Cyber Security: Protecting the Resilience of Canada's Financial System

Harold Gallagher, Wade McMahon and Ron Morrow

- Cyber attacks have the potential to pose systemic risk by disrupting the business operations of key participants in Canada's financial system.
- The operational resilience of these participants—large financial institutions and the financial market infrastructures (FMIs) they participate in—is central to the overall resilience of the financial system.
- The attackers targeting elements of Canada's financial system are a diverse group, with varying levels of sophistication and capabilities.
- Canadian financial institutions and FMIs have been proactive in building up their defences against cyber attacks, and actively collaborate with one another and with the federal government.

Introduction

The financial system depends on the collective operational resilience of financial institutions and the payment clearing and settlement systems that facilitate financial transactions. These entities, collectively referred to as financial market infrastructures (FMIs), act as a hub for financial transactions, connecting financial institutions like the spokes of a wheel. Resilient connections between financial institutions and FMIs are integral to the safety and efficiency of the financial system, but these connections also potentially serve as a means to propagate shocks. A long and impressive history of operational resilience is no reason for complacency. An operational event such as a cyber attack that causes a significant interruption to financial services and transactions could have a disruptive effect across the financial system.

To address these vulnerabilities, Canadian financial institutions and FMIs invest considerable effort and resources to ensure the resilience of their operations to a wide variety of disruptions (e.g., natural disasters, power outages and terrorist attacks). However, the rising threat of cyber attacks presents a fresh set of challenges to operational resilience. A cyber attack is the malicious attempt by a group or an individual to compromise or gain unauthorized access to an institution's systems and technology. Globally, the average number of cyber attacks on financial institutions grew by 169 per cent between 2012 and 2013 (PWC 2013). Cyber attacks on FMIs are not as frequent, but FMIs' heavy reliance on technology puts them at risk of a disruptive attack.

This report explores the increasing significance of cyber attacks as a potential source of systemic risk, as well as the types of actors responsible for them and the methods they use. Following a discussion of the risks posed by cyber attacks, the report describes some of the measures being taken by international organizations, financial institutions, FMIs and the federal government to enhance cyber security.

Critical Financial Market Infrastructures

FMIs facilitate the safe and efficient exchange of funds, securities and other financial products between financial institutions such as banks and investment dealers, which rely on FMIs to facilitate the transactions necessary for their operations. In Canada, FMIs have the capacity to process daily cash payments of $150 billion and more than $450 billion in trades of stocks and bonds.

Operational failures at FMIs can sometimes have implications for systemic risk. More specifically, the inability of one financial institution to meet its payment or settlement obligations to the FMI can cause other participants to be unable to meet their obligations, precipitating a cascading failure that spreads throughout the financial system. Given their potential to pose systemic risk, FMIs are overseen by the Bank of Canada to ensure the smooth functioning of the Canadian financial system (**Box 1**).

Box 1

Bank of Canada Oversight of Designated FMIs

A financial market infrastructure (FMI) is a system that facilitates the clearing, settling or recording of payments, securities, derivatives or other financial transactions among participating entities. FMIs allow consumers and firms to safely and efficiently purchase goods and services, make financial investments, and transfer funds.

Some FMIs are designated as "systemically important" because they have the potential to pose systemic risk, in that the inability of one participant to make a payment or deliver a security to the FMI could cause other participants to be unable to meet their obligations, propagating risk throughout the financial system. It is therefore essential that these FMIs incorporate appropriate risk-control mechanisms so that systemic risk is adequately controlled. The Governor of the Bank of Canada has designated several FMIs as systemically important to the Canadian financial system and subject to Bank oversight (**Table 1-A**).[1] The Bank's objectives for its oversight are (i) to ensure that the FMIs operate in such a manner that risk is properly controlled; and (ii) to promote efficiency and stability in the Canadian financial system.

1 For more details on the Bank of Canada's oversight role, see the Bank's website at www.bankofcanada.ca/core-functions/financial-system/oversight-designated-clearing-settlement-systems/.

Table 1-A: Activities of Designated FMIs in 2013

	Volume	Value (Can$ billions)
Large Value Transfer System		
▪ Processes large-value time-critical payments		
▪ Operated by the Canadian Payments Association		
▪ Daily average of Canadian-dollar transactions settled:	30,000	150
CDSX		
▪ Settles equities and fixed-income securities		
▪ Operated by the Canadian Depository for Securities Limited		
▪ Daily average of Canadian-dollar transactions settled:	1,372,000	452
Canadian Derivatives Clearing Service		
▪ Clears repos and derivatives		
▪ Operated by the Canadian Derivatives Clearing Corporation		
▪ Daily average value cleared, cash and repurchase agreements:	--	20
▪ Daily average value cleared (notional), exchange-traded derivatives:	--	101
Continuous Linked Settlement Bank		
▪ Settles foreign exchange payments		
▪ Operated by CLS Bank		
▪ Daily average of Canadian-dollar transactions settled:	27,000	126
SwapClear		
▪ Clears over-the-counter interest rate swaps		
▪ Operated by LCH.Clearnet Limited		
▪ Daily average value of Canadian-dollar swaps cleared:	--	30

Source: Bank of Canada (2014)

Sources of Cyber Attacks

Cyber attacks on Canadian financial institutions and FMIs are a growing concern for both government and industry. While Canadians are most familiar with the web-based services offered by financial institutions, these services make up a small portion of the technology employed by large and complex financial institutions. Consequently, significant effort goes into blocking intruders from using web-based services as an access point to the internal networks, systems and data that support firm operations. In the case of FMIs, internal systems are typically segregated from web-based applications, and thus present a more difficult target for potential intruders. Nevertheless, mitigation efforts must keep pace with the increasingly sophisticated and changing tactics employed by cyber actors.

Cyber actors are a diverse group who represent different threat levels, depending on their motivation and capabilities (**Table 1**). The impact of cyber attacks can vary considerably, but the greatest potential to cause systemic risk comes from cyber actors seeking to disrupt the business operations of financial institutions or to impair FMI critical functions (**Table 2**).

Adversaries are well-organized and well-funded groups of hackers with the most advanced attack capabilities and are motivated by more than just the potential for financial gain. For example, the NASDAQ stock exchange was reportedly infiltrated by adversaries who were able to gain access to confidential information for what might have been years without detection. Once the breach was discovered, investigators suggested that the infiltrators' capabilities extended beyond espionage

and provided the means to sabotage the operations of infected targets (Riley 2014). The impact of the cyber attack was purportedly limited to the theft of proprietary information, but had the group exploited the full extent of its capabilities, the resulting operational disruption could have had implications for systemic risk.

The attack on the NASDAQ revealed that the attackers exploited defects in the architecture of NASDAQ's information technology to allow them access to internal systems. The Heartbleed and Shellshock flaws are examples of this kind of defect, since attackers could exploit defects in commonly used software to access sensitive data, alter website content or compromise visitors' computers (Symantec 2014). Another commonly used technique to gain access to internal systems is known as "spear phishing," which involves sending personalized emails to employees. Once opened, the email installs malware that provides intruders with access to internal systems.

The business operations of financial institutions and FMIs may also be subject to more frequent low-level attacks from groups with less-advanced capabilities. These attacks are often perpetrated by "hacktivists," cyber actors who focus on disrupting operations rather than seeking financial gain. Distributed denial of service (DDoS) attacks are one example of a hacktivist activity, in which high volumes of Internet traffic are manipulated or redirected by hackers to overwhelm company networks. Such attacks are often a daily occurrence for financial institutions and, in some cases, have successfully crashed websites and interrupted the online services of large international banks (Nguyen 2013; Crosman 2014). While these attacks, if successful, are a

Table 1: Cyber Actors—Categories and Attack Capabilities

Cyber actors	Definition
Organized crime	Groups of hackers primarily motivated by profit who seek to attack underdefended targets with techniques previously employed by cyber actors with more advanced capabilities
Hacktivists	Hackers with similar capabilities to those of organized crime but motivated by ideological beliefs rather than financial gain
Adversaries	Groups of hackers with the financial resources and technical expertise to carry out prolonged attacks with motivations that span economic, financial and political factors
Insiders	Disgruntled employees who violate the trust placed in them by using their access to internal systems to launch cyber attacks
Third parties	Competitors or third-party vendors seeking access to proprietary information or to sell information on a system's vulnerabilities to other cyber actors on the black market
Skilled individual hackers	Individuals seeking to exploit target vulnerabilities to achieve notoriety or receive compensation

Table 2: Risk Map—Rating Cyber Actors by Their Potential Impact

	Impacts						
Cyber actors	Financial theft/ fraud	Theft of intellectual property on strategic plans	Business disruption	Destruction of critical infrastructure	Reputational damage	Threats to life/ safety	Regulatory
Organized crime	Very High	Moderate	Low	Low	Very High	Low	Very High
Hacktivists	High	High	Very High	High	Very High	Low	High
Adversaries	High	High	Very High	Very High	Very High	Low	Very High
Insiders	Very High	High	High	High	High	Moderate	High
Third parties	High	Moderate	Moderate	Moderate	Very High	Low	Very High
Skilled individual hackers	Very High	High	High	High	High	Low	High

Very High High Moderate Low

Note: The ratings are adapted from a Deloitte assessment of risks to financial institutions.
Source: Deloitte Center for Financial Services (2014)

source of reputational risk because of short-term outages to web-based services, they do not compromise internal systems.

Many cyber attacks are also motivated by the potential for financial gain. In particular, the theft of proprietary data and financial information (i.e., cyber espionage) can be attempted by a wide variety of cyber actors, including competitors, third parties and insiders (i.e., an institution's own employees). The threat from insiders can be especially difficult to protect against because of pre-existing access to internal systems. Cyber espionage is not exclusive to financial institutions or FMIs but can also include attacks on government entities (Perlroth 2014; Weston 2011). While these types of attacks may not directly affect the functioning of operations, the inability of financial institutions or FMIs to protect the confidentiality of their financial transactions could lead to reduced confidence in the financial system.

Cyber attacks aimed more directly at achieving financial gain by means of theft or fraud could also affect confidence in the financial system. Organized crime groups have recently progressed to more diverse tools and techniques that were previously employed by only the most sophisticated cyber actors. Publicized attacks on financial institutions include the theft in 2013 of US$45 million in cash from ATMs in over two dozen countries, which was coordinated by hackers who manipulated withdrawal limits on compromised credit cards (Santora 2013).

The importance of financial institutions to the economy and the potential for financial gain will continue to provide motivation for cyber attacks from a broad range of actors. Not surprisingly, industry sources cite the financial sector as the target of 15 per cent of all cyber attacks globally, the highest percentage for any industry (Mandiant 2014). FMIs are subject to fewer cyber attacks than are financial institutions; nonetheless, they should remain vigilant and take appropriate precautions to defend against attacks.

Potential Risks

An important part of assessing the potential for systemic risk from a cyber attack is understanding the channels that could propagate the effects of an attack across the financial system.

The potential seriousness of such attacks depends on the degree to which an entity's business operations are impaired. A cyber attack that results in the theft of financial or proprietary data does not affect the core functions of the financial institution or FMI. However, the reputational damage from a data breach can have a negative impact on investors' perceptions of a firm's future profitability (Sharf 2014). It is possible that a loss of confidence in the ability of a financial institution or an FMI to function could have broader implications for systemic risk, since financial system participants could cease to enter financial transactions and withdraw funds in response to a security breach. However, past experience shows that reputational effects may only be transitory and depend on a number of factors, including the type of security breach that occurs and the size of the entity affected (Acquisti, Friedman and Telang 2006).

A cyber attack that disrupts business operations has the potential to directly create systemic risk, depending on the services affected and the duration of the outage. For example, an operational outage that disrupts the core functions of financial institutions or FMIs likely outweighs the impact of DDoS attacks experienced by Canadian financial institutions where only online services are affected.

The impact of a business disruption could also become more severe if core data and systems are corrupted. When the integrity of information and systems can no longer be relied on, services may be interrupted for an extended period as attempts are made to restore the system. The potential for systemic risk could also be amplified if financial market participants lose trust in the accuracy of their financial transactions and positions (CPMI 2014). Financial institutions and FMIs recognize the potential risk of cyber attacks that penetrate internal systems and have taken individual and collective actions to address these risks.

Responses to Cyber Threats

Given the risks, firms around the world are making significant investments to help protect their operations from threats to cyber security. This is particularly true for global operators of critical infrastructure in various sectors, which planned to spend up to US$46 billion on cyber security in 2013 (Rubenfeld 2013). As targets of cyber attacks, financial institutions and FMIs have strengthened cyber security through investments that cover a wide range of initiatives. The first line of defence is the protection of internal systems. The strategies, tools and technologies deployed to prevent a cyber breach include network-penetration testing, strict controls governing access to internal systems, vulnerability-scanning tools, data encryption and timely security updates (OSFI 2013). However, the goal of implementing impermeable perimeter defences to keep attackers out is no longer considered realistic or sufficient to effectively manage cyber-security risks (Kochan 2014). A proactive approach to cyber security involves monitoring the external environment for cyber threats and adopting tools such as network monitoring to detect system breaches when they happen. Financial institutions and

FMIs must also develop appropriate processes and procedures to respond to and recover from a cyber attack once a breach has occurred (NIST 2014).

In addition to the actions being taken by financial institutions and FMIs, authorities need to update supervisory frameworks to reflect cyber-security threats (Bin Ibrahim 2014). In Canada, this process is under way as authorities work to ensure that cyber-security practices incorporate the necessary properties and characteristics to protect against elevated threat levels. The Office of the Superintendent of Financial Institutions has published guidance on cyber security to assist federally regulated financial institutions in assessing the adequacy of their cyber-security practices and help determine the changes required to meet industry best practices (OSFI 2013). Similarly, the Bank of Canada has required systemically important domestic FMIs to complete a self-assessment of their cyber-security practices against standards that promote a risk-based approach to managing cyber-security risk.

Current efforts in Canada mirror actions taken in other jurisdictions since cyber security has been identified as a global public policy issue. In the United States, the Department of Homeland Security issued an Executive Order in early 2013 on "Improving Critical Infrastructure Cybersecurity." Similarly, in 2014, the European Commission published a cyber-security strategy for the European Union. A key point of the strategy is the assessment of security practices for critical infrastructure. These broad initiatives cover essential infrastructure in every industry and form the basis for regulation in the financial sector within those jurisdictions.

International organizations are also seeking to update their policy frameworks to reflect the evolving risk from cyber threats. The Committee on Payments and Market Infrastructures recently published a report on the current cyber-security practices of FMIs (CPMI 2014). The Bank of Canada has adopted the general risk-management guidance issued by this committee as the standard for designated FMIs, and fully expects to incorporate any subsequent guidance related to cyber security (CPSS-IOSCO 2012).

Co-operation on Cyber-Security Initiatives

The establishment of strong cyber-security defences at financial institutions and FMIs is not enough to mitigate the potential for risks to propagate in an interconnected financial system. Because a severe cyber attack could have spillover effects, effective collaboration among FMIs, financial institutions and the federal government is necessary. Engagement with other key sectors (e.g., telecommunications and energy) is also important for ensuring collective operational resilience.

Public Safety Canada is responsible for implementing Canada's cyber-security strategy, which seeks to secure government systems, work with others to secure systems outside of government and help Canadians to be safer online.[1] This approach employs a broad tool kit and focuses on an active, rather than reactive, approach to mitigating cyber-security threats. A key component of the strategy is to strengthen partnerships across sectors and between government and industry. Co-operative initiatives that facilitate information sharing enhance cyber security by creating a forum to exchange best practices, share threat-intelligence information and establish communities of trust between sectors. These initiatives represent a transition from strategies that rely solely on an entity's internal resources to one that leverages the expertise of partners to reduce the likelihood of cyber attacks occurring and to facilitate more effective mitigation strategies.

Initiatives such as Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC), in which Canadian financial institutions and FMIs actively participate, exemplify the benefits of information-sharing efforts. CCIRC is an intelligence exchange that combines key data on cyber attacks reported by participants across industries and government with input from law-enforcement agencies to produce relevant threat information for participating institutions. The receipt of timely threat information can lead to proactive solutions that could prevent a cyber attack from materializing. Furthermore, CCIRC continues to work together with Canadian financial institutions to search for better and more efficient ways to share intelligence information.

FMIs and financial institutions are also involved in co-operative initiatives that focus on exchanging best practices and developing long-term mitigation strategies. Such initiatives provide an effective means to share lessons learned and to develop strategies that address shared vulnerabilities to cyber attacks. While these programs continue to produce important benefits for participating entities, there is a need to expand the existing communities to include other strategic partners. Current efforts by the federal government, financial institutions and operators of FMIs continue to seek ways to establish formal information exchanges with each other and with other key sectors.

Information-sharing initiatives break down barriers to co-operation between entities to produce cyber-security strategies that are superior to any developed in isolation. Achieving meaningful progress on sector-wide operational resilience requires building a consensus among institutions that bring their own priorities and approaches to resolving an issue.

1 For more information, see the Public Safety Canada website at www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-eng.aspx.

Testing Cyber Security

Despite individual and collective actions to mitigate cyber threats, a large-scale cyber attack remains a possibility. The Canadian Bankers Association has a coordinated framework for managing a severe operational event that affects more than one financial institution, including a cyber-incident committee consisting of information technology experts. Canadian FMIs also have their own procedures and contingencies for managing a severe operational disruption. However, the scope of these separate frameworks is too limited for a truly sector-wide operational event. To coordinate actions in a severe disruption, the Joint Operational Resilience Management (JORM) program links members of major Canadian banks, FMIs and the federal government.

To this end, participants in the JORM program have conducted a series of "tabletop" exercises that use fictional scenarios to test the capabilities of both the private and public sectors in some form of crisis situation. These exercises can help to assess key risks, determine how to escalate incidents to decision-makers and coordinate mitigation strategies.

The recently completed 2014 exercise explored a scenario that included a targeted cyber attack on an FMI, resulting in delays and disruptions to the back-office operations of financial institutions. The objective of the exercise was to help clarify roles and responsibilities during a sector-wide operational event. The development of an escalation framework was a key component of the test, and helped to formalize how participants would share information during a crisis event and coordinate actions to respond to such an event. The observations and lessons learned from this exercise will help to further refine industry crisis-response procedures.

The scale of the exercises conducted, in terms of their complexity and the number of stakeholders involved, will continue to expand to a full-scale, sector-wide exercise planned for 2016. This exercise will require a level of planning and coordination comparable with similar exercises conducted by the Bank of England[2] and the Securities Industry and Financial Markets Association (SIFMA) in the United States.[3]

Continued collaboration on testing cyber-security vulnerabilities and capabilities will help to advance the complexity of these tests. In the realm of industry testing, many different dimensions could be expanded. For example, the U.K. financial authorities have focused on developing a framework for conducting tests based on specific cyber-threat intelligence to ensure that the tests replicate as closely as possible the evolving threat landscape.[4]

Conclusion

In addition to traditional threats to operational resilience, financial institutions and financial market infrastructures are facing growing challenges in the form of cyber-security threats. The extensive reliance on technology by financial institutions and financial market infrastructures, coupled with the high degree of interconnectedness between them, increases the sector's vulnerability to a cyber attack. Hence, both private and public sector stakeholders have recognized the need to work together to address these potential vulnerabilities.

Public-private partnerships such as the Canadian Cyber Incident Response Centre and the Joint Operational Resilience Management program have made progress in improving the resilience of financial institutions and FMIs to emerging cyber-security threats. However, to further advance cyber-security initiatives, Canadian financial institutions and FMIs, and their government partners, must continue to leverage established co-operative initiatives.

2 On 12 November 2013, the Bank of England held its second exercise (Waking Shark II) designed to rehearse the collective response of the wholesale banking sector, including investment banks and key FMIs, to understand and minimize the impact of a cyber attack on the sector.

3 On 18 July 2013, SIFMA held its second exercise (Quantum Dawn 2) that simulated a systemic cyber attack on the U.S. financial system and provided the industry with an opportunity to test its response procedures.

4 See "An introduction to CBEST," available on the Bank of England's website at www.bankofengland.co.uk/financialstability/fsc/Documents/anintroductiontocbest.pdf.

References

Acquisti, A., A. Friedman and R. Telang. 2006. "Is There a Cost to Privacy Breaches? An Event Study." Twenty-Seventh International Conference on Information Systems, Milwaukee.

Bank of Canada. 2014. "Oversight Activities during 2013 under the Payment Clearing and Settlement Act."

Bin Ibrahim, M. 2014. "Demystifying Cyber Risks: Evolving Regulatory Expectations." Speech at the SEACEN Cyber Security Summit, Kuala Lumpur, 25 August.

Committee on Payments and Market Infrastructures (CPMI). 2014. "Cyber Resilience in Financial Market Infrastructures" (November).

Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Security Commissions (CPSS-IOSCO). 2012. "Principles for Financial Market Infrastructures."

Crosman, P. 2014. "DDoS Attacks Are Still Happening—and Getting Bigger." *American Banker*, 28 July.

Deloitte Center for Financial Services. 2014. *Transforming Cybersecurity: New Approaches for an Evolving Threat Landscape*.

Kochan, N. 2014. "Taking the Strategic View of Cyber Security." Risk.net, 22 July.

Mandiant. 2014. *M-Trends 2014: Beyond the Breach*.

National Institute for Standards and Technology (NIST). 2014. "Framework for Improving Critical Infrastructure Cybersecurity." 12 February.

Nguyen, L. 2013. "TD Online Banking Services Hit by Cyber Attack." *The Globe and Mail*, 21 March.

Office of the Superintendent of Financial Institutions (OSFI). 2013. *Cyber Security Self-Assessment Guidance*, 28 October.

Perlroth, N. 2014. "JP Morgan and Other Banks Struck by Hackers." *New York Times*, 27 August.

PricewaterhouseCoopers (PWC). 2013. "Defending Yesterday: Key Findings from the Global State of Information Security Survey 2014." September.

Riley, M. 2014. "How Russian Hackers Stole the Nasdaq." *Bloomberg Businessweek*, 17 July.

Rubenfeld, S. 2013. "Cybersecurity Spending Set to Rise to $46 Billion." *Risk & Compliance Journal, The Wall Street Journal*, 17 July.

Santora, M. 2013. "In Hours, Thieves Took $45 Million in A.T.M. Scheme." *New York Times*, 9 May.

Sharf, S. 2014. "Target Shares Tumble as Retailer Reveals Cost of Data Breach." *Forbes*, 8 May.

Symantec. 2014. "2014 Internet Security Threat Report." *2013 Trends*, Vol. 19 (April).

Weston, G. 2011. "Foreign Hackers Attack Canadian Government." CBC News, 16 February.