TC NOTES

PRACTICAL **LEADERSHIP**
AND **GUIDANCE** FROM
TORONTO CENTRE

CYBER RISK

DETERMINING AND DELIVERING A SUPERVISORY STRATEGY

JULY 2023

TORONTOCENTRE
Global Leadership in Financial Supervision

Global Affairs Canada
Affaires mondiales Canada

INTERNATIONAL MONETARY FUND

Sida
SWEDISH INTERNATIONAL DEVELOPMENT COOPERATION AGENCY

CYBER RISK

DETERMINING AND DELIVERING
A SUPERVISORY STRATEGY

TABLE OF CONTENTS

CYBER RISK

DETERMINING AND DELIVERING A SUPERVISORY STRATEGY

Introduction

The risk of cyber-attack has risen rapidly and now regularly appears among the top three risks financial institutions face. This risk also applies to supervisory authorities as organizations themselves. Cyber risk presents some unique challenges to financial institutions and their supervisors. It constantly evolves and adapts, driven by a determined opponent. This makes it difficult to prioritize supervisory resources for maximum effect.

This Toronto Centre Note will help supervisors determine an effective strategy to deal with this constantly evolving risk, and to deliver that strategy with the resources available to them.

Despite the technical nature of cyber risk, most incidents faced by financial institutions result from the failure of basic controls. Consequently, supervising much of this risk can be accomplished with existing resources.

While both dedicated and specialist resources are needed to deliver a comprehensive supervisory strategy, the need for specialist resources can be relatively small.

This Note should be considered in conjunction with three other Toronto Centre Notes:

- Supervision of Cyber Risk,[1] which provides guidance on supervisory standards for cyber risk and the policies and procedures financial institutions should have in place;
- Operational Resilience: The Next Frontier for Supervisors?,[2] which can help supervisors approach operational resilience in financial institutions, since cyber incidents are a major cause of operational outages; and
- Ten Issues for Supervisors During Crises,[3] which is relevant since a severe cyber incident could trigger a crisis.

Risk-based supervision

Many supervisors use a risk-based approach to determine priorities and guide the allocation of resources. This approach must be adapted to accommodate cyber risk, which can have a different profile from other types of risk.

The impact of a firm (that is, the significance of a financial institution and the resources allocated to it) may change given its cyber vulnerability. For example:

- Cyber risk introduces other connections and sources of contagion through the use of a common computer network, software and hardware
- A factor includes whether and to what extent a firm plays a role in systemically important networks, such as clearing, settlement and payments.

[1] Toronto Centre (2018).
[2] Toronto Centre (2021).
[3] Toronto Centre (2020).

The probability of a financial institution failing may also change given its cyber risk. This will be a function of the cyber threat, the firm's vulnerability, and the likelihood that an attempt will succeed. For example:

- A firm's business model may require it to have a large number of external connections – for example, custodians and participants in high-volume payments.
- The business model may be particularly vulnerable to cyber risk. If very dependent on technology (such as service delivery to customers through a mobile phone app), it would be substantially affected even by a short disruption.
- The firm may use third-party providers for its core services.
- The firm's operations may be geographically dispersed, exposing the connections between the parts of the business.

Supervisors must establish their tolerance for harm caused by cyber risk. Several jurisdictions (such as the UK[4]) assume that a cyber failure is certain, so these jurisdictions place a lot of emphasis on resilience and recovery. No matter the risk appetite, accounting for cyber risk will substantially improve the supervisor's ability to determine an appropriate priority for cyber risk. This will help allocate resources.

Micro-supervision

Information

Supervisors need a good understanding of the cyber exposure of a financial institution. Some of this understanding will overlap with an assessment of the firm's technology risk. This should give the supervisor a good understanding of the technology strategy, the main hardware and software applications, recovery procedures, testing cycles, etc.

A supervisor also needs to cover any key third-party providers,[5] the firm's data assets (see Box 1), its upgrade cycle, the process for implementing security patches, and version control.

Box 1: Data assets

- Types
  - Transactional
  - IT configuration
  - Unstructured
- Environments
  - Data warehouses
  - Key databases
- Infrastructure
  - Servers
  - Network devices
  - Storage
  - End-user devices
- Applications
- Third parties
  - Any third-party hosted environments
  - Sharing of data files with other third parties

[4] Prudential Regulatory Authority (2022).
[5] G7 Cyber Experts Group (2018a).

In addition to some baseline data, supervisors must also establish a regular flow of information on some key metrics from financial institutions. The extent and frequency of this information will depend on the overall impact of each financial institution. The metrics should include any cyber events that have occurred, their severity, what was impacted, what was the main channel (vector) used by the cyber aggressor, and the level of escalation within the firm (see Box 2).

Box 2: Some key metrics

- Incidents of non-authorized access
  - Number of devices and length of access
  - Number of non-authenticated accesses and length of each
  - Number of unauthorized software applications on the network
  - Number of instances blocked
- Secure configurations
  - Number of systems not meeting configuration
  - Number of systems for which configuration is not enforced
  - Number of systems not using the latest available operating system software and software patches
  - Number of applications not using the latest available software and software patches
  - Number and frequency of configuration changes
- Information access
  - Number of staff with administrative privileges
  - Number of users
  - Scope of any controlled access based on need to know
- Amount of information transferred between networks at a lower trust level
- Number of instances where staff were fooled by an internal phishing test

Analysis

Armed with both baseline and regular flow information, supervisors need to analyze it. Some useful analytical methods can be used:

Component-driven assessment[6] is useful for exploring a financial institution's exposure to known technical vulnerabilities. For example, there might be a single computer that cannot be patched or upgraded for operational reasons, such as connecting with an older but still operational system. This is common with some types of operational technology. In this case, a component-driven risk analysis can be used to explore how the vulnerabilities of the unpatched machine could affect the financial institution. This analysis can identify safeguards that can be put in place around this unavoidably vulnerable computer.

Component-driven assessment is suitable for:

- Analyzing the risks faced by individual technical components.

[6] National Cyber Security Centre (2018).

- Deconstructing less complex systems, with understood connections between components.

System-driven assessment[7] is useful when analyzing large and complex systems, because it can explore potential failures that occur when systems interact. These happen when individual components within the system are working properly, but a flaw in the way these components interact makes a security breach possible.

System-driven assessment is useful for:

- Exploring security breaches that result from the complex interaction of many parts of a system.
- Analyzing a system that delivers a number of functions.
- Analyzing security breaches that cannot be tracked back to a single point of failure.

Supervisors should expect financial institutions themselves to carry out much of this analysis. If they are not doing so, supervisors should consider requiring it. The existence of such technical analysis is part of an overall assessment of the control environment of the firm, which is a core competence of the supervisor. In terms of cyber risk, supervisors must analyze governance and controls.

In terms of the governance of the financial institution, supervisors should look at the allocation of responsibilities at the board level. What is the capability of the board in relation to cyber risk? How much time does the board devote to cyber risk? How integrated is cyber risk in the overall risk approach of the firm and the information the board regularly receives? How evident is it that the board has fully considered the implications and impact of the strategy on the cyber risk of the firm?

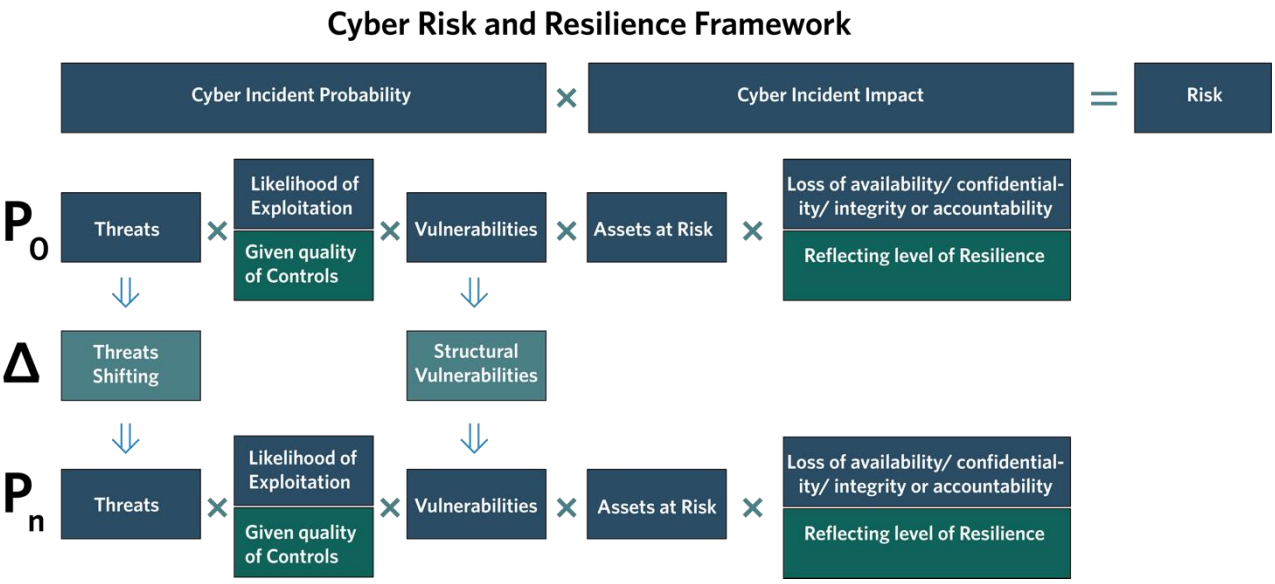
Below the board level, supervisors should look at the allocation of responsibilities. Is there a single accountable executive, such as a Chief Information Security Officer? At what level is this executive? What access do they have? What is the overall level of resource allocated to cyber risk?

[7] National Cyber Security Centre (2018).

Assessment

Having collected the information and the analysis on it, supervisors must make an overall assessment. A framework is set out in Figure 1. This is best approached from two perspectives: that of the potential adversary that could initiate a cyber incident, and that of a supervisor.

Figure 1: Assessment Framework



The probability of an incident occurring is based on assessing four factors: the threat; the likelihood that the exploit will succeed; the quality of controls; and the vulnerability. Taking each of these factors in turn:

A **threat assessment** needs to assemble any information available on potential adversaries. Several countries publish such assessments[8] and these will be a useful resource. Government agencies may also have intelligence available. Any assessment of an adversary needs to consider their intent. The threat will be very different if the intent is the theft of data or cash, the acquisition of intellectual property, or operational disruption. Given the intent, what are an adversary's capabilities? What access do they have to the latest malware? Based on intent and capability, who and what are they likely to target?

The **likelihood of any cyber-attack succeeding** will be a question of whether the financial institution's **controls** are a match for the capability of the adversary. Nearly all attempts by volume will be ones requiring low capabilities of the adversary. That is why firms with good basic controls will be able to defend against them. However, all firms will have **vulnerabilities** that can be exploited. These weaknesses will be both technical and cultural. Any assessment of vulnerabilities also needs to include those of third-party providers.

Supervisors will have a view on the culture of a financial institution from their general supervisory work. Adversaries most commonly find an entry point into a firm's systems by causing human error through social engineering, such as a phishing attack. It is therefore key for supervisors to assess a firm's people and culture as well as its processes and

[8] See the list of National Cyber Security Agencies in Table 1 in the References section.

organization. Assessing people also needs to take into account the possibility of insider action. An insider may have been mistakenly involved or may be an existing member of staff who has been recruited by the adversary.

The analysis of technology risks will give supervisors an idea of the technical vulnerabilities that could be exploited.

With a view on the probability of an incident, the assessment then needs to look at the potential **impact of an incident**. This will be a function of the assets at risk and the consequence of losses of availability, confidentiality, integrity, or accountability.

In making this assessment, supervisors should imagine that a loss has occurred and predict how long or how much the loss can be sustained by the financial institution. So, for example, if the loss of availability of an asset can only be for a very short time, either the controls around that asset must be high or the firm needs a back-up system or process to maintain availability. For some, the risk is a binary one: data are either confidential or they are not. Again, if the impact of a loss of confidentiality is high, controls must be high.

The assessment of probability and impact will provide the supervisor with an **assessment of risk**. However, given the dynamic nature of cyber risk, this should only be the first step. Risk managers describe the ability of a risk to change as migration. How could a risk migrate over time? Consider all the variables relevant to a risk in terms of their ability to migrate. Supervisors will be aware if control environments are changing or some new technology is being introduced. In practice, the two key variables will be the changing nature of the cyber threat and to what extent the vulnerabilities of the financial institution are structural and therefore slow to adapt or change.

Supervisors must keep up to date on any threat intelligence, including the emergence of new adversaries, changes in intent (which could change the target), and changes in capabilities. Some of this change in threat will itself be a response to the countermeasures being put in place by financial institutions. It is a continuing arms race. There will also be the discovery of new technical vulnerabilities to exploit. The ability of the financial institutions to react will depend on how many vulnerabilities are structural and therefore difficult to change. For example, a financial institution may need to be in a particular location or be required to use certain IT architecture for regulatory reporting or connections for payments.

The ability of the threat to change against a financial institution's ability to respond will be the basis of a judgment on migration. If the conclusion is that migration is high, supervisors are best to assume their overall assessment of risk should include potential deterioration.

The above describes a structured process of assessment, but it should not stop supervisors from carrying out additional scenario analysis. One key source of cyber incidents are attempts that missed their intended targets but hit unintended targets. The NotPetya[9] attack of 2017, for example, was at the time thought to be the most destructive piece of malware in history, causing more than $10 billion of damage. Yet most of those affected were thought to be incidental to the main target.

Adversaries have no incentive to make their actions free from side effects. While these unintended consequences are impossible to plan for, they do highlight the need for supervisors to ensure that all financial institutions maintain at least a basic level of cyber risk control.

[9] Cybersecurity & Infrastructure Security Agency Alert (2018).

Testing

Supervisors should adopt a testing regime that allows them to verify their assessments of impact and probability. There are three types of tests:

- Stress testing
- Penetration testing
- Market-wide exercises.

Stress testing is similar to financial stress testing. Either a financial institution or the supervisor can determine the scenario and its scope and complexity.[10] There are four types of stress test and they differ in their starting assumptions:

- *Single parameter shock:* The simplest form of stress, but still very effective. This scenario changes a single parameter, such as the availability of the credit control system or the loss of counterparty data.
- *Historical simulation:* Repeating a known stress event from history. This applies the consequences of a previous incident (from anywhere, not just the firm) to today's financial institution. For example, the supervisor could look at the impact on Maersk from NotPetya,[11] SolarWinds,[12] or one of the many examples that have been extensively written up.
- *Scenario shock:* The most creative form of stress, it requires a financial institution or the supervisor to create a scenario of an incident.
- *Reverse test:* This test flips the logic of the other forms of stress and asks the financial institutions themselves what it would take to cause a severe incident.

Although each test starts differently, all seek to determine the initial impact of the stress, and the financial institution's ability to respond and recover. These stress tests are best suited to probe the impact of incidents because the probability of events is assumed in the test.

Each type of stress has its strengths and weaknesses:

- The Parameter shock is easy to administer and understand but may lack realism; in a real incident, there is usually more than one component.
- The Historical simulation has the advantage of credibility because it has happened and there may be good records of the initial and subsequent rounds of impacts. The weakness is that the events from the Historic simulation may not reflect the current level of controls and current level of vulnerability.
- The Scenario shock combats this problem by being based on the current state, but requires more input from a financial institution or the supervisors to determine an appropriate and credible scenario.
- That challenge is met by the Reverse test, where the burden of creativity is placed on financial institutions. Supervisors need to assess whether the scenarios that financial institutions determine are credible.

[10] Financial institutions should devise and run stress tests as part of their own risk management. Supervisors may also want to require a specific financial institution or a set of financial institutions (usually the larger ones) to run a specific stress test (or tests) determined by the supervisor.
[11] Greenberg (2018).
[12] National Security Agency (2021).

Penetration testing[13] is specialized, requiring highly trained and trusted resources (ethical hackers) to carry out an ethical cyber intervention. Often armed with the latest threat intelligence, the penetration team will be given a mission by the supervisor. The test determines how far the ethical hackers can penetrate the systems of the firm and complete the mission. Such work provides an almost unparalleled view of the financial institution's cyber defence and contributes significantly to the supervisor's assessment of probability. The main downsides of the approach are cost, since expert resources are scarce and expensive; and the ethical approach does not test unethical approaches.

Both the stress and penetration tests are based on a single financial institution. Even if a number of financial institutions were provided with the same stress, the test would not provide insight into the interactions between financial institutions. A **market-wide exercise**[14] is probably the best way to assess "contagion" between financial institutions in a testing environment. A market-wide exercise will usually be scenario-based (generated or historical) and have stages. Supervisors will present a stage, then gather feedback from financial institutions as to how they might react. That reaction feeds into the next stage.

Testing provides a good source of data for supervisors in assessing risks, but it also helps with capacity building. Staff within financial institutions and supervisors themselves get to experience some of the same issues they would face in a real situation. It allows everyone to establish key relationships, determine the likely key questions, and work on areas the test exposes as needing improvement. A good test should, therefore, always pose new questions and provoke thinking and action.

Supervisory intervention

Reporting, analysis and assessment are not ends in themselves, and supervisors need to consider how they should respond to the risks they find. The supervisor's risk appetite will determine whether the supervisor accepts the risk; takes no further action but continues to monitor the risk; or institutes some form of risk mitigation at either a policy or financial institution level, or both. For policy responses, see the next section on Policy.

For firm-based risk mitigation, supervisors should develop a toolkit. The toolkit should cover all aspects of the risk, vulnerabilities and impact, and controls. Supervisory interventions may include:

- Requirements to improve controls.

[13] G7 Cyber Experts Group (2018b).
[14] G7 Cyber Experts Group (2020)

- Requirements to improve the quality and timeliness of risk identification. This could include additional analysis by the financial institution, or for it to undertake (further) penetration testing.
- Requirements to improve the capabilities of the financial institution to deal with incidents.
- Requirements to reduce the attack surface of the financial institution, such as the location of data assets.
- Requirements to reduce the impact of incidents by improving recovery and resilience.

Figure 2: Supervisory Operating Model

Supervisors will have their own approach to risk appetite, reflecting their powers and strategy.

Evaluation

Once supervisory intervention tools have been used, the supervisor should evaluate the success of their intervention. Further tools should be used if a gap remains between where the financial institution is and the supervisor's risk appetite.

Policy

Toronto Centre (2018) provides more detail on the standards supervisors should require of their firms, so this TCN will simply look at an overall framework.

The policy on cyber risk clearly needs to be compatible with the supervisors' overall approach to policy. There are, however, some features of cyber risk to keep in mind. Its rapidly evolving nature makes a system of detailed rules difficult to maintain. Also, given a determined opponent looking for vulnerabilities, supervisors need to be aware that overly prescriptive rules might introduce common vulnerabilities into the financial system.

This suggests that a more principles-based approach might be preferable. However, supervisors are aware this can pose some challenges, including the lack of compliance certainty, the demand for greater clarity from financial institutions, and the challenge of enforcement. That said, a principles-based approach is more likely able to cope with a risk that is quickly evolving.

The supervisory strategy will need some rules – for example, to establish the regular reporting regime and some minimum standards.

Supervisors should also consider whether to make it a requirement that firms have a Cybersecurity Incident Response Plan (see Box 3). Such a plan should establish a baseline of competence within financial institutions in dealing with incidents. It also provides a useful

resource for supervisors when they have to deal with a financial institution during an incident.

Box 3: Cyber incident response plan

- Allocation of responsibilities
  - Oversight
  - Support
  - Communication
- Oversight and governance
  - Escalation
  - Decision making
  - Cyber Incident Response Team
- Support
  - Key contact numbers
  - Conferencing system
  - Playbooks
- Response
  - Triage
  - Assessment
  - Remediation/containment
  - Recovery
  - Review
- Communication
  - Internally
  - Externally
  - Law enforcement
  - Regulators
  - Media
  - Other third parties
- Post-incident review

Specialist supervision

The skillsets needed for specialists within supervision will depend on whether the function needs or wants to be self-sufficient. If supervisors have access to a government agency that focuses on the jurisdiction's cyber expertise, supervisors may not need to replicate that capability.

If the supervisor chooses self-sufficiency or in the absence of a government agency, supervisors will need specialists in cyber security. The types of specialists are set out in Box 4.

Even if many skills are available elsewhere, supervisors should consider the advantages of having dedicated resources on cyber risk. Dedicated resources make it easier to keep pace with the rapidly changing risk landscape and to focus the activity.

Cyber specialists should be used to assess and analyze the highest risks facing the supervisor. They should also be charged with knowledge transfer to the general supervisors.

Box 4: Specialist cyber skillsets

- Malware and attack technology
  - Adversarial behaviour
- Security operations
  - Distributed systems
  - Authentication, authorization & accountability
  - Software
  - Web and mobile
  - Networks
  - Hardware
- Forensics
- Cryptography

Other stakeholders

Cyber risk is not just a financial services issue. It also affects a wide range of sectors, such as government, energy, and commerce. Although threats and the intent of adversaries may differ, many of the issues will be the same. This may therefore lead to mutually beneficial partnerships between supervisors and other public sector bodies.

Many jurisdictions have created a national centre of expertise on cyber risk, which can be a useful source of expertise and assistance with cyber risk.

In the early days of cyber risk, firms that were the victims of cyber incidents were reluctant to disclose any information for fear of harming their reputation. Now financial institutions are more apt to see the advantage of cooperation and partnership. Organizations that provide models of sectoral partnership, often in conjunction with supervisors, include the Financial Services Information Sharing and Analysis Center (FS-ISAC), an international cyber intelligence sharing community, and the Cross Market Operational Resilience Group (CMORG) in the UK.

College of supervisors

Cyber risk should form part of the regular dialogue within supervisory colleges. This dialogue should include not only a discussion of the current risk assessment, but also arrangements if an incident were to occur. This needs to be an open discussion that acknowledges the challenges of cyber risk. Malicious code can reside within a firm's systems for many months, if not years, and some codes contain instructions to destroy audit trails. That means it can take a long period of detailed forensic analysis to determine what happened. Information exchange under these conditions is difficult. Those receiving whatever information has been provided also need to be clear how they will respond to the likely high level of uncertainty of the position.

A number of groups continue to work on protocols. Hong Kong and Singapore, for example, signed a cyber security memorandum of understanding in 2019[15] that established a data

[15] Singapore Personal Data Protection Commission and Hong Kong Privacy Commissioner for Personal Data (2019).

protection information sharing mechanism. The G7 Cyber Experts Group has looked at incident reporting[16] and the Financial Stability Board (FSB) recently published a report that recommended greater convergence in cyber incident reporting.[17] The FSB also regularly updates its Cyber Lexicon.[18]

Macro-supervision

Cyber incidents have the potential to create financial stability issues, often affecting payment and settlement systems. Macro-supervisors, like their micro counterparts, must consider what their tolerance is for disruption. With this and the supervisory risk assessments and information from testing, macro-supervisors can determine whether the financial sector can continue to deliver essential services. Any gaps between the risk appetite and the current assessment of risk will require risk mitigation.

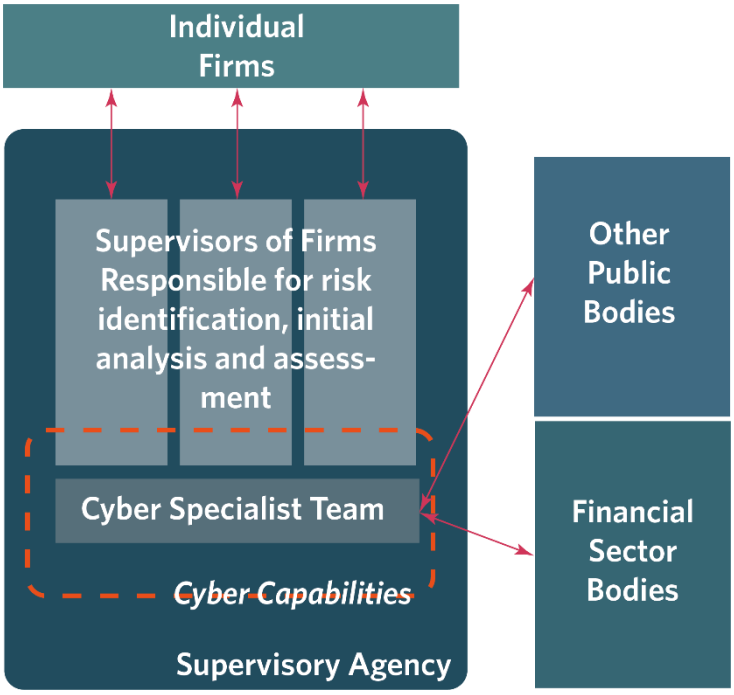
Resource model

Given the supervisory strategy set out above and the resources available, what resource model should supervisors consider?

Cyber risk justifies dedicated specialist resources that can assist the supervisory authority where expertise is most needed. Firm-based supervisors should be given the skills and training to carry out initial analysis and assessment of cyber risks. Given the rapidly changing nature of cyber risk, this training will need to be regularly refreshed.

Cyber specialists are on call to assist supervisors, but they should also be tasked with liaising with other public bodies with an interest and expertise in cyber risk. That may include financial sector groups that are driving collective action.

Figure 3: Resource model



Supervisors should also consider seeking the advice of staff charged with the cyber security of the supervisory authority itself.

[16] G7 Cyber Experts Group (2021).
[17] Financial Stability Board (2023a).
[18] Financial Stability Board (2023b).

Incident management

Toronto Centre (2020) provides useful guidance for supervisors that is relevant for all crises from whatever cause. There are two particular issues that supervisors should keep in mind with cyber incidents:

First, one of the main objectives in a crisis is to restore quickly, or keep open and functioning, retail and wholesale markets. In some cyber incidents, the objective or the consequence might be data corruption. Keeping markets open in such circumstances may make this data corruption worse.

Second, it may be difficult to restore functions after a cyber incident. Counterparties might be reluctant to deal with a financial institution that was the target of a cyber incident. This has particularly been the case where a financial institution was the victim of ransomware and was suspected of paying the ransom. The suspicion lingers that the financial institution may still be vulnerable. Supervisors will need to consider whether they require additional verification of financial institutions before restoration takes place, and who might have the credibility and resource to carry out this verification.

Risk management of the supervisory authority

Supervisors should be careful that their strategy and operations do not increase the cyber exposure of the authority without just cause. This risk is at its most acute when reviewing the information on financial institutions that supervisors gathered in the course of their work. Details of software and hardware configurations, assessments of control weaknesses and other vulnerabilities, and many other items would be very valuable to adversaries. The security of highly confidential information is nothing new to supervisory authorities, but it is worth considering the benefit of collection against the cost of its loss or disclosure.

Conclusions

Cyber risk is the scourge of our digital age. While it poses some unique challenges to supervisors, many of its elements – such as the assessment of business models, governance and controls – are familiar. Supervisors must incorporate the identification, assessment, and mitigation of cyber risk into their overall approach. They can do this by establishing regular reporting, an analytical capability to review those reports, and a structured assessment methodology that prioritizes their mitigation efforts. Supervisors are not alone; many face the challenges of cyber risk, so adopting a partnership approach has many benefits.

References

Cybersecurity & Infrastructure Security Agency Alert. *Petya Ransomware*. February 2018.

Financial Stability Board. *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report*. April 2023a.

Financial Stability Board. *Cyber Lexicon: Updated in 2023*. April 2023b.

G7 Cyber Experts Group. *G7 Fundamental Elements for third party cyber risk management in the financial sector*. October 2018a.

G7 Cyber Experts Group *G7 Fundamental Elements of Threat-led Penetration Testing*. October 2018b.

G7 Cyber Experts Group. *G7 Fundamental Elements of Cyber Exercise Programmes*. October 2020.

G7 Cyber Experts Group. *Proposal for a common categorisation of IT incidents*. April 2021.

Greenberg, Andy. *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.* Wired Magazine. August 2018.

National Cyber Security Centre. *Risk Management Guidance*. November 2018.

National Security Agency. *Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks*. April 2021.

Prudential Regulatory Authority. *Operational resilience: Impact tolerances for important business services*. March 2022.

Singapore Personal Data Protection Commission and Hong Kong Privacy Commissioner for Personal Data. *Hong Kong and Singapore Sign MOU to Strengthen Cooperation in Personal Data Protection*. May 2019.

Toronto Centre. *Supervision of Cyber Risk*. December 2018.

Toronto Centre. *Ten Issues For Supervisors During Crises*. April 2020.

Toronto Centre. *Operational resilience: The Next Frontier for Supervisors?* April 2021.

Table 1: National Cyber Security Agencies

The National Cyber Security Centre (UK)	https://www.ncsc.gov.uk
Cybersecurity and Infrastructure Security Agency (CISA) [US]	https://www.cisa.gov/
Australian Cyber Security Centre (ACSC)	https://www.cyber.gov.au
Canadian Centre for Cyber Security (CCCS)	https://www.cyber.gc.ca/en

New Zealand National Cyber Security Centre (NZ NCSC)	https://www.ncsc.govt.nz
National Security Agency (NSA) Cybersecurity Collaboration Center [US]	https://www.nsa.gov/Cybersecurity/
Federal Bureau of Investigation (FBI). Cyber Investigations [US]	https://www.fbi.gov/investigate/cyber

Table 2: Other Useful Groups

Financial Services Information Sharing and Analysis Center (FS-ISAC)	https://www.fsisac.com
Cross Market Operational Resilience Group (CMORG)	https://www.linkedin.com/company/65895562/

Table 3: Other useful publications

Carnegie Endowment for World Peace (Carnegie) Cyber Capacity-building Tool Box	https://carnegieendowment.org/specialprojects/fincyber/guides
Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment – Carnegie	https://carnegieendowment.org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911CMORG
Advancing Cyber Resilience Principles and Tools for Boards – World Economic Forum	https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards/
National Institute of Standards and Technology (NIST) Handbook on Information Security	https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-100.pdf