher Maturity
Alignment of cybersecurity resources with business priorities	38%	41%
Greater risk reduction for the organization	33%	42%
Optimized cybersecurity spending	27%	38%
Improved credibility of the cybersecurity team	24%	37%

CRM Maturity Shifts Cybersecurity Posture

CRM is also shifting how organizations approach cybersecurity at a strategic level. The data shows a clear relationship between CRM maturity and a proactive cybersecurity posture. Organizations reporting higher maturity are significantly more likely to describe their cybersecurity efforts as **more proactive**.

Survey Question: *Are your organization's cybersecurity efforts more proactive or reactive? [Segmented by CRM maturity level.].*



Based on our observations, mature organizations can anticipate threats and mitigate vulnerabilities before they manifest rather than simply responding to incidents. As CRM capabilities grow through better data, automation, integration, and decision support, so does the ability to manage cyber risk as a dynamic business challenge rather than a static compliance issue.

> "As a CISO, I've seen firsthand how maturity transforms cybersecurity from a checklist exercise into a dynamic part of business strategy. Proactive risk management gives us the ability to anticipate threats, support smarter decisions, and stay aligned with the speed of the business. I'm not surprised the research bears this out. Our opportunity now is to deepen our partnerships across the business to deliver solutions that balance protection with agility, customer experience, and growth."
>
> — Alexander Antukh, CISO, AboitizPower, and FAIR Institute Board Director

FAIR Success Leads to Better Outcomes

FAIR is the industry-leading approach to cyber risk quantification and the only open standard for CRQ. According to our data, awareness of FAIR among respondents is nearly universal, at **99%**, and adoption levels are strong: **24%** currently use FAIR, with another **22%** planning to adopt it. Among those who have implemented FAIR, **90% report being successful**[4] with it.

Beyond its openness, what sets FAIR apart is its impact. Organizations that are very successful with FAIR report better business outcomes than those relying on other approaches, including non-FAIR cyber risk quantification approaches. Indeed, financial quantification alone does not appear to significantly alter business outcomes, per our data, as shown below.

Survey Question: *What business outcomes has cyber risk management been most helpful in driving at your organization? Select up to three (3). [Segmented by CRQ approach / success.]*

Top 3 Business Outcome	All Respondents	Financial Quantifiers	Very Successful with FAIR
Greater risk reduction for the organization	40%	41%	54%
Improved credibility of cybersecurity team / trust of internal business partners	56%	53%	77%
Optimized cybersecurity spending / budget justification	58%	59%	65%

CRQ is also on the rise more broadly. **31%** of respondents report *primarily* using a quantitative approach to CRM, all of whom **quantify cyber risk in monetary terms**. This indicates a clear shift toward a financial framing of cyber risk.

> "What sets FAIR apart are the decades of community involvement and refinement. Over the years, the methodology has been proven in real-world scenarios; that's why the business outcomes with FAIR greatly exceed those of other approaches."
>
> — Mark Tomallo, Fortune 500 CISO and FAIR Institute Board Director

[4] The level of success was self-reported by respondents, with options being "Very unsuccessful, "Somewhat unsuccessful," "Neutral," "Somewhat successful," and "Very successful."

The Technology C-Suite Benefits the Most

One of the clearest signs of CRM's evolution is its direct support for executive and board-level decision-making. After all, the C-suite and board are accountable for enterprise risk management (ERM), encompassing cyber risks. Accountability begins with setting expectations for cyber risk. Nearly all respondents have **defined risk appetite and tolerance levels** (99%) and had them formally **approved by the board** (90%).

CRM also improves executive awareness and decision-making, primarily among those in technology-focused roles. **C-suite tech leaders are the primary consumers of cyber risk information,** utilizing it to inform their strategy, investments, and resource allocation.

On the other hand, **boards appear largely split in their use of risk insights**. This may be due to the number of organizations that do not quantify risk in financial terms (nearly 70%). Financial quantification translates technical risk information into meaningful terms for board members from any background. As more organizations adopt financial quantification, we expect corporate boards to become better informed.

Business unit and product leaders also remain much less likely to engage with CRM outputs, highlighting an opportunity for further use of cyber risk information when making line-of-business decisions.

Survey Question: *What roles/offices at your organization are using cyber risk information? Select all that apply.*

Offices/Roles Using Cyber Risk Information	% of Total
Chief Technology Officer (CTO)	94%
Chief Information Security Officer (CISO)	92%
Chief Information Officer (CIO)	87%
Chief Risk Officer (CRO)	76%
Chief Financial Officer (CFO)	62%
Legal / General Counsel	58%
Board of Directors	45%
Business Units / Product Leadership	6%

The alignment between CRM and technology executive decision-making not only strengthens oversight but also enables organizations to operate within clearly articulated and board-sanctioned risk boundaries. However, greater involvement of the board and line-of-business leadership will enhance risk outcomes, including business alignment and optimized cybersecurity spending.

CRM Is Integrated with Enterprise Risk

As cyber risk grows in scope and consequence, integrating CRM into broader ERM frameworks is essential. Leading standards such as the NIST Interagency Report (IR) 8286 series explicitly call for this alignment, urging organizations to treat cyber risk as a core component of enterprise risk analysis, reporting, and governance.

Our survey findings support this trajectory. Nearly all respondents communicate cyber risks to ERM, while nearly four in ten both communicate and manage cyber risks *together with enterprise risks*. This is a key marker of maturity, as integration fosters shared risk language, clearer accountability, and better-informed executive decisions.

Survey Question: *What best describes how cyber risks are integrated into enterprise risk management at your organization?*

Integration of Cyber Risks with Enterprise Risk Management	% of Total
Organization does not have an enterprise or corporate risk management function	0%
Cyber risks are not communicated to enterprise risk management	1%
Cyber risks are communicated to enterprise risk management but managed separately from other enterprise risks	61%
Cyber risks are communicated to enterprise risk management and are managed together with enterprise risks	38%

This convergence ensures that cyber risk is evaluated alongside financial, operational, reputational, and strategic risks, enabling organizations to:

- Prioritize cybersecurity investments based on enterprise impact
- Align cybersecurity goals with business strategy
- Facilitate board-level oversight of technology risk

As regulations continue to emphasize board accountability and risk transparency, integration between CRM and ERM is quickly becoming a hallmark of high-performing organizations.

Organizations Tackle Third-Party Cyber Risk

As digital ecosystems become increasingly complex, third-party cyber risk has become a strategic concern, prompting organizations to respond accordingly. Every respondent in this year's survey indicated that their CRM programs extend to their third-party risk processes, with **64% applying CRM strictly** and **36% doing so loosely** (informally). However, the maturity of third-party CRM appears lower, with fewer respondents (62%) rating their third-party CRM as high or very high maturity, compared to the portion (81%) who did the same for first-party CRM.

Organizations report a wide range of benefits from third-party cyber risk management, as shown in the following table.

Survey Question: *What business outcomes have your third-party cyber risk management processes been most helpful in driving at your organization? Select up to three (3).*

Integration of Cyber Risks with Enterprise Risk Management	% of Total
Better alignment between procurement, security, and legal functions	30%
Greater visibility into critical third-party dependencies and risks	26%
Increased trust with customers, partners, and regulators	24%
Reduced residual risk from high-impact third-party relationships	24%
Enhanced scalability of third-party risk management through automation or tiering	24%
Stronger negotiating position with vendors regarding security obligations	19%
Improved response time to third-party cyber incidents	17%
Improved risk-based prioritization of vendor assessments	16%
Higher assurance of business continuity across critical vendors	16%
Strengthened contractual protections related to cybersecurity and data privacy	15%
Increased confidence in vendor onboarding and renewal decisions	14%
Improved executive and board reporting on vendor-related cyber risks	14%
Reduced frequency of vendor-related security incidents or data breaches	13%
Enhanced ability to meet regulatory and compliance requirements (e.g., GDPR, HIPAA, DORA)	7%

CRM Programs Automate as They Mature

Cyber risk management is no longer a manual process. According to this year's findings, **72%** of organizations have **mostly (61%) or completely (12%) automated their CRM systems**, while another 26% use a blend of manual and automated systems.

The use of automation is strongly correlated with CRM maturity. The table below shows the percentage of respondents, by degree of automation, who rated themselves as moderate, high or very high maturity.

Survey Question: *Are your organization's current cyber risk management systems manual or automated? [Segmented by CRM maturity.]*

Degree of CRM System Automation	CRM Maturity		
	Moderate	High	Very High
Mostly or completely automated	0%	9%	**91%**
Even mix of manual and automated	1%	21%	**78%**
Mostly or completely manual	6%	**60%**	34%

To improve automation, organizations are increasingly turning to *purpose-built CRM tools*, also known as CRQ solutions. The **majority (56%) rely on special-purpose CRM software**[5], outpacing the use of general-purpose GRC platforms[6] (24%), cybersecurity vendor[7] add-ons (19%), and custom-built solutions (2%)[8]. This shift toward specialized platforms reflects the growing demand for solutions tailored to cyber risk workflows, quantification, and third-party integration capabilities, which are not typically offered by legacy GRC tools.

> "CRQ solutions today look very different from CRQ solutions two years ago, and they cover entirely new territory than they did when they were first introduced…Now, advances in automation, UX, and integrations, coupled with better industry loss data and threat intelligence, have ushered CRQ solutions into a new era. CRQ solutions address several governance, risk, and compliance (GRC) use cases that bridge the gap between risk and security operations."
>
> — Forrester (2025). The Forrester Wave™: Cyber Risk Quantification Solutions, Q2 2025. Cody Scott et al. June 18, 2025.

[5] Representative vendors include CRQ vendors such as Axio, Ostrich Cyber-Risk, KPMG, SAFE.

[6] Representative vendors include GRC vendors such as Archer, MetricStream, OneTrust, ServiceNow.

[7] Representative vendors include cybersecurity vendors such as Trend Micro, Qualys, Threat Connect, Zscaler.

[8] Percentages add up to 101% due to rounding of individual values.

CRM Automation Improves Business Outcomes

Automation isn't just becoming more widespread, its use is effective for driving the most essential outcomes cited earlier in this report. Survey data shows a strong correlation between higher levels of automation and improved business outcomes across the board.

As shown in the following table, organizations that have mostly or completely automated their CRM systems were more likely to cite the essential outcomes among their top three.

Survey Questions: *What business outcomes [has cyber risk management] | [have your third-party cyber risk management processes] been most helpful in driving at your organization? Select up to three (3). [Segmented by degree of CRM system automation.]*

Business Outcome	Partial Automation	High Automation
Greater risk reduction	36%	41%
More optimized cybersecurity spending	32%	37%
Better alignment across security, legal, and procurement	18%	34%
Improved scalability in third-party risk management	14%	28%
Reduced residual risk from high-impact third parties	17%	26%

In short, automation goes hand in hand with essential business outcomes for CRM programs that may otherwise struggle to keep pace with their businesses.

Programs Integrate with Non-Cyber Operations

Cyber risk management is no longer confined to security teams; it's increasingly embedded across the operational fabric of the enterprise. Our data shows that organizations are integrating CRM into a diverse array of business and IT functions, reflecting its growing role in day-to-day decision-making and governance.

The most common integration points are technical, involving IT asset management, configuration management, and IT service management (e.g., ticketing and resolution processes). However, CRM is also extending into core business disciplines such as finance and accounting, legal and compliance, and vendor/supply management.

Survey Question: *What best describes how cyber risks are integrated into enterprise risk management at your organization?*

Operational Process or Discipline Integrated with CRM	% of Total
IT asset management/configuration management	96%
IT service management (e.g., ticketing, resolution)	95%
Finance and accounting	81%
Legal and compliance	77%
Vendor/supply chain management	40%
Product development/management	29%
Change management	16%
Human resources	15%

Clearly, integration with product development, supply chain, and HR is still emerging. Given the importance of third-party cyber risk management (as discussed earlier), we expected to see vendor/supply chain management integration at a greater rate. As product development and other business changes often introduce or alter cyber risks for the enterprise, we would like to see tighter integration with those processes as well. Finally, in light of insider risk management programs (e.g., background checks) and security awareness initiatives, we expected to see more CRM-HR collaboration.

Despite opportunities for improvement, the pattern is clear: CRM is becoming an operational discipline across the organization, shifting from a siloed risk practice to a shared enterprise responsibility.

Data Is the Lifeblood of Cyber Risk Management

Cyber risk is fundamentally a problem of uncertainty. Effective CRM programs reduce that uncertainty by grounding decisions in measurable inputs, starting with data from commonly deployed cybersecurity tools. As shown here, organizations utilize a diverse range of data sources to inform their CRM decisions. The breadth of data inputs reflects both the complexity of the threat landscape and the growing maturity of CRM practices.

Survey Question: *What data does your organization regularly use for cyber risk management? Select all that apply.*

Data Sources Used for CRM	% of Respondents
Endpoint security data	78%
Cyber threat intelligence (CTI) data	77%
Compliance audit results	76%
SIEM data and/or network traffic logs	66%
Vulnerability assessment findings	65%
Incident response records	61%
Cloud management systems (e.g., AWS, Azure, GCP)	44%
Third-party risk assessments	39%
Asset data (e.g., CMDB)	35%
User access logs	32%
Vulnerability assessment reports	32%
Penetration testing / red teaming results	24%
Product/service definitions	21%

The more data CRM programs can draw upon, the better they can assess likelihoods, model impact, prioritize mitigation efforts, and communicate findings in business-relevant terms. As CRM has become increasingly quantitative and integrated, data is an indispensable component of CRM systems and programs.

AI Is Not Limited to Experimental Use

Artificial intelligence is rapidly becoming a core component of CRM and is not just an emerging technology. This year's data shows that **48% of organizations already use AI for CRM**, while 34% are actively experimenting, and yet another 16% plan to adopt AI. Of those experimenting with or planning to adopt AI for CRM, 61% expect to do so within the next 12 months.

We must interpret this data cautiously: it does not reveal *exactly how* organizations are using AI for CRM. In our experience, AI is often used for underlying capabilities such as threat detection, incident response, malware analysis, vulnerability management, and attack surface monitoring. AI is also supporting third-party risk management by processing unstructured data such as vendor contracts, SOC2 reports, and questionnaire responses, sometimes to populate CRQ models. However, its use for CRQ and other core aspects of CRM appears to be emerging and net yet well established.

In our data, AI adoption is **strongly correlated with CRM maturity**. Organizations using AI report significantly higher levels of maturity across nearly every major CRM capability, from first-party and third-party risk management to cyber risk mitigation, disclosure, and board reporting. AI users also demonstrate a **more proactive cybersecurity posture**. 91% of organizations using AI describe their approach as *slightly more proactive* or *much more proactive* than reactive, compared to just 62% of non-AI users. These findings suggest that AI is accelerating CRM workflows and reshaping how organizations identify, respond to, and communicate cyber risk.

> "AI is fast becoming a pervasive enabler of innovation and productivity. But the speed at which businesses are now innovating and the uncertainties it brings are creating new challenges for CISOs. It's great to see that CISOs and risk teams are increasingly utilizing AI to better manage cyber risk. Since this often involves working with unstructured data and complex data relationships, AI is well-suited to many cyber risk tasks. Businesses should continue to embrace AI where they can get an edge, as our adversaries certainly will be doing so."
>
> — Omar Khawaja, Field CISO, Databricks and FAIR Institute Board Director

Challenges and Gaps Persist

Even among organizations with established cyber risk management programs, obstacles often remain. The three most cited challenges or gaps are **poor communication between departments** (37%), **resistance from peers and stakeholders** (34%), and a **lack of executive commitment or prioritization** (33%).

Those organizational issues are far more common than technical issues such as **lack of reliable threat intelligence** (19%) and **inadequate third-party control data** (15%), or resource constraints such as **insufficient resources and budget allocation** (10%) or **inadequate analyst skills** (9%).

When it comes to gaps and challenges, there are some areas where maturity matters more than others. The following table reveals the barriers where lower CRM maturity increases their likelihood more dramatically.

Survey Questions: *What challenges with cyber risk management do your organization face? Select all that apply. | What gaps do you believe exist in your organization's current cyber risk governance and accountability structures? Select all that apply. [Segmented by CRM maturity level.]*

CRM Challenge or Gap	% Reporting Gap or Challenge, by Maturity Level		Decreased Likelihood with Higher Maturity
	Lower Maturity	Higher Maturity	
Insufficient resources and budget allocation	17%	8%	-53%
Inadequate third-party risk management	21%	12%	-43%
Lack of integration with overall business strategy	26%	17%	-35%
Lack of support from business partners	29%	20%	-31%
Lack of a formalized risk management framework	30%	24%	-20%
Lack of executive commitment or prioritization	38%	32%	-16%
Poor communication between departments	42%	36%	-14%

The Future of Cyber Risk Management

CRM is entering a new era defined by risk quantification, increased automation, and business impact. As our research reveals, leading organizations have made CRM a proactive, data-driven discipline that informs strategic decisions and drives enterprise value. While CRM is mandated across many industries and countries, it is no longer constrained to (or by) compliance mandates.

Several powerful trends are shaping this future:

- **Demand for CRM Is Growing Internally**
  Nearly three-quarters of respondents face rising demand for CRM from internal stakeholders, driven by executive awareness, regulatory expectations, and the need for credible, data-driven cybersecurity decisions based on quantitative insights.

- **FAIR and Quantification Continue to Expand**
  With nearly half of our respondents using or planning to use the FAIR model, financial quantification is rapidly becoming the standard for expressing cyber risk. This movement enables clearer communication, more defensible decisions, and better alignment with the business.

- **Automation and AI Become Institutionalized**
  What began as experimentation is quickly becoming infrastructure. Most organizations now use automated CRM systems, and nearly half are using AI to drive greater scale and consistency. These technologies are becoming foundational to effective CRM.

- **CRM Embeds into Enterprise Governance**
  As boards demand clearer visibility and tighter control over cyber risk, CRM is increasingly integrated into governance processes. High-maturity organizations define and approve risk appetite and tolerance at the board level, embedding cyber risk oversight into the enterprise risk management structure.

- **Regulatory Pressure Accelerates Progress**
  Far from being a drag on innovation, regulatory developments such as the SEC Cybersecurity Disclosure Rule and the EU's Digital Operational Resilience Act are acting as accelerants. They're driving clarity, consistency, and executive engagement, raising the bar for CRM performance.

Together, these shifts point toward a future where cyber risk is better managed and delivers greater value beyond compliance. CRM is maturing into a discipline that empowers organizations to navigate uncertainty with confidence, communicate risk in business terms, and protect what matters most in an increasingly digital world.

Participant Demographics

Respondent Country	%
Australia	3%
Canada	11%
France	7%
Germany	9%
Italy	5%
New Zealand	2%
Philippines	<1%
Singapore	1%
South Korea	1%
Spain	5%
Taiwan	1%
United Kingdom	16%
United States	37%

Annual Revenue	%
$0 to <$50 million	<1%
$50 million to <$250 million	7%
$250 million to <$500 million	7%
$500 million to <$1 billion	15%
$1 billion to <$5 billion	35%
$5 billion or more	34%
Don't know/Prefer not to respond	1%

Respondent Industry	%
Arts, Entertainment, & Recreation	<1%
Automotive	1%
Banking	14%
Consumer Products (CPG)	<1%
Construction/Architecture	5%
Distribution/Transportation	<1%
Education	1%
Financial Services	11%
Healthcare/Medical	13%
Hospitality/Travel	1%
Information Technology	9%
Insurance	12%
Manufacturing	10%
Oil and Gas	<1%
Public Admin / Government	1%
Retail	10%
Telecommunications	5%
Utilities	4%

Organization Size	%
1,000 to 4,999 employees	37%
5,000 to 24,999 employees	43%
25,000 to 49,999 employees	6%
50,000 employees or more	13%

Respondent Office	%
Chief Info Security Officer	37%
Chief Risk Officer	26%
Chief Information Officer	4%
Chief Technology Officer	32%
Chief Financial Officer	<1%
Internal Audit	<1%

Respondent Job Function	%
Compliance	12%
Cybersecurity	19%
Cyber Risk Management	21%
Enterprise Risk Management	5%
Third-Party Risk Management	1%
Information Security	13%
Information Technology	28%

Job Level	%
Associate/Analyst	19%
Manager/Sr. Manager	38%
Director/Sr. Director	36%
VP/SVP/C-Suite	7%

Years of Experience	%
2 to 5 years	19%
6 to 10 years	33%
11 to 15 years	34%
16 to 20 years	8%
More than 20 years	5%

Report Contributors and Reviewers

The FAIR Institute would like to thank the following professionals and thought leaders for their time, contributions, advice, and feedback in the development of this report.

- **Dr. Chon Abraham**, PhD, Pulley Professor of Principled Leadership (Cyber Risk), Mason School of Business, William & Mary
- **Alexander Antukh**, CISO, AboitizPower, and FAIR Institute Board Member
- **Glen Armes**, Founder and Fractional CISO, Armes-Vantage
- **Brandon Bapst**, Senior Manager, EY
- **Zach Cossairt**, Integrated Risk Program Lead, Equinix
- **Pankaj Goyal**, Chief Operating Officer, SAFE
- **Michelle Grist**, Head of Info Security and Resilience, Unite Students
- **Dana Haubold**, Cyber Security Advisor/CISO, DH Cyber Security Consultancy
- **Abhishek Iyer**, Manager, Information Risk and Compliance, CarGurus
- **Jack Jones**, Chairman Emeritus, FAIR Institute
- **Caleb Juhnke**, Head of Cyber Risk Management, Elsevier
- **Tony Martin-Vegue**, Staff Security Risk Engineer, Netflix
- **Ben Moreland**, Practice Director, IA, GuidePoint Security
- **Steve Reznik**, Lead Security Analyst, TriNet
- **Shaun Roberts**, CISO, Railpen
- **Nick Sanna**, President and Founder, FAIR Institute
- **Eugene Teo,** Chief Security Advisor, ASEAN, Microsoft, and Co-Chair, FAIR Institute Singapore Chapter
- **Todd Tucker**[9]**,** Managing Director, FAIR Institute
- **Jay Vinda**, Global CISO & Cyber Risk Engineering Lead, Mosaic Insurance
- **Laura Voicu**, PhD, Principal Security Assurance, Elastic.io, and Co-Chair, FAIR Institute Swiss Chapter
- **Michael Walters**, CISO, Washington State University
- **Denny Wan**, Founder and Principal Consultant, The Reasonable Security Institute, and Co-Chair, FAIR Institute Sydney Chapter

[9] Principal author of this report.

About Our Sponsors and the FAIR Institute

The FAIR Institute thanks GuidePoint Security and SAFE for their counsel and support for this research.

GuidePoint Security

GuidePoint Security is an advisory partner of the FAIR Institute. GuidePoint provides trusted cybersecurity expertise, solutions, and services that help organizations make better decisions that minimize risk. GuidePoint's experts act as your trusted advisor to understand your business and challenges, helping you through an evaluation of your cybersecurity posture and ecosystem to expose risks, optimize resources, and implement best-fit solutions. GuidePoint's unmatched expertise has enabled 40% of Fortune 500 companies and more than half of the U.S. government cabinet-level agencies to improve their security posture and reduce risk. Learn more at www.guidepointsecurity.com.

SAFE

SAFE is the founder and technical advisor of the non-profit FAIR Institute. SAFE is redefining cyber risk management through Agentic AI. SAFE helps CISOs, GRC, and TPRM leaders continuously and efficiently quantify, prioritize, and mitigate cyber risks — enabling digital growth and resilience. SAFE is the category leader in Cyber Risk Quantification (CRQ) and the first vendor to deliver fully autonomous Third-Party Risk Management. Trusted by global enterprises such as Google, Fidelity, T-Mobile, Chevron, and Peloton, SAFE has achieved over 100% year-over-year revenue growth for three consecutive years and has raised over $100m. Learn more at www.safe.security.

The FAIR Institute

The FAIR Institute is a non-profit professional organization dedicated to advancing the discipline of measuring and managing cyber and operational risk. With over 17,000 members worldwide, the Institute is recognized as a leading authority on cyber risk quantification and best practices in management. The FAIR Cyber Risk Management Framework, based on the industry's leading CRQ methodology, has been adopted by organizations across sectors to enhance security governance and risk-informed decision-making. Learn more at www.fairinstitute.org.