

FINANCIAL INDUSTRY FORUM ON ARTIFICIAL INTELLIGENCE II: **A COLLABORATIVE APPROACH TO AI THREATS, OPPORTUNITIES, AND BEST PRACTICES**

WORKSHOP 1- SECURITY AND CYBERSECURITY

JULY 2025



**GLOBAL
RISK**
INSTITUTE



Government
of Canada

Gouvernement
du Canada

“Today’s forum is a great step toward a better understanding of AI, its role in the financial industry, and how to think about security and cybersecurity risks. A better understanding can dispel unfounded fears and enable us to focus on real problems and to identify tailored solutions.”

Suzy McDonald, Associate Deputy Minister, Department of Finance Canada, May 2025

PREFACE

In recent years, the need to understand, integrate, and responsibly manage the use of Artificial Intelligence (AI) in the financial industry has become increasingly important. There is an urgent need for collaboration and development of best practices in this area.

To drive discussion and debate on this critical issue, in 2022, the Office of the Superintendent of Financial Institutions (OSFI) and the Global Risk Institute (GRI) hosted the first Financial Industry Forum on Artificial Intelligence (FIFAI I) to promote the responsible use of AI in Canada’s financial sector. This initiative brought together AI experts from the financial industry, as well as policymakers, regulators, academics, and research institutes.

The resulting report, “[A Canadian Perspective on Responsible AI](#),” highlighted the need for financial institutions to adopt comprehensive risk management strategies to address the unique challenges posed by AI. It identified the four EDGE principles as critical for AI’s responsible use: Explainability, Data, Governance, and Ethics.

The rapid evolution of AI tools and heightened risk awareness highlight the need to expand this dialogue with the Financial Industry Forum on Artificial Intelligence II: A Collaborative Approach to AI Threats, Opportunities, and Best Practices. Four workshopsⁱ will focus on urgent AI-related challenges facing Canada’s financial industry: security and cybersecurity, financial crime, consumer protection, and financial stability. Each workshop will result in an interim report, like this one, along with a final report that will highlight key themes, insights, best practices, and recommendations across all the topic areas.

ⁱ The workshops are organized by OSFI, the Department of Finance Canada, the Financial Consumer Agency of Canada (FCAC), the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and GRI.

The first workshop, held on May 28, 2025, was sponsored by OSFI, Department of Finance Canada, and GRI. It brought together 56 Canadian and global AI experts from across the industry including banks, credit unions, insurers, asset managers, academia, and technology providers, as well as federal and provincial policymakers, regulators, and supervisors.

They met with two objectives:

- deepen our understanding of how AI technologies are reshaping security and cybersecurity threats and opportunities, and
- discuss best practices and effective AI risk management strategies and learn how to build resilience into organizations and security frameworks.

Here, “security” refers to financial institutions protecting against internal and external threats to their physical assets, infrastructure, personnel, technology, and data. Security extends beyond the soundness of individual institutions, carrying national security implications. The growing capabilities of AI amplify the scope, scale, and speed of existing security risks, particularly in cybersecurity, which is already one of the most significant risks facing Canada’s financial system. Addressing these risks requires a vigilant and proactive approach from all stakeholders.

AI presents both opportunities and risks for the financial system, and the sponsors, in this case, OSFI, Department of Finance Canada and GRI, would like to express their sincere gratitude to all workshop participants for their support of this collaborative dialogue.

Global Risk Institute

Office of the Superintendent
of Financial Institutions

Department of
Finance Canada

AI SECURITY AND CYBERSECURITY
- PERSPECTIVES ON THREATS, RISK,
AND MITIGATION

“Estimates of direct and indirect costs of cyber incidents range from 1 to 10 percent of global GDP. Deepfake attacks have seen a twentyfold increase over the last three years.”

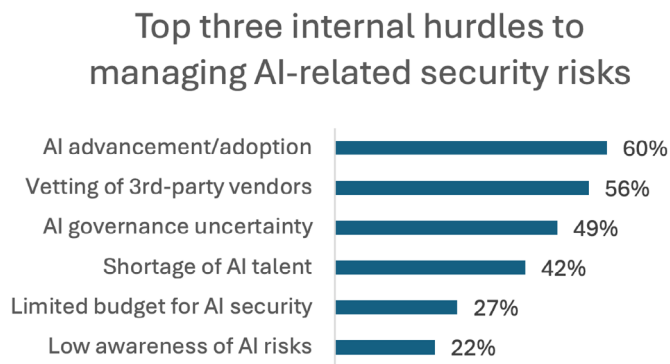
Michael Barr, Board of Governors,
Federal Reserve, April 2025

AI is a double-edged sword. The financial industry is adopting AI solutions that include opportunities to enhance customer service, improve fraud detection, and automate claims adjudication. Similar AI tools, however, also create and amplify risks, empowering threat actors to rapidly adopt AI to achieve effective and malicious outcomes.

Financial sector perspectives on AI adoption

When asked to identify the top three internal hurdles financial institutions face in managing AI-related security risks, 60% of workshop participants identified the speed at which AI advancement outpaces risk management adaptation as the most significant. This was closely followed by third-party vendor vetting.

Figure 1: Participant questionnaire, May 28, 2025



Financial sector AI experts stressed that AI-related risks must be fully integrated into the governance and risk management frameworks of institutions. Doing so, in many cases, may require updates given the scope and pace of AI developments, including the establishment of AI executive oversight. This includes reinforcing existing policies and controls. Participants emphasized that foundational technology hygiene is critically important and “sometimes simple, basic controls are a key part of managing these significant AI-related risks, like with third parties.”

Forum participants also stressed the importance of AI adoption to be use-case or business-case driven. Rather than seeing AI as the next “bright shiny object,” successful AI adoption should yield measurable shareholder or stakeholder results.

Workshop participants identified the following four financial sector AI-enabled threats, risks, and mitigations.

1. Social engineering and synthetic identity fraud

Nature of the risk

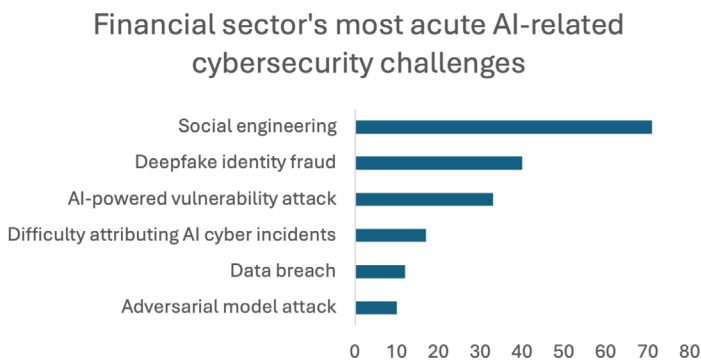
AI supercharges phishing and synthetic identity attacks through convincing, scalable, and adaptive social engineering, escalating risks to financial integrity and national security. Virtual onboarding enables threat actors to use deepfakes and other AI tools to place insiders within firms.

Modern AI can mimic an individual’s voice, with only seconds of audio, enabling deepfake schemes that can deceive employees into compromising actions. Social media content provides exploitable material to create

convincing, hyper-personalized phishing attempts that can be executed at scale and speed, increasing opportunities for success.

71% of workshop participants identified AI-enhanced social engineering as the financial sector’s most acute AI-related challenge. This was followed by 40% who highlighted deepfake identity fraud as a major concern.

Figure 2: Participant questionnaire, May 28, 2025



Today, firms must be more conscious of social engineering and identity fraud risks, which heighten the possibility of infiltration, including through the hiring process. One recent case highlighted this risk when AI-generated synthetic identities enabled North Korean operatives to secure remote jobs at North American firms. Once hired, they gained access to internal systems, exposing proprietary and customer data to potential exfiltration.ⁱ

Risk management implications

To counter AI-enhanced social engineering threats, institutions are strengthening identity verification and updating employee training.

Preventive efforts also include promoting a culture of vigilance and encouraging staff to question unexpected requests, especially those involving sensitive data or financial transactions. In parallel, some institutions are adopting AI-based monitoring tools to detect unusual communication patterns and identify real-time intrusions.

2. AI-assisted cyberattacks

Nature of the risk

Threat actors are weaponizing AI to automate, accelerate, and tailor cyberattacks. At the same time, the expanding use of AI by financial institutions increases the overall attack surface and susceptibility to exploitation.

Advances in AI have lowered barriers to entry for threat actors and introduced sophisticated tools that render traditional security measures less effective. AI-enhanced tools, such as adaptive malware, enable threat actors to move quickly and inflict significant damage on their targets. They may also allow threat actors to more quickly and accurately identify security vulnerabilities in financial institutions.

Internal AI models used by financial institutions often process sensitive data, and threats such as data poisoning, model extraction, and adversarial manipulation pose significant risks. Data breaches can result in the exposure of sensitive data, increased vulnerability to adversarial attacks, and loss of intellectual property, undermining operational integrity and eroding customer trust.

One workshop presenter noted that cyber risk attacks have evolved from the “possibility” phase, where a single threat actor could

ⁱ [Office of Public Affairs | Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions | United States Department of Justice](#)

launch a single malicious attack, to the “automation” phase, where one threat actor, using AI-assisted tools, can create millions of concurrent incidents.

Workshop participants also expressed concern that social media “disinformation” campaigns could amplify AI-assisted cyberattacks. Market disruption is seen as a real threat, especially where multi-faceted attacks target a single institution, groups of institutions, or other key components of Canada’s financial infrastructure.

It was also discussed that government agencies are also vulnerable to cyberattack risks, as they are custodians of significant amounts of proprietary and sensitive financial institution data. The integrity of data relies on the security and cybersecurity efforts of everyone in the ecosystem.

Risk management implications

To defend against increasingly sophisticated AI-driven cyber threats, participants suggested adopting a mix of proactive tactics to address these vulnerabilities.

1. Adopt AI-assisted security tools

- adopt existing security tools that detect anomalies and unusual activity in real time
- implement “zero trust” security standards to verify every request for data access

2. Establish AI model integrity standards

- adopt adversarial testing and training to build resilience
- establish query monitoring and use rate limiting tools to detect and block anomalous access patterns

3. Enhance employee training

- create employee training tools to provide knowledge and capability to recognize and report suspicious behavior

4. Improve information sharing protocols

- leverage information sharing among all stakeholders to build threat awareness intelligence

3. AI third-party and supply chain vulnerabilities

Nature of the risk

Reliance on opaque third-party AI models and infrastructure exposes financial institutions to cascading risks. This results from growing webs of multi-source supply chain dependencies which create new points of potential failure and avenues for attack.

Canada’s financial sector relies heavily on third-party service providers, particularly those related to AI. AI adoption deepens third-party dependencies for model development, data services, and computing infrastructure. Mid-sized and smaller financial institutions often rely more heavily on external vendors, increasing their risk surface and AI-related third-party risks.

Growing reliance on fourth, fifth, and nth-party providers in AI “supply chains” increases the risk that the disruption or failure of a single vendor could trigger significant impacts. Smaller AI providers may compromise supply chains if they lack the necessary resilience controls.

Conversely, concentration risk is also increasing, as the failure of any one of the few material AI cloud service providers and foundational model developers could trigger cascading financial sector disruptions.

Another common risk among third-party AI providers is the lack of transparency in data, design, and algorithms, which undermines data integrity and complicates model validation. Even fully open-source models often function as black boxes, with billions of machine-learned parameters that are extremely difficult, if not impossible, to interpret.

Risk management implications

Increasing third-party AI dependencies and supply chain vulnerabilities require updated due diligence protocols and clear vendor accountability to ensure consistent and heightened security and operational resilience standards.

Possible steps discussed to enhance third-party resilience include:

- 1. Standardize contractual obligations**
 - standardize contractual language that can be leveraged by institutions of all sizes
 - create clear accountability frameworks and audit rights
- 2. Establish uniform security standards**
 - require independent security testing for external models
 - necessitate AI-third third-party suppliers to meet ISO or other international standards
- 3. Establish uniform disclosure requirements**
 - require data and model transparency
 - establish protocols for visibility into third-party supply chain dependencies
 - Initiate requirements for documentation
- 4. Enhance third-party oversight**
 - explore means of increasing regulatory oversight over key AI third parties
 - establish a joint industry and regulator-approved inventory of certified AI service providers

5. Engage collaboratively

- establish an information sharing forum involving financial institutions, regulators, and supervisors to support the management of AI-related third-party risks

4. AI-driven data vulnerabilities

Nature of the risk

AI systems not only increase the risk of data leakage and corruption but also turn high-value sensitive institutional and client data into increasingly vulnerable targets for threat actors.

AI models and systems consume vast amounts of proprietary or customer-sensitive data. Their rapid development has significantly increased the risk of data loss for proprietary commercial, financial, and sensitive customer data. The adoption of AI systems across business functions also elevates data vulnerabilities. This potential for data corruption can lead to errors in risk assessment, asset pricing, or automated decision-making, resulting in the erosion of trust, reputation, or operational loss.

Data that has been segregated on a “need to know” basis now has a broader network of individuals who “need to know” to deliver sought-after AI benefits. This increases the risk of data loss or data privacy breach.

Risk management implications

Possible steps discussed amongst participants to mitigate AI-related data vulnerabilities include:

- 1. Commit to the fundamentals**
 - prioritize fundamental security hygiene, including network security
 - incentivize multi-factor authentication adoption

2. Clearly define “need to know”

- improve identity and access management controls (IAM) to differentiate business and AI development access to sensitive data

3. Establish new standards for data export

- expand governance and risk guidelines to include the export of proprietary and customer sensitive data

4. Adopt new AI-enhanced tools

- invest to develop and introduce AI-enhanced security monitoring tools to scan and support data access, privacy and network vulnerabilities

5. Augment business recovery tools

- augment business recovery plans to provide for the unintended release of commercial and institutional proprietary data

AI-related opportunities for Canada’s financial sector

Threats, risks, and timely information sharing

Participants identified a key opportunity to strengthen the financial sector’s security arrangements via improving information sharing between governments and institutions, particularly through timely, anonymized, and actionable intelligence. They also saw enhanced collaboration, within organizations, across industry sectors, and between firms of all sizes, as essential for managing AI-related cyber risks and responding to security incidents.

Digital identification and digital verification

The surge in AI-driven social engineering, deepfakes, and synthetic identity fraud underscored for some participants the

need for secure digital identification and authentication. A robust digital ID framework could help ensure that only verified individuals gain access to sensitive systems and data.

Universal adoption of multi-factor authentication

Some participants argued that multi-factor authentication (MFA) adoption is essential to counter AI-powered attacks. A second verification layer protects systems, data, and client accounts from compromise, making MFA a critical baseline for institutional and customer security. One participant noted that “consumers demand speed and convenience, but there needs to be a balance between redundancies and the risk.”

Rethinking employee training against social engineering

Workshop participants advocated for a “rethinking” of employee training against hyper-personalized phishing attempts, balancing realism with ethical and privacy concerns. Rather than deceptive simulations, institutions could focus on engaging scenario-based learning and habit-building to prepare staff for sophisticated threats without compromising trust.

Next Steps

“Public-private forums make sense for learning together and finding ways to bring the benefits of using AI with appropriate controls and risk management.”

Angie Radiskovic, Deputy Superintendent,
Office of the Superintendent of Financial Institutions,
May 2025

Participants heard that financial services are particularly well-suited to benefit from the development and adoption of AI systems, given the data-driven nature of the sector. AI holds the promise to address some of Canada's longstanding productivity challenges. Our financial industry is uniquely positioned to demonstrate leadership in responsible AI adoption.

There was a significant appetite among financial institutions, regulators, supervisors, and academics to continue these and other AI-related conversations to advance policy, best practices in risk management, and accelerate responsible AI innovation. The sponsors will continue to drive those conversations to strike an effective balance between risk management and innovation.

Additionally, there will be opportunities to explore further the topics discussed in this interim report over the remaining three FIFAI

II workshops. Several of the discussions in this first workshop directly relate to upcoming workshops on financial crime, consumer protection, and financial stability, including:

- i. social engineering tactics and synthetic ID fraud, which are primarily used in conventional financial crimes and money laundering efforts (Workshop II),
- ii. the importance of customer communication regarding the use of their data and any potential risks to which they are exposed (Workshop III), and
- iii. how AI-amplified disinformation campaigns and misinformation present an emerging threat to financial stability, capable of eroding public trust and disrupting markets (Workshop IV).

Interim reports will be issued following each upcoming workshop, and a comprehensive final report covering key insights and best practices will follow the conclusion of all workshops.