SYSTEMIC CYBER PREPAREDNESS

AUTHOR:
Mark Caplan, *President, Global Risk Institute*

GLOBAL RISK INSTITUTE

CYBER SECURITY AND FRAUD

Planning for Risks and Repercussions of a Systemic Cyber Issue[1]

Cyber intrusion and cyber resilience are topics receiving tremendous attention, discussion and action currently and for good reason. Financial firms fend off millions of cyber threats daily. Central Bank of Bangladesh, Equifax and others are recent examples of the vulnerability of large organizations and demonstrate the often severe consequences of falling victim.

Being cyber resilient as a financial institution is of paramount importance. Practiced, considered national arrangements are also critical to ensure that critical financial systems and networks can recover to serve their purpose in facilitating a vibrant economy. Given the global networked nature of wholesale finance, the potential impacts to retail confidence and functionality, and lessons learned in combatting spreading systemic risk, there are also important international responses for which consideration and planning is also necessary.

This paper frames the learnings from the most recent efforts to combat global, systemic risk – the 2008 Global Financial Crisis. Important responses came at all three levels – institutional, national, and international. While many of these past efforts will prove beneficial when a systemic cyber event occurs, cyber crime and its potential impacts differs in important ways. As the cyber scenario contemplated in this paper shows, an attack can meaningfully impact the availability of financial institutions, networks, infrastructures, and markets. It could also undermine the integrity of data records which can severely impact the ability to recover and to maintain confidence in the system overall. Given much of global finance relies on critical 3rd parties both within and external to the financial system, the ability to contain risk to and control the resilience of financial networks could be quite different than crises past.

There are many potential domains of impact in the event of a systemic cyber incident – most notably liquidity, functionality and integrity. Wholesale financing, payments, and markets are highly reliant on key players distributing liquidity and risk, and key infrastructures such as central counterparties, trade repositories and data providers. Individuals and businesses rely on access to payment mechanisms and markets, the integrity of record keeping and data, and confidence in institutions and the system as a whole. Retail participants are also at risk to confidence effects spilling over from wholesale finance. Lost confidence in the means to provide the necessities of life is likely most severe consequence of all and in an age of increasing cyber dependency, timelines to withstand a cyber shock are shortening.

1 *The author would like to thank participants in the Global Risk Institute Cyber roundtable discussions for their insights*

There is a clear need for international policy makers to consider these adverse possibilities and take steps to ensure systemic risk is met with targeted, considered response including:

- ***Communications*** *aimed at promoting and restoring confidence*
- ***Contingency*** *planning to enable economies to function in the event of an outage*
- ***Considered*** *responses to denigration of function in secured finance markets*
- ***Cooperation*** *by entities tasked with ensuring response is executed in a contingency*

Introduction

The Global Risk Institute in Financial Services conducted a series of Cyber Security roundtables with leading Canadian financial firms and policy makers in early 2018 with the intent of better understanding the risks and repercussions of a global, systemic cyber outage from the perspective of the Canadian financial services industry.

It is becoming widely accepted that not only must firms plan and prepare their perimeter defenses for a cyber attack, they must also ensure resiliency. Resiliency includes a thought out and practised response in the increasingly inevitable event that a successful cyber breach were to occur. Responsibility for planning and practice rest clearly with senior management and oversight of preparedness with boards of directors. Major financial firms in Canada are on their way to having robust defences including extensive contingency plans, regularly practiced cyber-threat simulations, frequent penetration testing, and coordinated industry technological response.

At a national level in Canada, policy makers, regulators, and industry associations are coordinating cyber response:

- *In the most recently budget, the federal government announced in excess of $500mm directed toward cyber security including the creation of a Canadian Centre for Cyber Security which will include Public Safety Canada's Canadian Cyber Incident Response Centre, the formation of a National Crime Coordination Unit, and monies specifically targeted to safeguard the protection of data held by the Canada Revenue Agency.*
- *The Bank of Canada is supervising key Financial Market Infrastructures as well as driving forward a Joint Operational Resilience Management (JORM) Program.*
- *An industry led not-for-profit – The Canadian Cyber Threat Exchange - has been formed and is aimed at sharing information and analyzing and advising on cyber threats.*

This list is only a sample of some of the work that is occurring.[2] All good progress and clearly necessary.

But is it sufficient?

Given continuing advances in and reliance on technology, the propensity of criminal actors, and the need for coordination to resolve a systemic issue, the answer is likely not.

2 *See GRI's piece "National Approach to Cyber Intrusion" comparing Canada and the UK*

When systemic risk become reality -

Lessons from the 2008 Global Financial Crisis

Financial systems are complex. By their very nature these systems operate as connected networks of institutions and infrastructures – connected locally and, increasingly, globally. And if the 2008 Global Financial Crisis (GFC) taught us anything, it is that when dealing with large and complex institutions and networks in finance, idiosyncratic risk can quickly transform into systemic risk. An issue that may be specific to a market or geography can rapidly spill over through confidence and network effects to other markets, geographies and the real economy.

In reviewing the late '08 to early '09 period, it is apparent that crisis response to events of a systemic nature need to occur at three levels – firm/institution, national and international levels.

Firms responded to the GFC in many and varied ways as the impacts affected each uniquely. Individual actions ranged from asset sales, bolstered liquidity and risk management practices, and business repositioning. More transformational events such as mergers, fundamental structural change (i.e. becoming bank holding companies) and insolvency also occurred.

Nations responded to combat the crisis – capital injections, asset relief/purchase programs, debt guarantees, resolution regimes, monetary policy adjustment, fiscal stimulus, and housing market reform to name a few.

Internationally, many things were globally agreed and implemented on a coordinated basis, in order, in the words of Tiff Macklem, Canada's G7 deputy at the time, "to crush the crisis". Central bank liquidity (swap) arrangements, bank capital and liquidity standards, derivatives market reforms (including standardization, transparency and central clearing), resolution regimes (including cross border elements and bail-in), and a framework for identification and supervision of Globally Systemically Important Financial Institutions (so called G SIFIs). Some have marked the turning point of the financial crisis as the declaration by G7 Finance Ministers and Central Bank Governors after their meeting in Washington, October 2008 to

> *"…Use all available tools to support systemically important institutions and prevent their failure."* [3]

As most will remember, the initial response to the crisis was somewhat uncoordinated, which is to be expected; however, once the systemic risk impacts were becoming apparent, global policy came together under the G7 and G20 forums to set an agenda forward. Sadly, the full effects of the crisis entailed trillions of lost potential global output and tens of millions of lost jobs.[4] The effects continue to be felt and the final chapters likely have not yet been written – central bank balance sheets remain extended, governments' fiscal balance/space remains precarious and the scars of the extraordinary measures taken have likely fuelled the rise of global populism, one of the key global risks highlighted by the World Economic Forum.[5]

---

3 *G7/8 Finance Ministers Meetings, G7 Finance Ministers and Central Bank Governors Plan of Action, October 10, 2008, Washington DC*

4 *In a November 2014 speech by Stephen Poloz, Governor of the Bank of Canada, cited the loss to global output from the crisis was roughly US$10 trillion, which is close to 15 per cent of global GDP. He also noted that there were over 60 million fewer jobs around the world than there would have been had the crisis not occurred. - Bank of Canada, "The Legacy of the Financial Crisis: What we know, and what we don't"*

5 *World Economic Forum, "The Global Risks Report 2018", (Jan 17, 2018)*

Dealing with systemic risk when it manifests – particularly on a global scale – requires a number of things. It requires the right policy prescriptions, intense global cooperation, and perhaps most precious of all during a crisis, time. During the crisis, a senior banking executive called a senior policy maker to inform him of the spreading panic and gridlock in the system. The policy maker thanked him for the information and asked "so what would you like me to do about it"? Top of this wish list likely was to put in place the structures- institutional, national and international- to combat the specific areas of systemic stress. A time machine would have been helpful but this disruptive technology was not yet available.

The point here is not to second guess or seem wise with the benefit of hindsight; rather perhaps some of the learning from the financial crisis regarding necessary international response can be applied to the issue of cyber security. Electronic intrusion and disruptions are becoming part of the fabric of commerce and finance. They are the present and they are the future.

Why is Cyber different?

Cyber actors are many and varied – random criminals, malicious individuals embedded within institutions or critical third-party entities, competitors, activists, Nation states, and terrorists. Cyber incidents can also take myriad forms.

To frame a discussion around the potential domains of impact in financial networks, it is worth noting the types of incidents that have been suffered by global organizations in the recent past[6]:

- *Virus infestation*
- *Email Phishing*
- *Data – breaches, deletions, and theft of IP/trade secrets*
- *Equipment – stolen or lost*
- *Fraud*
- *Attacks involving denial of service and/or ransomware*

The need for vigilance and information exchange regarding new developments on the topic is high- cyber actors have proven to be imaginative and resourceful when it comes to inventing of new threats. Advanced planning is vitally important. According to a recent briefing hosted by the Province of Ontario, the average cyber incident takes on average 191 days to identify and 58 days to contain.

Cyber attacks can manifest as theft or fraud – data or financial – and can have severe impacts on individuals or institutions; however, when thinking through the ex-post impacts for the system as a whole, the two impacts most likely to cause a crisis are problems of availability and problems of integrity.

6 *Financial Times, "Special Report Cyber Security", (March 15, 2008,)*

A systemic scenario could look something like this:

A nation state launched a low-key and initially low-impact cyber attack intended to undermine confidence in institutions and the financial system as a whole. The attack focused initially on compromising back-up data at a number of key financial intermediaries and infrastructures. Once back up data is successfully compromised, previously dormant viruses are activated and attack real-time systems affecting data and in some cases their availability. While institutions scramble to investigate the specific impacts on their systems, data, and networks, social media begins spreading rumors about affected institutions, promoting uncertainty and undermining confidence broadly. Some, but not all, institutions and financial market infrastructures have availability issues limiting their ability to service wholesale clients (trading, payments, securities settlement, asset markets), and retail clients (access to online banking, ATMs, retail brokerage, etc.). Panic is starting to spread as customers demand up to date records of their holdings from institutions where they have accounts.

In both cases, Internal IT resources are fully occupied trying to restore services and the ETA to recovery is uncertain.

The need for detailed, well considered and practiced contingency planning is not a new concept. All mature Canadian financial firms have detailed business contingency plans and processes that are frequently updated; however, the scenario above shows how cyber adds a different and complex element:

1. *Most contingency planning assumes access to technology, technologists and data remain available throughout an incident, usually at a back-up/hot site from which business can continue operating while remediation occurs. As can be seen from the scenario above, this premise may prove false.*

2. *Contingency planning often assumes critical functions can be restored within a prescribed timeframe. While it is clear that a 58 day recovery is beyond the planning horizon for most contingency plans, there will also likely be a time-lag within institutions to determine whether the issue is a cyber attack or a 'generic' systems/data problem. Communication during this lag is of critical importance.*

3. *Current contingency approaches generally assume idiosyncratic outage (or, at a maximum, specific geographic isolation). Given the interconnectedness of technologies, markets, and participants as well as reliance on central hubs (i.e. head office) for technology and data, this assumption needs to be stressed.*

4. *Recovery from a contingency relies heavily on the ability to recover back to a pre-incident state. As the scenario shows, cyber attacks have the potential to undermine data integrity, and with it the ability to affect client and counterparty trust and confidence – a foundational impact to the financial services industry which is potentially profound.*

Many institutions are practicing scenarios of availability, however, response to issues of integrity seem to be less advanced although potentially more impactful. In the event of a wide ranging data integrity issue, there remain a number of unanswered questions – Will liquidity markets (at a minimum) open if participants are unsure of their positions, risk and counterparties? How will deposit insurance work- whose records will take precedence and do individuals understand their coverage? What communications will be helpful to restore confidence?

Critical 3rd parties

In discussing systemic cyber impacts on the global financial system, it is clear that there exists concentrated risk to certain service providers. Some of these providers are endogenous to the financial system itself such as central banks and central counterparties. These entities are indeed central to the functioning of the system, although in planning for resiliency it is important to note that a destabilizing source may not come from within the financial services industry. Issues in exogenous but critical service providers in computing (cloud or common operating platform applications), telecommunications, transportation, or energy grids may have knock-on effects that compromise the financial networks on which all industries rely.

The Day After an attack - Domains of Impact

Financial systems and financial institutions serve governments, corporations, and individuals for the benefit of overall economic efficiency and growth. To prepare and plan for systemic cyber issues broadly it is important to consider issues at an individual institutional level as well as consider the domains of impact to both wholesale and retail finance overall.

There are a number of potential domains of impact from the cyber actors and threats listed above; however, from the scenario exploration undertaken, the three most impactful are liquidity, integrity, and functionality.

Wholesale – Impacts on institutions, systems and markets

MONEY MARKETS - LIQUIDITY AND FUNDING

Borrowing is central to the functioning of the economies of all developed nations. While considerable amounts of debt are issued for term, there is and will always be heavy reliance on the ability to raise short term liquidity to meet obligations as they come due.

Short term financing markets take many forms – interbank lending, repurchase financing, commercial paper, treasury bills – and are characterized by a landscape of participants who are international in nature. For the most part these markets are over-the-counter and bilateral. They contain heavy participation from central banks and fiscal authorities who often act as liquidity providers to the marketplace through auctions of liquidity and securities, and through operations in repurchase arrangements for monetary policy and other purposes. These markets operate on both an unsecured and a secured basis. Security relies fundamentally on the ability to transfer claims on collateral between participants.

A cyber incident that impacts institutions' ability to access short term liquidity could have tremendous disruptive effect. While many emergency arrangements were put in place during the GFC to allow central banks to provide emergency liquidity to the system during times of disruption, the system remains highly reliant on a number of large financial players – nodes, if you will – to intermediate transactions, since only a limited number of participants have access to official sector liquidity. Should just a few key nodes be unable to perform their function, the ability of funding markets to function could become severely impaired and the ability of authorities to provide liquidity compromised.

As was seen in the GFC, this market is heavily reliant on participants' confidence in counterparties' credit worthiness and their ability to settle obligations on a timely basis. A cyber incident could have the effect of dramatically undermining participants' confidence in participating institutions which would lead, at a minimum, to additional inefficiencies and cost to users. In a truly global and systemic issue of confidence, it is likely that foreign sources of liquidity will cease to exist for a period of time.

PAYMENTS AND CLEARING

Highly linked to liquidity and funding are activities around payments and clearing. While payment systems are predominantly national, international payments transactions are of critical importance to the smooth functioning of the global financial system. International payments are conducted through a web of correspondent and intermediary relationships that allow the system to function. As with funding markets, the system is highly reliant on some very large, key financial intermediaries to facilitate payment clearing. While it is fair to say that the use of multiple counterparties builds some redundancy into the system, an attack that was systemic in nature or that adversely affected a central, (national) financial infrastructure could foreseeably prevent the international payment system from functioning.

FINANCIAL MARKETS AND MARKETPLACES

Beside short-term financing markets, further domains of potential impact in wholesale finance are markets and marketplaces. The largest and most important marketplaces as it relates to the global financial system are government and corporate debt markets, equity markets, foreign exchange markets, and derivatives markets. Market microstructure can differ by geography, but it would be a close approximation to suggest that Fixed Income, Currency and Commodities (FICC) markets trade predominantly over the counter, equities trade predominantly on exchanges, and derivatives represent a hybrid.

While many reforms were put in place in the aftermath of the GFC to increase transparency and resilience, notably in derivatives markets, many of these markets are highly connected and remain vulnerable to cyber incidents.

Should an equity exchange be unavailable due to a cyber outage (for any intermediate length of time), not only would there be obvious confidence impacts (at a wholesale and retail level), but many securities would be unable to be traded or effectively valued during the outage. If the exchange were globally significant, one could see large potential spillover effects – investors and speculators might rush to other exchanges to hedge or otherwise transact. And if it were systemic in nature – multiple exchanges for example – the impact on those that remained open could cause harmful asset spiral effects.

Most financial markets are heavily reliant on central counterparties (CCPs) to clear, settle and record transactions. These CCPs likely now fall into a supervisory oversight regime; however, as discussed above, they remain central to market function and therefore represent a key vulnerability.

Many markets that trade over the counter, such as FICC, remain dependent on a few, large intermediaries to facilitate transactions. Most counterparties ensure a breadth of relationships allowing for some resilience, but there is no doubt that a systemic cyber incident involving a few key 'market makers' could be highly impactful on the functioning on these markets, from both an availability and efficiency perspective. The knock-on effects to the real economy of these effects could be similar to those seen during the GFC.

CUSTODIAL SERVICES, MARKET DATA AND TRADE REPOSITORIES

Custodians (be they securities depositories or custody institutions) play a vital role in recording registered owners of securities and holders of collateral. While large financial intermediaries keep their own transactional records up to date, many marketplaces would be unable to function without these key market players. Custodians also play an important role in relation to asset managers who rely on them to hold, record, and settle transactions. Custodians often act as agent for other activities such as securities borrowing and lending.

If a specific cyber event related to data integrity or custodial ability to recognize collateral, the functioning of the short term secured finance market, where trillions of securities are financed daily, could be compromised with likely knock-on effects to the underlying asset markets of debt and equity.

In addition, reliable, real time market data is a foundational element of an effective wholesale financial market infrastructure. Data, of course, comes from many sources such as exchanges and intermediaries and is used not just as an informative input to market making and investment decisions, but also is central to activities such as algorithmic trading and arbitrage. Should market data become corrupted, or its providers unavailable, the first order effects to transactions and second order effects to function and confidence could be large.

Similarly, trade repositories, be they part of an exchange offering or a separate effort such as recently initiated as part of derivatives reform, are an important piece of financial markets function and oversight. Should a trade repository`s data become corrupted it may have a somewhat lesser but not insignificant impact on markets.

Retail- Impacts on Individuals and SMEs

While individuals are exposed at a personal level to cyber threats, all (certainly in the developed world) are also potentially exposed to threats to financial networks.

Individuals rely heavily on financial networks to conduct day to day personal financial transactions. People use cash, card- debit and credit- and digital means of exchange to provide for the necessities of daily life. They store net worth in financial assets that are meant to provide security and liquidity when needed in the future. They purchase insurance to protect against short term and long term peril. Individuals generally trust their financial institutions to maintain accurate and complete records of their holdings and transactions – the exchange of paper records, for positive environmental reasons, is occurring with less frequency. People rely on central banks to control inflation and promote financial stability. And the list could go on.

At an individual (retail) level, the domains of impact relating to financial cyber risk can be summarized as:

- *Access to payment mechanisms and market*
- *Reliance on the integrity of record keeping and data*
- *Confidence in institutions specifically, and the system as a whole*

A problem within the domain of international wholesale finance as discussed above could certainly affect individuals at a retail level; however, it is fair to suggest that most finance involving individuals is national in nature. While it is true that individuals may hold accounts or assets in foreign jurisdictions, the majority of activity and interest is within institutions and systems that reside and operate within the construct of their national borders. Few payment systems are truly international in nature and most institutions offering services to individual customers do so through nationally organized and supervised subsidiaries and branches.

So if the most important domains of individual impact are inherently national in nature, is it important that they be considered when thinking about international cyber readiness? For policy makers concerned with financial system preparedness, the answer needs to be an emphatic yes for a number of reasons.

One obvious issue is spill over. Many firms and institutions are multinational if not global. While considerable work has been underway on home/host prudential oversight, many firms' technologies remain highly linked and somewhat centralized. A retail problem in one jurisdiction – availability or data integrity – could spill over to become a retail impact in other jurisdictions. Coordinating to minimize possible spill over is essential.

But the biggest issue in the domain of individual impact as it relates to international cooperation must be confidence. While retail financial network problems in Japan, for example, may not be of much initial consequence to someone in Germany, should the incident become large or nationally systemic, it could absolutely affect the confidence of individual actors in other not (yet) affected jurisdictions. Social media and other information sharing methods ensures that communications cycles are increasing fast – faster than during the GFC and with the potential to spread misinformation. Attacks in one jurisdiction have the risk of becoming panics and liquidity runs in another.

A national populace affected by lost confidence in the means to provide the necessities of life is likely most severe consequence of all. The most fundamental question to consider in assessing retail impacts is: How long can a nation's populace cope? People tend to be resilient and there are examples of societies continuing for an extended period without a functioning financial system (Ireland in the 1970s comes to mind). But in today's digital world, most individuals and small businesses don't keep much physical cash on hand and many don't have deep relationships with their service providers like they may have in the past. Depending on timing (and weather) our roundtable discussion suggests this timeframe is likely measured in weeks – perhaps as long as a tank of gasoline or two can last but not much after the larger, monthly bills like rent and utilities come due or pension/payroll remittances are expected.

Conclusion and Next Steps

While it is a worthwhile exercise to consider the potential domains of impact of a systemic cyber issue, one must keep in mind that response will always, ultimately, come down to human elements – the response function of agents when confronted with a crisis. People, acting as individuals or agents of institutions, will likely demonstrate typical behaviours when faced with uncertainty. International policy responses need to be tailored to counter individual's natural inclinations of self-protection, withdrawal and lack of trust. Prepared policy needs to lean against the tendency to disconnect from global financial networks in times of uncertain data integrity as a result of cyber stress- rational for each individual institution perhaps but highly damaging to the system and its recovery. Limiting emergent phenomena is critical to preventing social unrest.

Given what we know about the time to implement, the necessity of cooperation, and the 'fog' of policy prescription in a crisis, now is a good time for global policy makers to consider the responses required to ensure financial networks maintain confidence and function.

Responses to be considered must include:

- ***Communications*** *aimed at promoting and restoring confidence by providing accurate and timely information, potentially in advance of complete certainty*
- ***Contingency*** *planning to provide individuals (and economies broadly) with the means to continue to function in the event of an outage*
- ***Considered*** *responses to denigration of function in critical markets – notably short term secured finance*
- ***Cooperation****, nationally and internationally, by entities tasked with ensuring response is planned for and executed in a contingency*

These responses will necessarily entail ensuring ex ante requirements are in place – cooperation protocols, defined responsibilities, and infrastructures that enable reconstruction of critical functions, systems and data to enable recovery on a timeline to prevent crisis.

This paper has hopefully shed some light and provoked some thought on the issue of cyber risk- it remains the issue of foremost concern for members of the Global Risk Institute. We are committed to continuing the dialogue on this important topic and, in a future paper, will publish suggested prescriptions to help ensure resilience.