cafii acifa
The Canadian Association of Financial Institutions in Insurance | L'association canadienne des institutions financières en assurance

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

CAFII ALERTS WEEKLY DIGEST: March 18 – March 22, 2024

March 22, 2024

The CAFII Alerts Weekly Digest is intended to provide a curated compendium of news on insurance, regulatory, and industry/business/societal topics of relevance to CAFII Members – drawn from domestic and international industry trade press and mainstream media – to aid in Members' awareness of recently published media content in those areas.

TABLE OF CONTENTS

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

GOVERNMENT/LEGAL/REGULATORY/ BUSINESS DEVELOPMENTS

Most Canadian Homeowners Do Not Carry Sufficient Coverage

By Kate McCaffery, Insurance Portal, March 20, 2024

New research by LIMRA, commissioned by the Canadian Association of Financial Institutions in Insurance (CAFII), found that 80 per cent of Canadian homeowners lack sufficient insurance coverage, being either uninsured or underinsured with creditor protection insurance (CPI) or traditional life insurance.

The research also found that and 38 per cent of homeowners with credit are "at risk." These are homeowners with credit who have dependents but are not sufficiently insured.

Furthermore, the study showed that 55 per cent of Canadian homeowners use CPI.

CAFII says the primary objective of the research was to show the prevalence of insurance products, with a particular focus on CPI. "The results have raised significant concerns about the financial security of numerous Canadian families," they write in a statement about the survey's release. "The report set out to address pivotal questions regarding the insurance environment among Canadian homeowners. It sought to ascertain whether individuals with lower incomes prioritize CPI over others and whether CPI plays a significant role in the market for homeowners.

Read full article (subscription reqiured): *https://insurance-portal.ca/article/most-canadian-homeowners-do-not-carry-sufficient-coverage/*

Regulatory Organization Appoints New Chair

By Donna Glasgow, Insurance Portal, March 14, 2024

https://insurance-portal.ca/society/regulatory-organization-appoints-new-chair/?utm_source=sendinblue&utm_campaign=daily_complete_202403-19&utm_medium=email

The Canadian Insurance Services Regulatory Organizations (CISRO) announced on March 14 that Patrick Ballantyne has been appointed as its new Chair. He succeeds Eric Jacob in this position.

Ballantyne is currently CEO of the Registered Insurance Brokers of Ontario (RIBO). He has held this position since 2016. According to a statement on March 14 that Patrick Ballantyne has been appointed about his announcement, Ballantyne has more than 30 years of leadership experience in legal and regulatory compliance in the financial services industry. He was called to the Ontario Bar in 1987.

Outgoing Chair, Eric Jacob is Executive Director, Enforcement at the Autorité des marchés financiers (AMF). He held the position as CISRO's Chair from December 2021 to February 2024, according to his LinkedIn profile.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

In a statement, Ballantyne thanked Jacob for his work with the organization. "Under Eric's leadership, CISRO has invested in important activities to strengthen the organization, while pursuing initiatives in close collaboration with the Canadian Council of Insurance Regulators to enhance the fair treatment of customers."

CISRO is a forum of Canadian regulatory authorities for information sharing and collaboration between regulators responsible for licensing and registration of insurance intermediaries. Last fall it published its three-year plan, Strategic Plan 2023-2026.

OTHER CAFII MEMBER-RELEVANT NEWS

Is The Gender Wage Gap Widening In Insurance?

Desjardins Sheds Light

By Gia Snape, Insurance Business, March 21, 2024

https://www.insurancebusinessmag.com/ca/news/breaking-news/is-the-gender-wage-gap-widening-in-insurance-482220.aspx?hsmemberId=83982452&tu=&utm_campaign=&utm_medium=20240321&_hsmi=299269177&_hsenc=p2ANqtz-_lTjiI_f7VZI1fyThYLwaptmm2XKZuXTfBQjwHsweArypNRyckBhKsQypx5Yr8VxLDsKjGYmF2lpRuIBctDxVkswWMag&utm_content=&utm_source=

While many Canadian industries have made progress toward narrowing the gender wage gap over the past decade, insurance has gone the opposite way.

Data from Statistics Canada and Desjardins Economic Studies has shown that the gender wage gap widened in insurance between 2013 and 2023. That's despite women holding 56% of roles in insurance.

The findings were shown in a recent Desjardins report highlighting persistent gender disparities in the Canadian workforce.

The research found that despite the narrowing of gaps, significant barriers remain to a more equitable environment for women professionals and entrepreneurs.

"Narrowing the earnings gap is not just a women's issue, it's an issue for all Canadians," said Kari Norman (pictured), Desjardins economist and the study's co-author.

Gender Wage Gap – How Does Canada And Its Industries Fare?

Despite being highly educated, Canadian women earn an average of 17% less than men, according to the Desjardins study.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

This figure is significantly higher than other Organisation for Economic Co-operation and Development (OECD) peers, with the OECD average standing at 12%.

Scotiabank Unveils 2023 ESG And Climate Reports

The Bank Details Progress In Sustainability And Climate Action, Highlighting Investments And Achievements

By Freschia Gonzales, Wealth Professional, March 15, 2024

https://www.wealthprofessional.ca/investments/socially-responsible-investing/scotiabank-unveils-2023-esg-and-climate-reports/384579?hsmemberId=83982452&tu=&utm_campaign=&utm_medium=20240315&_hsmi=298398913&_hsenc=p2ANqtz--uZCn1gbPlmi6nJqHqPBtFTwCetLVj4JC23s-nJR3ks08puo5dTbLq9rLOyfJ2VRzl-b_j8iAaxeg7aM3V4PO0N06fSA&utm_content=&utm_source=

Scotiabank has announced the release of its 2023 environmental, social, and governance (ESG) Report alongside its 2023 Climate Report.

The reports provide detailed insights into the bank's sustainability endeavors and achievements over the year.

"I am proud to share Scotiabank's 2023 ESG and Climate reports, which outline our ongoing progress towards our social and environmental goals, with a view to supporting our clients, employees, and communities," stated Scott Thomson, Scotiabank's president and CEO.

He further emphasized the bank's commitment to integrating ESG actions within its business strategy to fortify its position as clients' most trusted financial partner. This strategic integration encompasses enhancements in products and services and the bank's approach to recognizing and rewarding success.

The 2023 ESG Report is notable for including Scotiabank's Canadian Public Accountability Statement and its annual sustainable bond use of proceeds reporting.

The report features significant achievements, such as the ScotiaRISE initiative's investment of a cumulative $102m over the last three years in 200 organizations. This effort is part of a broader goal to invest $500m over ten years to strengthen economic resilience.

The report also highlights an employee engagement rate of 87 percent, surpassing the average in the financial sector.

Another noteworthy accomplishment is the Scotiabank Women Initiative, which has engaged over 25,000 women entrepreneurs worldwide and has deployed $8bn in capital to women-led and women-owned businesses in Canada since the fiscal year 2019.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

This initiative is on track to meet its commitment of deploying $10bn in capital by 2025.

In its 2023 Climate Report, Scotiabank delineates its climate-related goals, including financing climate-related activities, advancing towards net-zero financed emissions, and reducing the bank's own emissions.

Meigan Terry, the SVP and chief sustainability, social impact, and communications officer at Scotiabank, acknowledged the "challenging, urgent, and complex work ahead of us in addressing climate change."

The bank pledges to support clients across all sectors in their transition efforts and contribute to a more resilient planet.

Among the Climate Report's updates, Scotiabank has released the Climate-related Finance Framework and has achieved $132bn towards its goal of providing $350bn in climate-related finance by 2030.

It has set an interim emissions intensity reduction target for the automotive manufacturing sector. It has distributed $1m through the Net-Zero Research Fund, totaling $3m since the fiscal year 2021, to support 31 research projects and initiatives.

Scotiabank's sustainability reporting has consistently earned accolades. For the third consecutive year, it maintained a "AAA" ESG rating from MSCI, a distinction shared by only 5 percent of global industry peers.

TD On Sustainability And Corporate Citizenship

Targets Being Met For The Benefit Of Clients And Communities

By Terry Gangcuangco, Insurance Business, March 15, 2024

https://www.insurancebusinessmag.com/ca/news/environmental/td-on-sustainability-and-corporate-citizenship-481337.aspx?hsmemberId=83982452&tu=&utm_campaign=&utm_medium=20240315&_hsmi=298391744&_hsenc=p2ANqtz-_npI-jbNUYXCSUxnt2hjJAtH7qcyyt36BT8Z7QzAg_EvBXTlKuQUL_0ywEe1vr9aJBeiysvagFLM9kXsGFQUytcqnKbw&utm_content=&utm_source=

TD Bank Group, also known simply as TD, has updated its stakeholders on the progress of the company's sustainability strategy, as it commits to helping clientele, local communities, and employees.

Janice Farrell Jones, senior vice president of sustainability and corporate citizenship at TD, pointed out the significant challenges faced by people over the past year, including escalating living costs and the impacts of climate change.

She said: "As a financial institution and corporate citizen, TD has a role to play in supporting our customers and communities through these times while contributing to efforts to build a more

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

sustainable and inclusive future. The updates shared in our Sustainability Reporting Suite highlight the ways we're taking action to help drive sustainable value creation for our customers and our communities."

According to TD, it has made strides in its climate action plan, which doubles as the bank's blueprint for transition. TD also reached a significant milestone in its sustainable & decarbonization finance target by facilitating $69.5 billion in eligible business activities last year.

Additionally, the bank surpassed its objective of engaging 50% of its clientele in the energy and power generation sectors, thanks to the initiatives spearheaded by TD Securities, and has set an ambitious target of 75% engagement for 2024.

Further cementing its role in promoting sustainability and corporate responsibility, TD has intensified its efforts to support financial and economic inclusion. As part of its commitment to the TD Pathways to Economic Inclusion initiative, the bank unveiled five new targets spanning US and Canadian small business lending, North American financial education, affordable housing finance in North America, and home lending in the US.

The 2023 TD Ready Challenge also saw the bank awarding $10 million in grants to innovative projects tackling housing affordability.

Noteworthy achievements from the 2023 Sustainability Reporting Suite also include the issuance of a US$500 million green bond led by a diverse syndicate of underwriters. In addition, TD contributed $157 million to various non-profit and community organizations in 2023, progressing towards its goal of $1 billion in philanthropic contributions by 2030.

The Cyber Clock Is Ticking: Derisking Emerging Technologies In Financial Services

As Financial Institutions Actively Adopt Emerging Technologies, They Should Act Now To Future-Proof Themselves Against Growing Cyber Risks.

By Lamont Akins, Soumya Banerjee, Lauren Craig, Grace Hao, Justin Greis, Matin Boer, and Melanie Idler, McKinsey & Company, March 11, 2024

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services?cid=sig-eml-nsl-mst-mck-ext---sig--&hlkid=23521302efeb4e02aade76c54fcb471b&hctky=10045072&hdpid=59bdf92b-5b64-4b27-aecf-d5296e8cd633

As financial-services companies around the world race to keep pace with a rapidly evolving technology landscape, they should consider not only what benefits new emerging technologies offer but also what risks they introduce.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

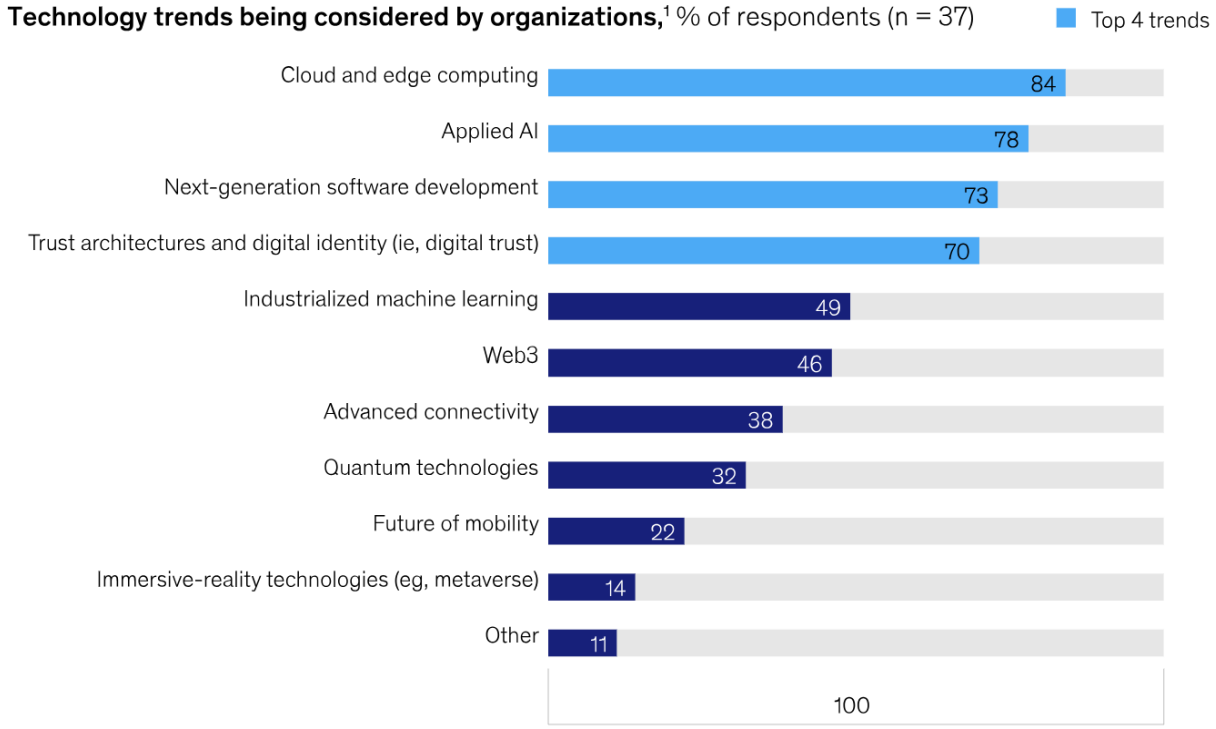
To understand how companies are grappling with the best ways to use and protect the technologies of today and tomorrow, McKinsey partnered with the Institute of International Finance (IIF) to survey financial institutions around the world regarding their current and planned usage of ten key emerging technologies. (For details on research methodology, including the short-listing of top technology trends, based on global industry trends, see "Appendix: Approach and methodology.") How are companies approaching emerging technologies? What emerging technologies are they adopting? How do they plan to secure and mitigate the associated cyber risks? What cybersecurity capabilities will be needed to successfully adopt and secure new technologies?

Of the emerging technologies included in the survey (see sidebar "Ten emerging technologies"), a majority of financial-services companies indicated that they are prioritizing adoption of and investment in four of them: cloud and edge computing, applied AI, next-gen software development, and digital identity and trust architecture (Exhibit 1). All four technologies are likely to see quicker adoption than advanced connectivity, future mobility, immersive reality, quantum, machine learning, and Web3. This is perhaps because of their widespread applicability and maturity, as well as their proven, value-based use cases for financial-services companies.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Exhibit 1

Among technology trends, cloud and edge computing are applicable to most financial-services organizations, followed by applied AI.



[1]Question: Which technology trends are applicable (ie, have already been considered or discussed) to your organization?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

While these technologies can provide exponential benefits, they can also bring cyber risks that companies must mitigate using their existing cybersecurity capabilities. The research shows that current capabilities are falling short of addressing these risks. Most survey respondents also recognize the need to strengthen critical cybersecurity capabilities, including third-party or supply chain management and privileged access management (PAM). As companies continue to increase their reliance on newer technologies, they must ensure they have thought through and implemented the necessary risk management capabilities. Otherwise, they may find the risks outweigh the benefits.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

As the technology landscape in the financial-services industry continues to evolve rapidly over the next three to five years and as the associated risks mount, now is the time to future-proof the environment. Financial institutions can lay the foundations for action by asking themselves four questions about their pursuit of emerging technologies:

- Are we prioritizing the right technologies and cybersecurity capabilities? Are our technology priorities aligned with our security capabilities?
- Are we investing in the right technologies and cybersecurity capabilities?
- Do we have the right metrics and reporting? Can we, and do we, accurately and confidently measure against our risk appetite, provide transparency to regulators and executives, and identify strengths and weaknesses?
- Do we have the right talent to close capability gaps? Do we have sufficient and appropriate talent not just to maintain existing capabilities now but to support future maturity and technology expansions?

Financial Institutions Have Emerging Technologies In Their Sights

With an increasingly crowded and fast-moving technology landscape, companies are facing pressure to keep up.

Financial institutions must not only grapple with how to best employ and protect their current technologies but also pay more and more attention to the growing field of emerging technologies that promise to strengthen their businesses—offering benefits such as increased automation, scalability, and cost savings.

To better understand how institutions are approaching and prioritizing new technologies, we surveyed companies around the world about the applicability of ten emerging technologies to their businesses.

The survey results reveal that financial-services companies are not exploring all the emerging technologies equally. Instead, they are concentrating on those they perceive as most applicable to their organizations and likely to bring the most value, all while factoring in their current technological capabilities, their long-term business and tech strategies, and the potential regulatory impacts.

In recent years, financial-services companies have evolved into technology-driven companies. This tech-centric approach is visible in the ways they are prioritizing their investments; in addition to embracing software technologies, they are prioritizing investments in scaling technology development, such as DevOps (software development and IT operations), and industrializing machine learning and AI.

Institutions are also weighing the current level of maturity of each technology in their plans, considering the proven (and unproven) use cases that could add value to their businesses. The most applicable technologies were further along in their maturity journeys than some of those that were deemed less relevant.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Cloud and edge computing lead the list, with 84 percent of respondents recognizing their relevance to their businesses. Among those respondents, six in ten reported that more than 25 percent of their workload now resides in the cloud. This share will undoubtedly rise as cloud capabilities continue to evolve and as companies continue to transform their IT infrastructure through cloud migration and investment into cloud-native infrastructure—enticed by benefits such as flexibility, scalability, and cost efficiencies that are otherwise not offered by traditional, on-premise data centers.

Maturity and proven use cases undoubtedly help propel widespread adoption, and indeed survey respondents confirmed that cloud computing is already the most mature emerging technology used across financial-services companies. Over 70 percent of companies see their cloud adoption in the post-pilot stage, and 42 percent consider their capabilities fully adopted and in the maintenance stage.

Applied AI gets nearly as much attention, with almost 80 percent of respondents calling it relevant to their businesses. AI and machine learning have a long history in financial services. Corporate and investment banks, as well as insurers, were early adopters of AI and machine learning, decades before other financial institutions. The rest of the financial-services industry has caught up in recent years, and adoption has only continued to grow.

This aligns with broader technology trends in financial services, as applied AI technologies continue to evolve and offer the potential for increasing value to companies. The next stage of AI—generative AI—promises unprecedented disruption of the industry (see sidebar "The promises—and risks—of generative AI").

Unlike with cloud adoption, however, the maturity level of applied AI is still evolving. While many financial-services companies recognize the relevance of applied AI, most of their use cases remain in the early stages of development. Seventy percent of the survey respondents reported being in the pilot stage or earlier. Some use cases such as financial-crime, financial-risk, and asset modeling are quite mature. Those that are in the early stages include gen AI and large language models. Many institutions are still exploring their use in customer interaction support, personalized marketing, and fraud. These efforts offer companies the opportunity to gain a competitive advantage in the applied AI space before the technology is ready to be deployed. They can implement, for instance, proper oversight and responsible guardrails and controls for AI technology, thereby hastening its adoption for when it has sufficiently matured.

Almost 75 percent recognize the applicability of next-gen software development to their businesses, enticed by the ability to transform their software development life cycle and simplify previously complicated custom development tasks. AI-enabled development and testing, low-code and no-code tools, and other advances can improve processes and software quality in each stage of the development life cycle.

Next-gen software development is largely in the pilot stage across many companies. They stand to transform their software development life cycle, reaping the rewards of simplifying complicated tasks in custom application development. While only 11 percent of the survey respondents have fully adopted this technology, more than 50 percent are in the pilot or post-pilot expansion stage, indicating they have had time to consider the benefits and use cases of the technology.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Trust architecture and digital identity are also advanced across many companies. Almost 50 percent of the survey respondents put themselves in the post-pilot or maintenance stage of digital identity, and 70 percent call trust architecture applicable to their businesses, with use cases regarding digital banking, omnichannel customer experience, a 360-degree view of customers, and digital-wallet offerings. These efforts have demonstrated such benefits as faster innovation, stronger asset protection, and better customer experience, further persuading institutions to invest in underlying technologies, including zero-trust architecture, digital-identity systems, and privacy engineering.

Digital-trust efforts will most certainly increase as identity-related breaches, especially cyberattacks on identity systems, continue to grow. Eighty-four percent of companies participating in a 2022 Identity Defined Security Alliance survey reported suffering an identity-related breach during that year. As organizations continue expanding their digital footprints, they must securely build and closely monitor their identity-related capabilities.

At the other end of the spectrum, less than one-third of the survey respondents are considering the following emerging technologies that stand to benefit financial-services companies applicable to their companies today: quantum, future of mobility, and immersive reality. Many institutions may not see adoption of these technologies happening soon and therefore are not prioritizing them today, because of the longer runway for adoption. It could well be that advances in quantum computing over the next few years may result in quantum quickly rising to a top concern, given its potential for materially affecting areas like password breaches and encryption breaking.

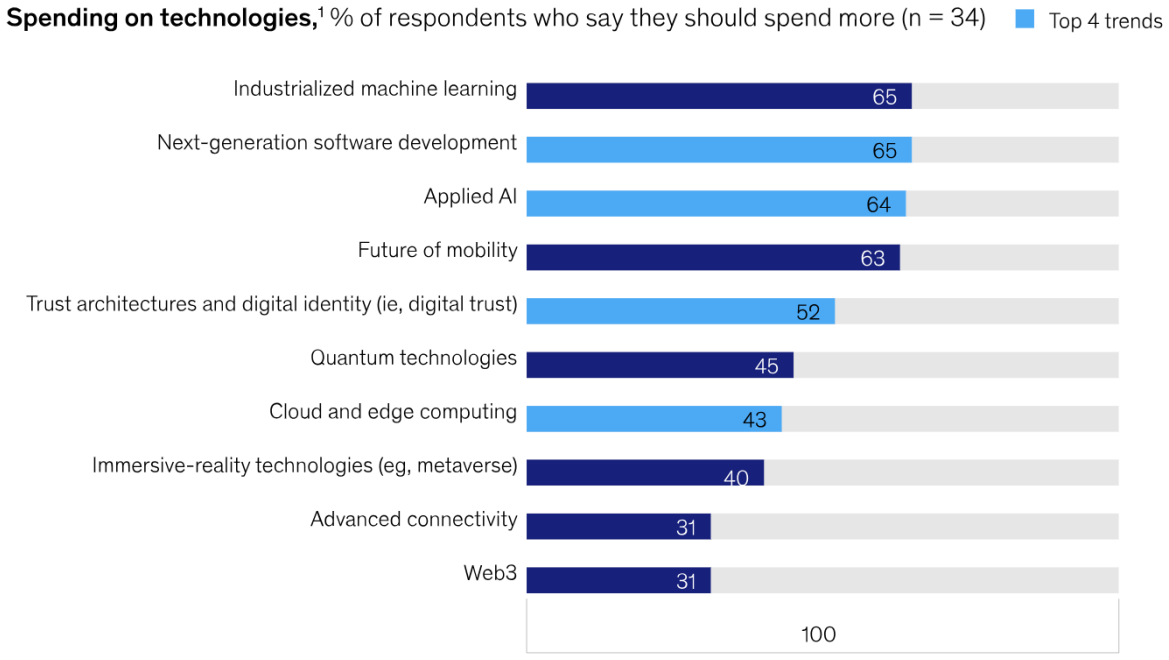
While this perspective is appropriate when considering the current maturity of these technologies, especially compared with more advanced and widely adopted technologies such as cloud and edge computing, financial-services companies should not be so quick to dismiss them. Quantum computing, for example, is estimated to bring over $600 billion in value to finance, with potential benefits such as real-time automated decision making and support activities such as holistic stimulations of liquidity or risk stimulations as part of large-scale, high-margin deals.

Adoption and maturity of these technologies, and undoubtedly others, is only expected to expand, as companies believe they should be spending more on those perceived as most applicable to their organizations. Many noted that they do not believe they are spending enough on applicable technologies. More than half of the survey respondents recognize the need to spend more to continue building their capabilities in industrializing machine learning, next-gen software development, applied AI, future mobility, and trust architecture and digital identity (Exhibit 2). This spending imperative will only accelerate as the technologies ripe for investment continue to mature and proliferate.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Exhibit 2

Financial-services organizations are spending the most on cloud and edge computing technologies.



[1]Question: What percentage of the IT budget does your organization currently spend on tech trends?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

Emerging Technologies Amplify Existing Risks And Add New Ones

Emerging technologies can offer significant benefits, but they can also exacerbate existing risks and introduce new cyber risks.

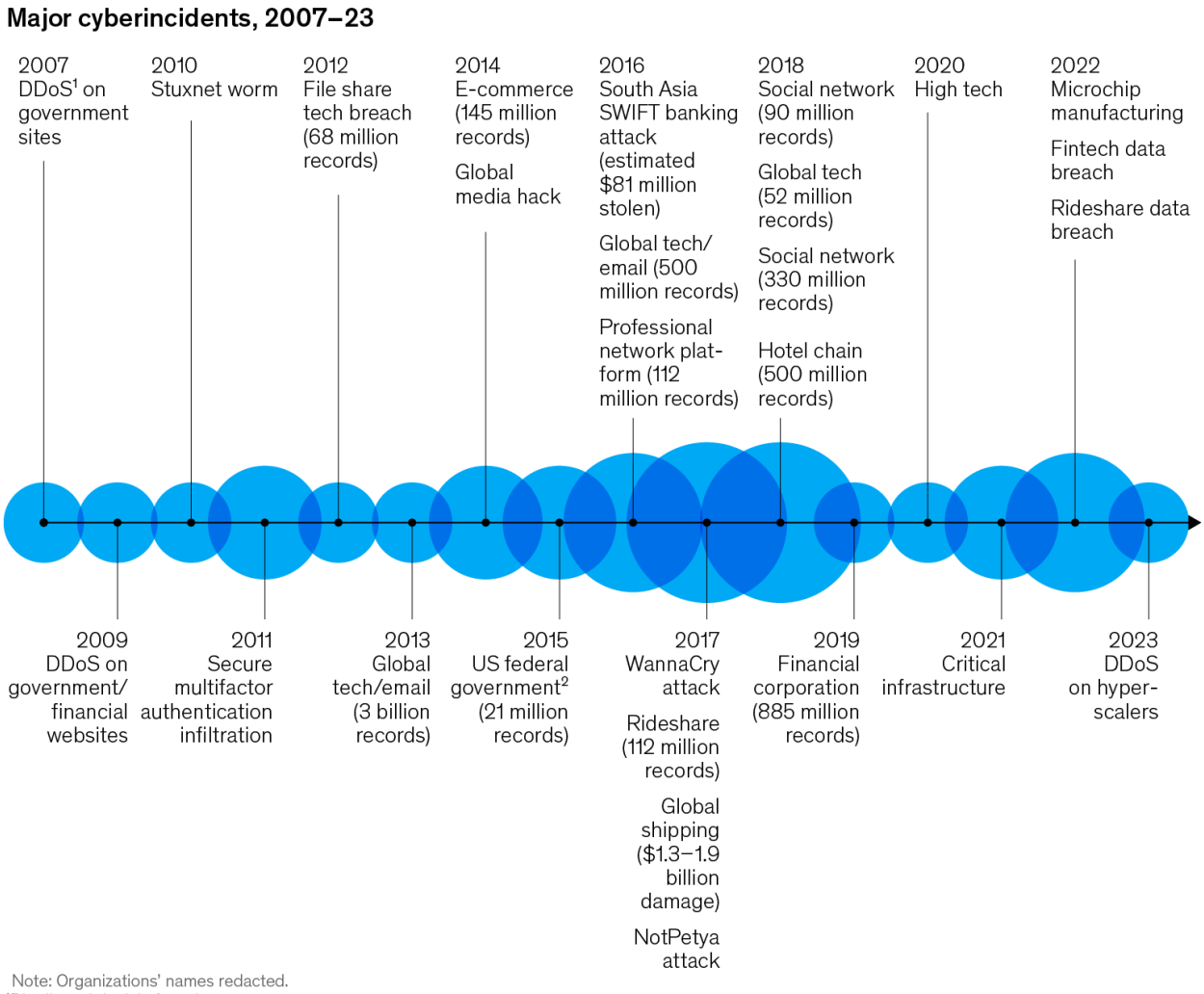
Cyber risk management is nothing new to financial-services companies, but the importance of a robust, comprehensive strategy has never been more critical and will only increase as institutions expand their technological footprint. Cyberattacks continue to increase, and financial-services companies face well-funded, highly organized, and well-trained cyber criminals. These criminals are also adopting emerging technologies to aid in their attacks, including recent attacks utilizing gen AI as part of sophisticated phishing campaigns.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Cyber incidents are increasing in both frequency and severity year over year, and institutions must stay vigilant in their capabilities to defend themselves and protect their assets and finances against electronic crime (Exhibit 3). According to the 2024 CrowdStrike global threat report, Electronic Crime (eCrime) continues to rise and led as the most pervasive threat in 2023. Data-theft extortion also continues to rise, and 2023 saw a 76 percent increase in victims named on eCrime dedicated leak sites compared with 2022. As companies increase their use of technology, they are also increasing the number of avenues for a potential cyberattack by mature threat actors.

Exhibit 3

As financial-services organizations continue to transform and modernize, the frequency and severity of cyberattacks are increasing.



Note: Organizations' names redacted.
[1]Distributed denial of service.
[2]Sensitive personnel data stolen from US government employees who underwent security clearance background checks.
Source: Munich Re; McKinsey Global Institute analysis on the Future of Work after COVID-19

McKinsey & Company

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

We further surveyed financial institutions to better understand what cyber risks were top of mind. The biggest risks they reported that their organizations face include cyberattacks, AI, talent management, third-party and supply chain management, and data security (Exhibit 4). While this proves that companies are aware and considering the risks they face, it also raises a couple of questions: Do they have the right capabilities to mitigate risks? Are they considering the potential for increased risks as they expand their adoption of new technologies? While they overwhelmingly recognize that they are under attack and that emerging technologies introduce risk, they still lack the appropriately skilled talent to address these risks.

Exhibit 4

Cyberattacks, AI misuse, and talent management are key risks for financial-services organizations.

Top three cyber risks in next 3–5 years,[1] % of respondents (n = 37)

32 *of 37 respondents highlighted* ***cyber attacks*** *(eg, ransomware, fraud, social engineering, phishing, advanced persistent threat) as a top risk priority for their organizations. Attacks that exploit third parties and supply chains were singled out due to the difficulty in maintaining governance and visibility.*

22 *of 37 respondents highlighted* ***emerging technology and their potential misuse*** *(eg, AI risk, digital trust, cloud) as a key concern.*

7 *of 37 respondents highlighted* ***cyber talent management*** *as a concern, particularly with regard to upskilling, retention, hiring, and churn rate.*

[1]Question: What do you see as the top three cyber risks your organization will face over the next 3–5 years?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

As companies expand their technology adoption, cyber risks are likely to grow. Specifically, each of the four technologies that received the greatest attention from survey respondents introduces its own risks.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Take cloud migration, for example. As financial institutions move their workloads to the cloud and as network boundaries disappear, there's an increased risk of exposure to threat actors and of nation-states gaining access to networks. Without proper management anchored in a robust cloud security strategy and strong security capabilities, companies face a multitude of cyber risks, including misconfigurations, data privacy breaches, and data loss. Strong access controls, vulnerability management programs, data protection, and third-party management capabilities are critical to mitigating these risks; otherwise, organizations may find themselves susceptible to risks such as data loss through weak internal connections and service disruptions because of a heavy reliance on third-party exposure.

Applied AI and gen AI usage introduces significant regulatory risks for companies. Regulators are increasingly eyeing the risks associated with AI and are developing requirements, such as those set forth in the EU AI Act, that are likely to see enforcement in the coming years. Financial-services companies should build their security capabilities—including reporting, governance, and data privacy—in line with emerging regulations before they take force.

Next-gen software development and trust architecture can also subject companies to risks if they are not securely developed and implemented. Both technologies can provide increased efficiencies and increase security within an organization's technology environment, but with them comes the risk of failure in involving the right skills in development and implementation or of failure to integrate the technologies fully and securely into the environment.

Consider the implementation of zero-trust architecture. Security misconfiguration and integration issues associated with legacy tools may increase the risks of data loss, reputational harm, and insider threats.

Financial-services companies must rely upon their foundational cybersecurity capabilities to secure their technologies and protect their environments. Cybersecurity capabilities should be prioritized within the business as institutions continue to undergo technology transformations and recognize the benefits they bring with them. Without strong foundational security capabilities and controls within their cybersecurity programs, organizations will be exposed to risks brought on by their technology investments.

"DIGITAL TRANSFORMATION IS AT THE HEART OF OUR STRATEGY. WE RECOGNIZE THE IMPORTANCE OF ADOPTING AND INVESTING IN EMERGING TECHNOLOGIES, SUCH AS CLOUD AND AI. AT THE SAME TIME, MANAGING THE ASSOCIATED CYBER AND TECHNOLOGY RISKS IS OF UTMOST IMPORTANCE TO ENSURE OVERALL RESILIENCE OF OUR VITAL SERVICES. THIS HELPS ENHANCE THE DIGITAL TRUST OF OUR CUSTOMERS WHILE PROTECTING THE SAFETY AND SOUNDNESS OF THE BANK."

—JAY PUTHANVEEDU; GLOBAL HEAD OF RESILIENCE, CYBER AND DIGITAL FRAUD; BNP PARIBAS

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

With this risk in mind, it is critical that organizations understand not only the benefits that new technologies may bring but also the accompanying risks. For institutions to truly harness their benefits, they must first coordinate their current capabilities by strategically investing in and maturing those that support the new technologies. While financial companies undoubtedly recognize the importance of cyber risks and the actions they should take to manage them, the question is, are they fully aware of the added risks these new technologies bring?

Companies Need Strong Foundational Cybersecurity Capabilities To Counter Cyber Risks

Financial institutions feel pressure to keep pace with other organizations and worry they are not investing the right level of resources in the adoption of new technologies.

Fifty-seven percent of surveyed respondents admitted they were concerned with keeping pace with emerging technologies, specifically with respect to their cybersecurity expenditures.

While they recognize the importance of having strong cybersecurity capabilities to mitigate cyber risks, 31 percent of companies are not confident that their capabilities can do so. To understand how companies are prioritizing and managing risks, we asked them to select their top strengths and weaknesses in their security capabilities across eight domains and numerous subdomains (Exhibit 5).

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Exhibit 5

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

The weakest capabilities they identified require immediate attention, as many of them are essential to successfully developing and deploying the five technologies of greatest interest to the survey respondents (Exhibit 6):

- *Third-party and supply chain management.* By far the greatest capability weakness—topping the list for 65 percent of survey respondents—third-party management is critical as companies continue to expand emerging-technology use in cloud computing and applied AI, which rely heavily on third-party services for such critical components as computing, data usage, model bias, model usage, and security.

- As financial-services companies rely more and more on third-party services, they must enhance their own security capabilities to avoid exceeding their risk appetites and making their environments vulnerable to risks.

- *Metrics and reporting.* Despite compliance being an important factor for investment into cybersecurity, a significant portion of the survey respondents (41 percent) called their metrics and reporting capabilities a core weakness. Companies need reliable, insightful metrics and reporting (such as security compliance, risk metrics, and vulnerability tracking) to prove to regulators the health of their security capabilities and to manage those capabilities. New regulations such as the US SEC Cyber Disclosure Rule4 and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and similar regulations around the world have underscored the importance of better reporting, transparency, and governance of cybersecurity risk.5 Additionally, with an increased focus around the world on regulatory compliance, operational resilience, as well as third-party risk management, more and more financial institutions are being challenged to prove the resilience of their vendors and their reliability in times of extreme stress. It is therefore more critical than ever that companies can measure their risks properly.

- Without a robust process for measuring, reporting, and governing the risks associated with capabilities, organizations are flying blind, not knowing how much risk emerging technologies will pose. Companies, for example, will need evolved controls to measure model bias and risk, average time spent responding to incidents in the cloud environment, and the severity of vulnerabilities. These controls enable companies to identify their strengths and weaknesses and address those gaps before an issue materializes.

- *Identity and access management (IAM) capabilities.* The survey respondents passed similar judgment on their IAM capabilities, specifically the higher-risk PAM capability. Despite investment in digital identity and an increased technology domain to protect, companies are still struggling to protect accounts with high-risk access. Without proper PAM, emerging-tech capabilities remain vulnerable to backdoor compromise by threat actors. In addition, as financial institutions increasingly depend on automated software development (like the next-gen software development that 74 percent of respondents are funding), they need to implement safe IAM and PAM practices.

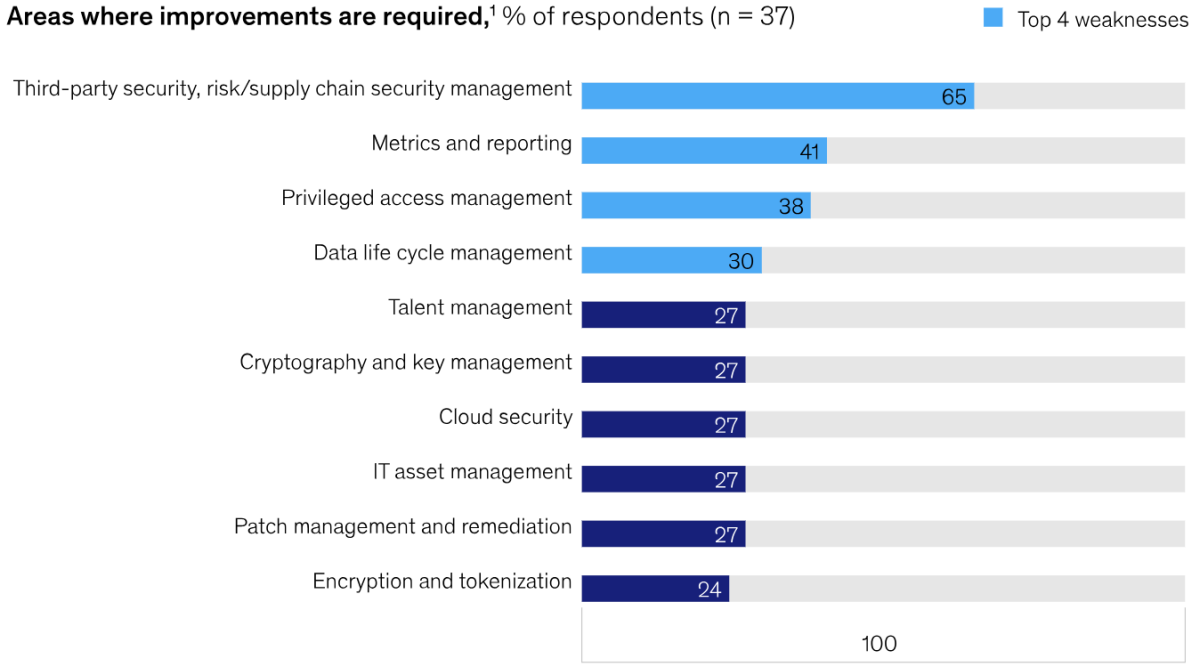
200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

- *The cloud.* The cloud expands the digital environment and overall attack vector that companies must secure. While they embrace digital trust, organizations struggle to manage digital identities. The automated deployment and easily scalable infrastructure in the cloud can increase the risk of data exposure. Unfortunately, developers often use domain administrator or master privileged accounts and default credentials in the cloud environment. Without proper PAM, they are practically inviting bad actors to grab the keys to the kingdom.

- *Data life cycle management.* While many financial-services companies are using next-gen software development and applied AI to pursue efficiencies and automation opportunities, they often fall short on the major foundational capability of data life cycle management, as 30 percent of the survey respondents admitted. Without secure, reliable data management in following best practices from creation to destruction, companies will have difficulty optimizing the benefits of technologies that require reliable data sources.

Exhibit 6

Financial-services organizations are often strong in overarching security governance and strategy but feel they could improve technical capabilities.



[1]Question: My organization needs improvements in which areas (select up to 10 capabilities).
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Think about applied AI. Securing the model training data to prevent tampering and the introduction of bias is essential. As AI models are applied to data sets and as data passes through the models, understanding the full life cycle of data security from discovery to classification, monitoring, compliance, and protection is equally essential. The top technologies in which institutions are investing also have the highest correlation with weaker capabilities. There is also a disconnect between the top-of-mind risks reported and the capability weaknesses companies are facing. These disconnects pose huge risks for organizations, especially as they continue to rapidly invest, pilot, and deploy these technologies in their environments. Organizations should strengthen these capabilities now to protect themselves in the future against the growing level of risk associated with these technologies.

How Are Companies Prioritizing And Investing In Cybersecurity?

Financial-services organizations' cybersecurity capabilities are struggling to keep up with the rapid pace of adoption.

To better understand how companies are approaching cybersecurity, we asked three important questions: What is causing organizations to mature their cybersecurity capabilities? How are they prioritizing spending on cybersecurity? Do they have the right talent to address their capabilities and gaps? (See sidebar "Cloud and edge computing—investments planned in tech but not security.")

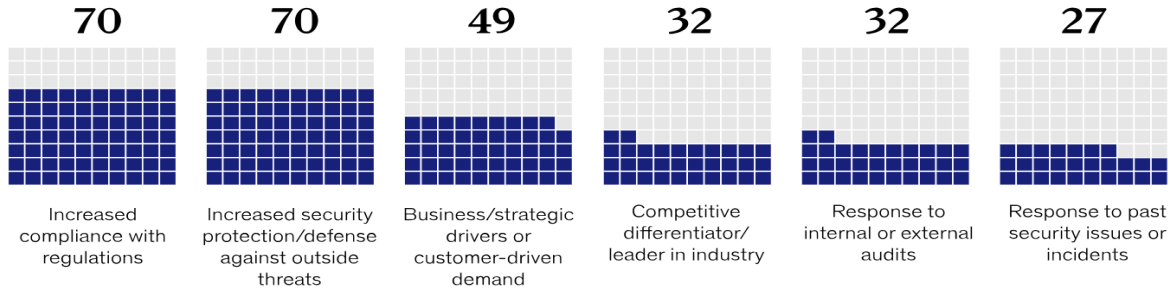
Compliance Advances Cybersecurity Maturity

As to what causes financial institutions to mature their cybersecurity capabilities, our survey found that there were two common factors across financial-services organizations: increased compliance with regulations and increased defense against outside threats. Seventy percent of companies said that increased compliance with regulations causes their organizations to mature their cybersecurity capabilities (Exhibit 7).

Exhibit 7

Financial-services organizations value compliance and security against threats as top drivers for cybersecurity capabilities.

Factors driving organizations in maturing cybersecurity,[1] % of respondents (n = 37)



[1]Question: What are the primary factors driving your organization in maturing its cybersecurity capabilities?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

The desire for increased protection against security breaches comes as no surprise; it is the secondary top factor for maturity. Similarly, given increasing regulation of financial services, it is understandable that increased compliance with regulations would drive capability maturity, likely in areas with known gaps.

"A KEY TO ENHANCED SECURITY FOR EMERGING AND CRITICAL TECHNOLOGIES IS TO DEVELOP STANDARDS ON HOW CURRENT CYBERSECURITY AND INFORMATION SECURITY MEASURES ARE INTEGRATED INTO THE USE OF THESE TECHNOLOGIES. TIGHTER INTEGRATION BETWEEN THESE STANDARDS AND CURRENT CYBER FRAMEWORKS, SUCH AS ISO AND THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S CSF, WILL CREATE UNIFORMITY IN HOW THESE TECHNOLOGIES ARE IMPLEMENTED BETWEEN FINANCIAL INSTITUTIONS AND THE AGREED SECURITY MEASURES FOR THESE TECHNOLOGY USAGES."

—JASON HARRELL; HEAD OF EXTERNAL ENGAGEMENTS, OPERATIONAL AND TECHNOLOGY RISK, DEPOSITORY TRUST AND CLEARING CORPORATION

Companies should approach compliance as the minimum baseline of expectations rather than the aspirational goal. Likewise, regulatory compliance should be baked in proactively rather than a reaction or an afterthought, especially as rule makers delve into emerging technologies. For many technologies, regulations are still under development (most notably in the AI space). As regulations catch up with the level of adoption across organizations, companies need to be prepared to comply. By using compliance as an essential aspect of adoption, organizations can future-proof their technologies by getting ahead of emerging regulations before their implementation.

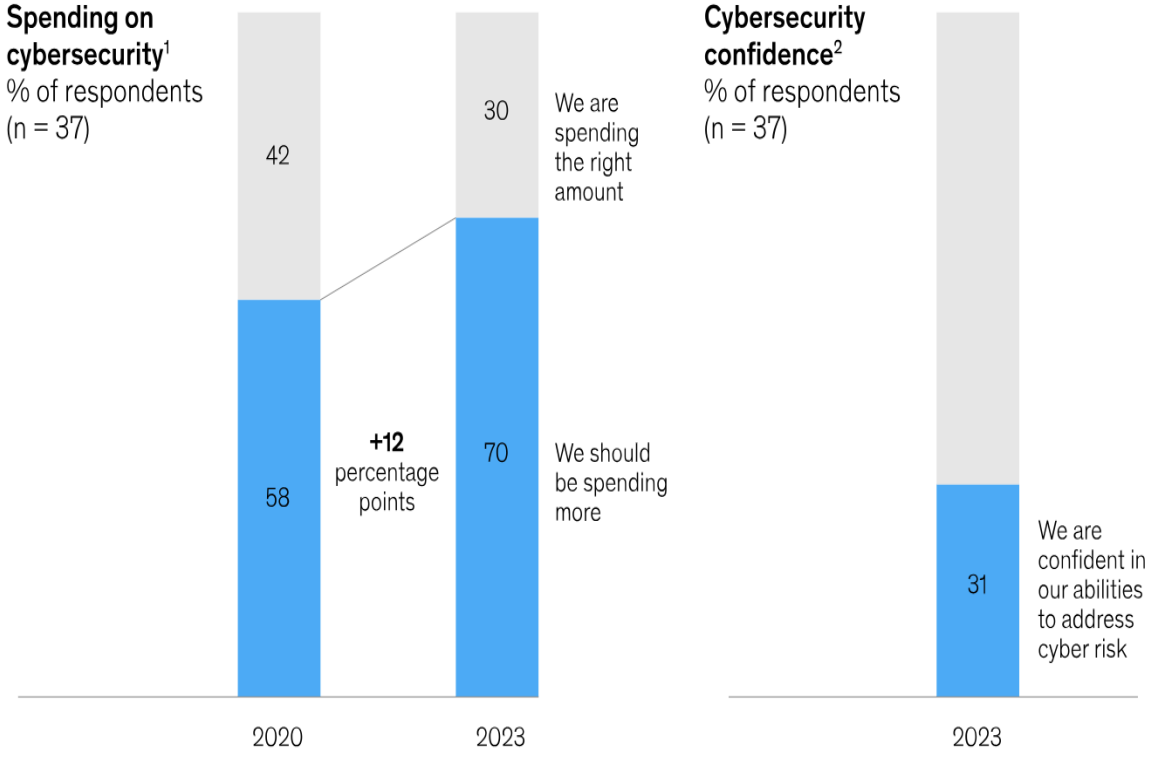
Spending Habits: Companies Recognize Critical Underinvestment In Cybersecurity

Acknowledgment of underspending in capabilities has grown in the last three years. Seventy percent of the survey respondents believe they are underspending and should spend more. Not one organization reported overspending. This marks a shift from prior surveys: in the 2020 IIF and McKinsey Cyber Resilience Survey, only 58 percent of respondents acknowledged underspending. In 2023, a majority of companies said that they should increase cybersecurity spending more than 20 percent to build the requisite capabilities (Exhibit 8).

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Exhibit 8

The lack of investment in capabilities has grown in the last three years as financial firms continue to acknowledge underspending in cybersecurity.



[1]Question: I believe we should be spending (more/less/the same) on our cybersecurity program.
[2]Question: Do you currently feel you have the appropriate level of full-time cybersecurity employees?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

Today, financial-services companies devote 13 percent of their overall IT budget, on average, to cybersecurity. As they continue investing heavily in technologies, they should consider the short- and long-term implications of these technologies for cybersecurity to maintain protection of their environments.

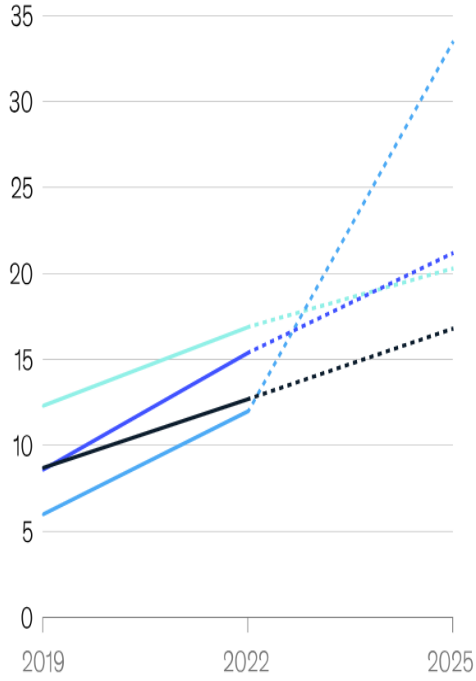
200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Fortunately, cybersecurity spend is expected to increase over the next two to three years, with regional banks (Tier 2) expected to see the largest growth. Tier 2 banks' anticipated cybersecurity spend likely comes as they near the Tier 1 capital threshold and anticipate increased scrutiny from regulators (Exhibit 9).

Exhibit 9

In the US, Tier 2 regional banks are increasing their spend on cybersecurity relative to IT.

Planned cybersecurity spend as a share of IT budget, by type of bank,[1] % (n = 26)



		Assets under management	Number in 2022
Mega	Tier 0	>$1 trillion	4
	Tier 1	>$0.1 trillion–$1.0 trillion	30
Super regional	Tier 2	>$50 billion–$100 billion	16
Regional	Tier 3	>$5 billion–$50 billion	223
Midcap and credit unions	Tier 4	>$1 billion–$5 billion	707
	Tier 5	>$0.5 billion–$1.0 billion	771
	Tier 6	≤$0.5 billion	2,952
	Credit unions	–	4,866

[1]Banks assigned to capital tiers using self-reported revenue ranges, based on an assumed profit margin of ~15% and presumed return on assets of 1.18%.
Source: SNL Financial; McKinsey Cyber Market Map

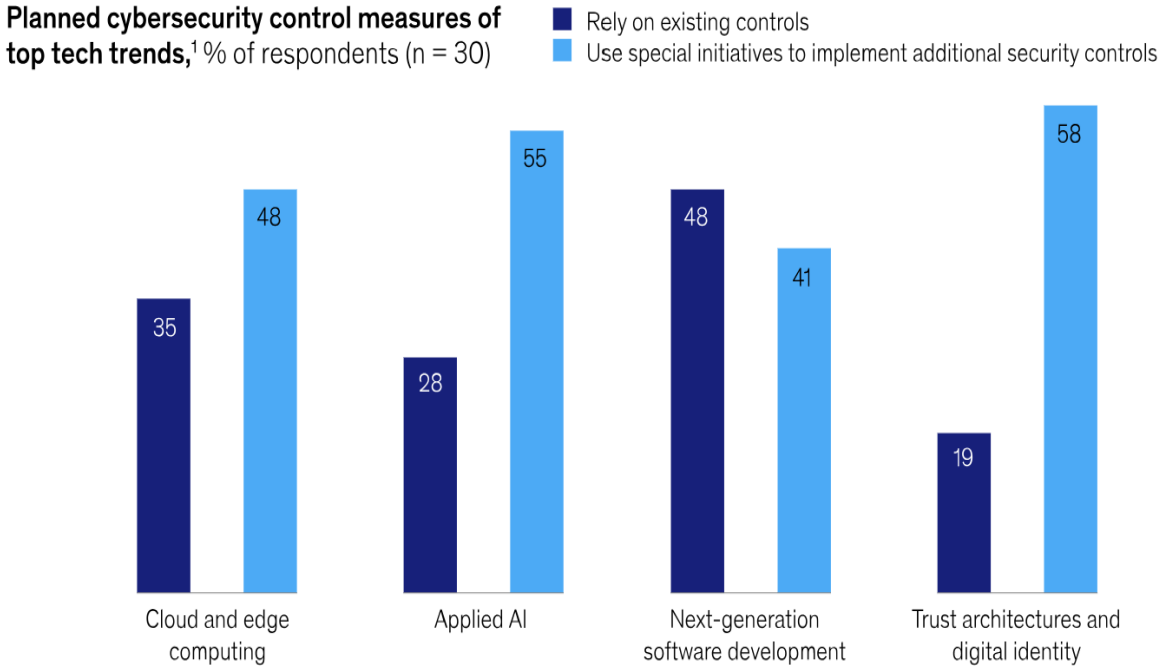
A portion of the expected increased funding is likely to go toward special initiatives to address growing cyber risk. Many companies also acknowledge that they are not currently prepared to mitigate risks associated with emerging technologies and that they must implement special initiatives and controls to secure their environments. But with the ever-increasing need for additional funding, special initiatives will only add to existing budget strains.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

More than 40 percent of the survey respondents have launched special initiatives to address the security control gaps related to the adoption of emerging technologies (Exhibit 10). Fewer than 10 percent lack plans to invest in protecting the top four technologies.

Exhibit 10

More than 40 percent of respondents are utilizing special initiatives to secure each of the top four tech trends.



[1]Question: Describe the cybersecurity control measures you are planning on implementing to secure the top tech trends.
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

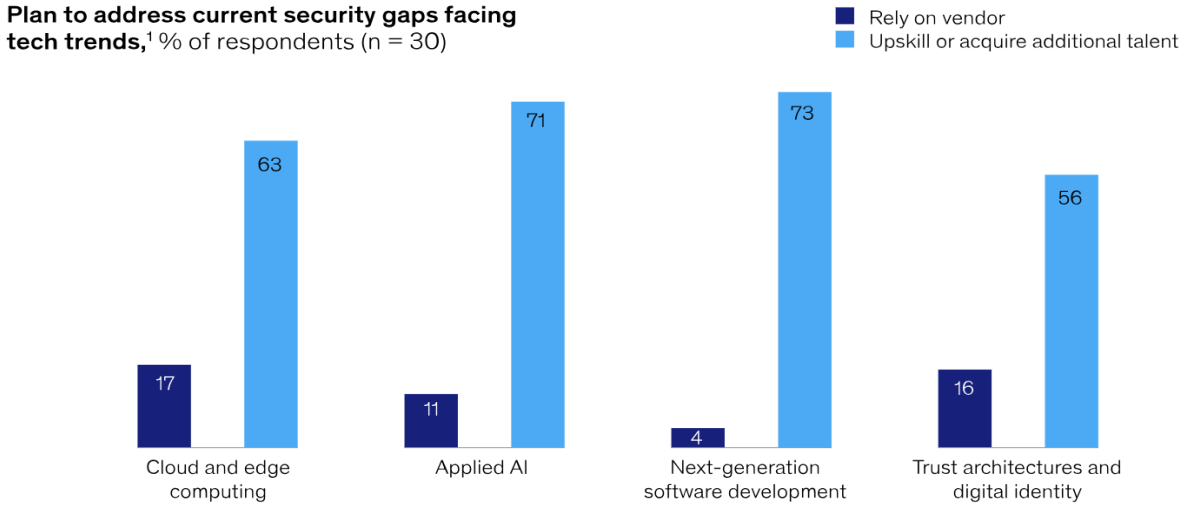
200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Companies Rely On Talent To Address Capability Gaps

Efforts to close security capability gaps typically revolve around recruiting new talent and upskilling existing talent. All respondents reported relying on existing talent, as well as new talent, to secure their technologies. However, 65 percent noted concerns about gaining and retaining appropriately skilled cybersecurity talent. While companies can outsource some cybersecurity work, more than half of the respondents plan to rely on internal resources to close the capability gaps related to their emerging technologies (Exhibit 11).

Exhibit 11

More than 50 percent of respondents are planning to address security gaps for each of the top four tech trends with internal resources.



[1]Question: How are you planning on addressing the current security gaps your organization is facing on the top tech trends?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

Financial-services companies may encounter obstacles in finding and retaining the right talent to handle their particular security risks, as talent attraction and retention is an ever-growing concern for cybersecurity more broadly. They should consider other options, including the use of technology to augment talent—making gen AI a copilot in security operations, for example.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Call To Action: Future-Proof The Environment

The technology landscape in the financial-services industry will evolve rapidly over the next three to five years, accompanied by mounting risks.

Technologies that are popular today may change tomorrow, and as use cases develop and mature, companies are likely to continually reassess their applicability and investment priorities. The time for action to future-proof the environment is now. Our survey found that even leading institutions are falling short and that smaller companies with significantly less budget or ability to attract top security talent face even greater challenges.

Financial institutions should lay the foundation for action by asking themselves the following four questions about their pursuit of emerging technologies:

- *Do we have the right technology priorities, and are they aligned with our security capabilities?* Expansion into newer technologies, such as the cloud and applied AI, usually means greater reliance on third-party services. Companies should reflect on their capabilities and the maturity of their security before introducing any technology. The third-party risk management capability warrants special attention.
- *Do we have the right metrics and reporting?* Whether to satisfy regulators or to hold teams accountable, financial-services companies need transparent, value-based metrics for managing cyber risks. They can aid in monitoring performance, informing decisions, and identifying emerging issues for quick action. These metrics should measure cyber risk from an emerging-technology perspective and be reported appropriately to the right stakeholders, including board members and executives, lines of defense, and the risk management team.
- *Are we investing in the right things?* Decisions on technology investments should take security capabilities, especially IAM capabilities, into account. The growing risk of security breaches and the looming need for regulatory compliance shine a spotlight on these capabilities.
- *Do we have the right talent and technology to close capability gaps?* Every organization needs to invest in talent, but hiring and retaining the right talent is a challenge and calls for exploring other ways to fill the talent gap, such as utilizing emerging technologies themselves, including AI.

Emerging technologies are grabbing lots of attention in the financial-services industry. Each brings cyber opportunities and risks. Most companies will have to build their cybersecurity capabilities to handle the risks. Today is the time to future-proof the environment, ensuring success for tomorrow.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

'Growing Appetite' To Tackle Insurance Fraud, But Challenges Are Evolving

Why insurance organizations should "think global, not local"

By Gia Snape, Insurance Business, March 06, 2024

https://www.insurancebusinessmag.com/us/news/claims/growing-appetite-to-tackle-insurance-fraud-but-challenges-are-evolving-480016.aspx

There is a growing appetite among insurers to tackle claims fraud more comprehensively. At the same time, fraudsters are ramping up their strategies and targeting markets beyond the US and UK, posing huge risks to insurers operating globally.

That's according to Steve Crystal (pictured), head of claims fraud and investigation services, international at Sedgwick, who spoke to insurance leaders and anti-fraud professionals at last week's Insurance Innovators Fraud & Claims summit in London.

"The rest of the world has noticeably been waking up to the risk posed by insurance fraud over the last five years," Crystal said.

"There is definitely a growing appetite to tackle insurance fraud, not just by those insurers that operate internationally, but also by those insurers who operate only in the local markets."

Claims Fraud Evolving As Criminals Find New Targets

According to the Coalition Against Insurance Fraud (CAIF), insurers make around $308 billion in fraud claims payments annually in the US alone, making the country one of the biggest markets for fraudsters.

But Crystal noted that other fraud hotspots are emerging worldwide, such as South Africa and France.

Additionally, organized crime groups are targeting product lines beyond auto insurance. The emergence of embedded insurance has also given fraudsters a new avenue to target insurers.

Finally, Crystal named the rise of generative artificial intelligence (AI) as a potent threat. A notable case of claims fraud last year, for instance, stemmed from convincing fake boarding passes from a series of organized lost luggage claims between the US and the Dominican Republic costing around £1,500 ($1,900) each.

AI tools have made fraud easier and more accessible than ever, necessitating collective action from the industry, Crystal warned.

"I have seen some really good fake documents, photos and videos all around the world, incredible hologram foil strips on documents in real life," said Crystal.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

"But there is an opportunity to fight back against these challenges through global education, cooperation and disruption."

"Think Global, Act Local" – A Strategy For Tackling Insurance Fraud

Addressing insurance industry stakeholders, Crystal shared his strategy for helping new markets tackle fraud as insurers seek to protect their reputations, retain genuine customers, and plug revenue leaks.

"It's advisable to be flexible [and] deliver a strategy that fits globally," said Crystal.

He recommended a process centered on detection (spotting potentially fraudulent insurance claims from portfolios) and containment (triaging and investigating suspicious claims). Insurance organizations must be accountable at all steps.

Finally, Crystal stressed the importance of a "top-down culture" when it comes to eliminating claims fraud.

"It's got to be lived and breathed from the very top. Let's do the right thing," he said. "Do provide colleagues who are new to this area with in-country support when it's relevant to do so, especially around coaching.

"And in the market, build partnerships, make affiliations, and develop intelligence and explore technology."

Crystal underscored the importance of collaboration and information-sharing in the war against fraud, advocating for a united front against organized crime networks.

He also highlighted the role of technology in enhancing fraud detection and prevention efforts, urging insurers to leverage innovative solutions to stay ahead of fraudsters.

"There were different challenges [affecting anti-fraud efforts], including legislation, regulation, data protection, market approach, policy wordings, culture, and language," Crystal said.

"But my experience is that today, despite these challenges, there is a common denominator. Whatever your language, claims fraud is seen internationally as bad news, and I think that's good news for our industry.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

UPCOMING CAFII-RELEVANT WEBINARS & EVENTS; AND RELATED EDUCATION CONTENT

LIMRA and LOMA Canada Annual Conference

Time: Wednesday, May 1, 2024
Location: Manulife, Toronto, ON

The world is moving fast. Each industry is very different today than it was 10 years ago. The change 10 years from now will be even greater. Where will these changes take place in the life insurance industry and what are the critical success factors for winning companies? David Levenson, CEO and President, LIMRA and LOMA, will share our organization's research and best thinking to guide companies on how to expertly navigate what's ahead.

Register Here
Early bird rate (by April 1, 2024)
LIMRA/LOMA member: CD$725 + HST
Non-member: CD$950 + HST

Regular rate (after April 1, 2024)
LIMRA/LOMA member: CD$950 + HST
Non-member: CD$1,175 + HST

THIA's 2024 Annual Conference

Date: May 22-24, 2024
Location: Quebec City, Canada

THIA's conference is the highlight of the Canadian travel insurance year and for the first time we are hosting this special event on Canadian soil. We expect to welcome many returning attendees and, by holding our premier event in beautiful Quebec City, we hope to meet many first-time attendees as well.

As always, you won't want to miss:

- Engaging insights from industry experts
- Networking opportunities with peers and prospects from across the globe

A chance to participate in scheduled professional and leisure activities

Register Here - *'Early Bird' registration for THIA and UStiA members is $1,025 CAD until March 31, 2024.*