IT Risk: Cybersecurity

Agenda – Purpose of Presentation

- Define cybersecurity
- Describe the challenges unique to cyber risk
- Discuss how financial institutions have responded to cyber risk
- Describe supervisory tools used for this risk
- Discuss approaches to supervising cyber

Ground Rules for Cybersecurity Discussion

Cybersecurity…

does not recognize borders, so neither should your comments and questions.

is a dynamic risk, so think outside the box in terms of supervisory approach.

is a pervasive business risk, so consider our discussions as a safety and soundness challenge where technical skills are not required.

risk management places great importance on information sharing, so share for the betterment of all.

What is Cybersecurity?

How would you define Cybersecurity?

- Is there an organization /agency whose definition you utilize?
- What immediately comes to mind when you hear the term?
- What connotations does it carry within your country?

What is Cybersecurity?

A broad concept for which there is no consensus definition…

Strategies, policies and standards encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities and policies regarding the security of (an FMI's) operations. *– Bank for International Settlements*

The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets *– International Telecommunications Union*

The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems

– ISACA

What makes Cyber Risk Challenging?

Why is Cyber Risk Challenging?

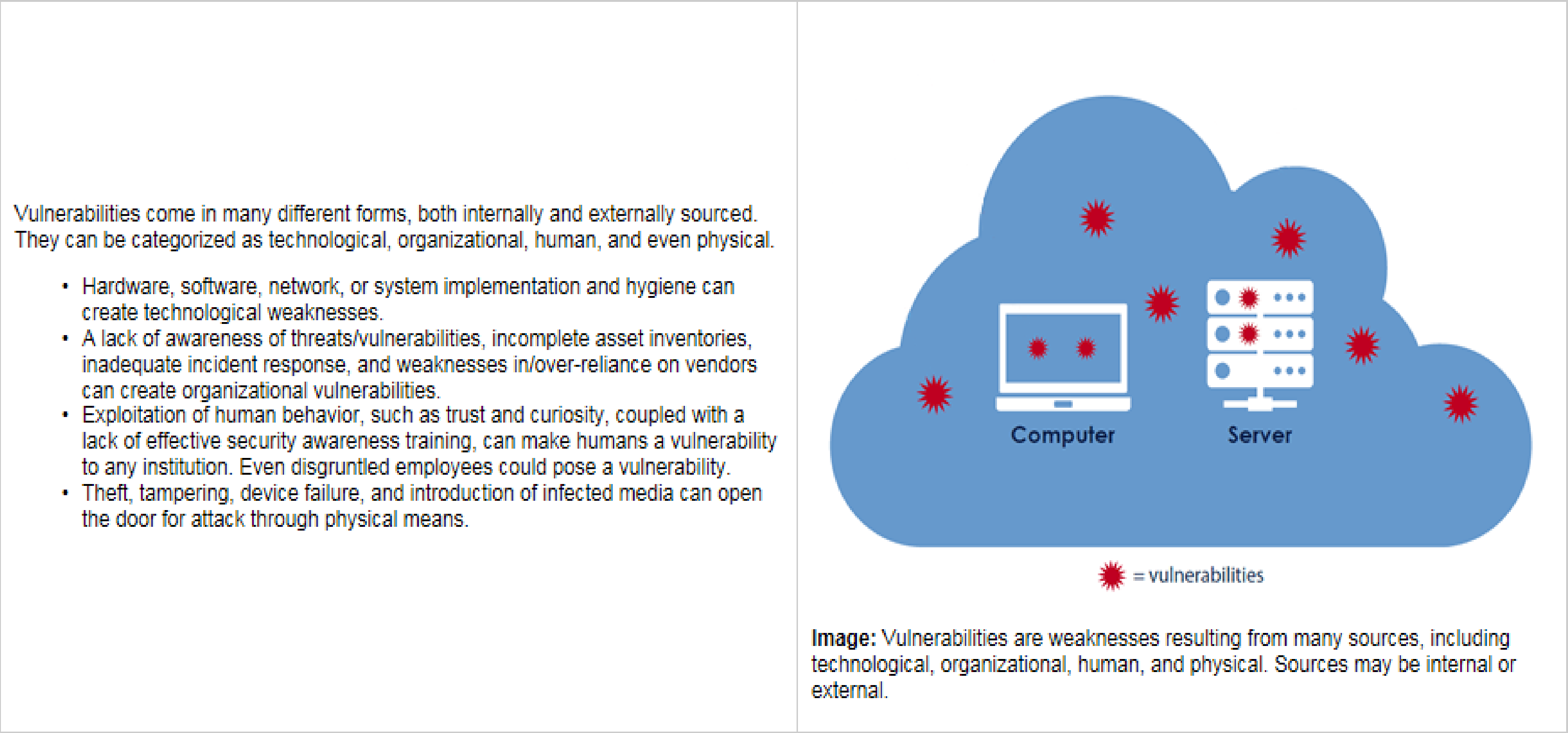
- What makes cyber risk different from other risks we supervise?
  - Dynamic Nature – Evolving Threats
  - Lack of Geographic Barriers
  - Specialized Knowledge Gap
  - Applicability to Current Practices
  - Absence of Guidance/Standards

- What other risks do we supervise that share these traits?

- How do our supervisory practices promote or deter us from supervising this risk?

What makes Cyber Risk Challenging?

Identifying and addressing vulnerabilities is a constant game of cat and mouse for our firms, as fast as patches are implemented new vulnerabilities surface.



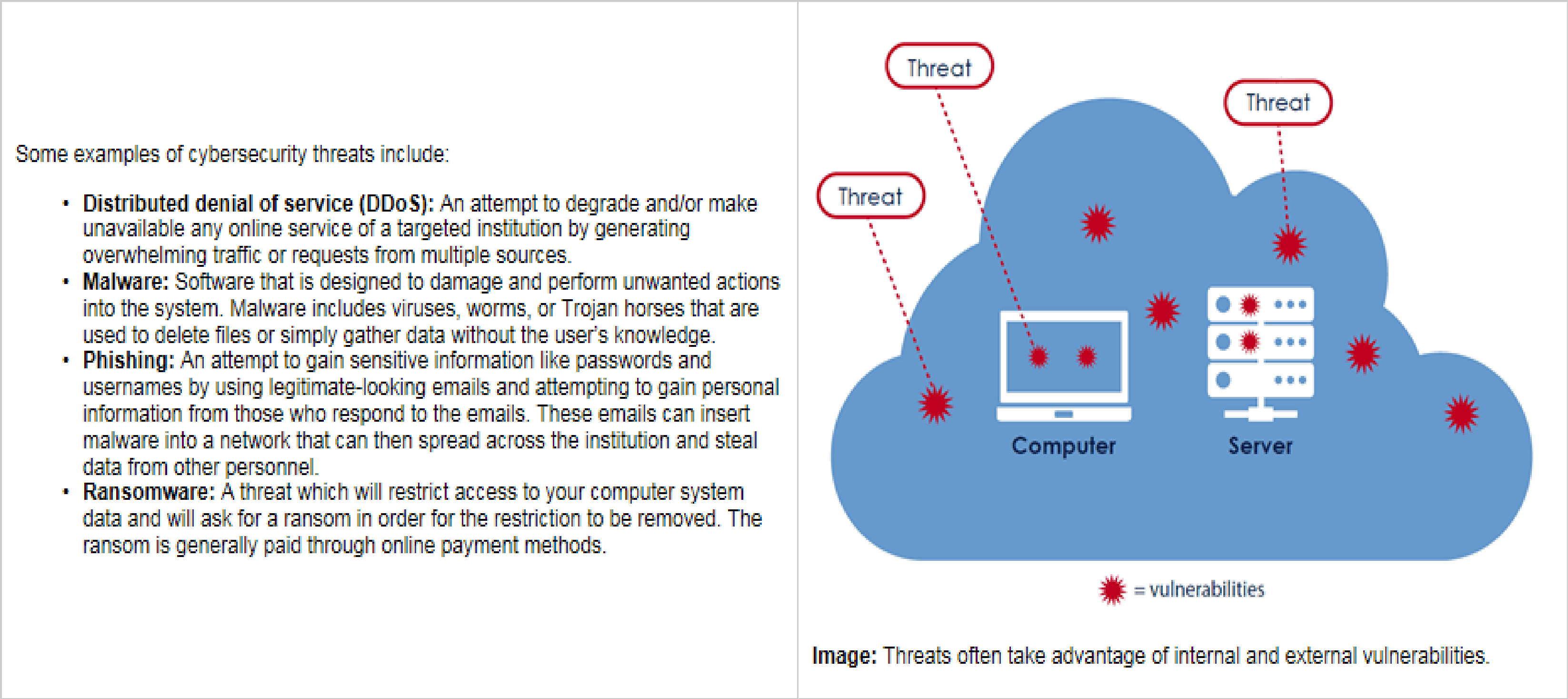
Vulnerabilities come in many different forms, both internally and externally sourced. They can be categorized as technological, organizational, human, and even physical.

- Hardware, software, network, or system implementation and hygiene can create technological weaknesses.
- A lack of awareness of threats/vulnerabilities, incomplete asset inventories, inadequate incident response, and weaknesses in/over-reliance on vendors can create organizational vulnerabilities.
- Exploitation of human behavior, such as trust and curiosity, coupled with a lack of effective security awareness training, can make humans a vulnerability to any institution. Even disgruntled employees could pose a vulnerability.
- Theft, tampering, device failure, and introduction of infected media can open the door for attack through physical means.

Image: Vulnerabilities are weaknesses resulting from many sources, including technological, organizational, human, and physical. Sources may be internal or external.

What makes Cyber Risk Challenging?

One of the primary challenges with monitoring and responding to cybersecurity risk is the constantly evolving threat landscape.



Some examples of cybersecurity threats include:

- **Distributed denial of service (DDoS):** An attempt to degrade and/or make unavailable any online service of a targeted institution by generating overwhelming traffic or requests from multiple sources.
- **Malware:** Software that is designed to damage and perform unwanted actions into the system. Malware includes viruses, worms, or Trojan horses that are used to delete files or simply gather data without the user's knowledge.
- **Phishing:** An attempt to gain sensitive information like passwords and usernames by using legitimate-looking emails and attempting to gain personal information from those who respond to the emails. These emails can insert malware into a network that can then spread across the institution and steal data from other personnel.
- **Ransomware:** A threat which will restrict access to your computer system data and will ask for a ransom in order for the restriction to be removed. The ransom is generally paid through online payment methods.

Image: Threats often take advantage of internal and external vulnerabilities.

Threats could include entry from third parties that are aimed at exploiting interconnections of firms and service providers.

What makes Cyber Risk Challenging?

Across the industry it is recognized that cybersecurity cannot be fought alone and, thus, the sharing of cybersecurity threat intelligence and vulnerability compromises is also important to an institution’s ability to keep pace with this dynamic threat landscape and prevent costly incidents from occurring.

Incidents may include but are not limited to:

- unauthorized scans or probes,
- denial of service,
- social engineering,
- unauthorized entry,
- malicious code or virus,
- security breach or potential security breach,
- networking system failure (widespread), and
- application or database failure (widespread).

In financial institutions, there are millions of possible signs of incidents that may occur each day. These are often recorded by logging and computer security software. A financial institution needs to be able to filter these logs quickly to identify possible security incidents, and automation is generally necessary to conduct this analysis.

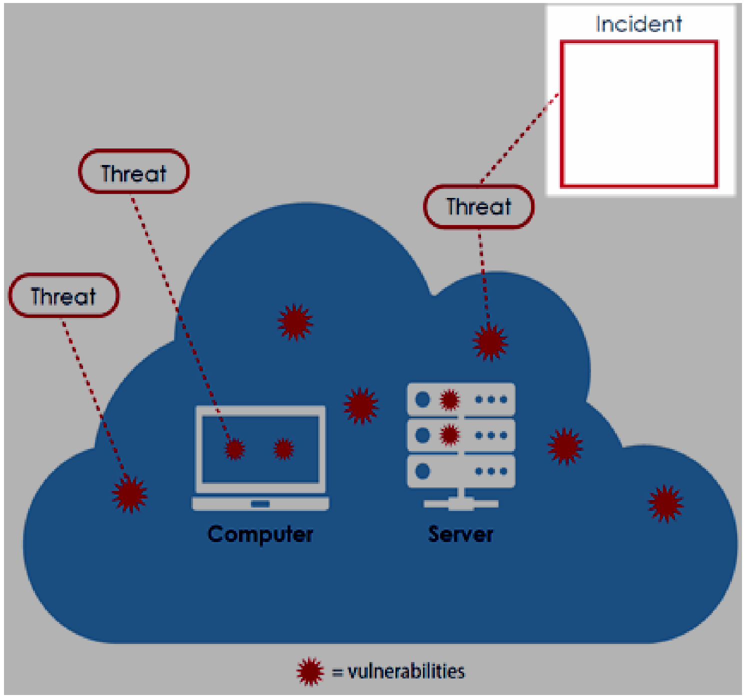
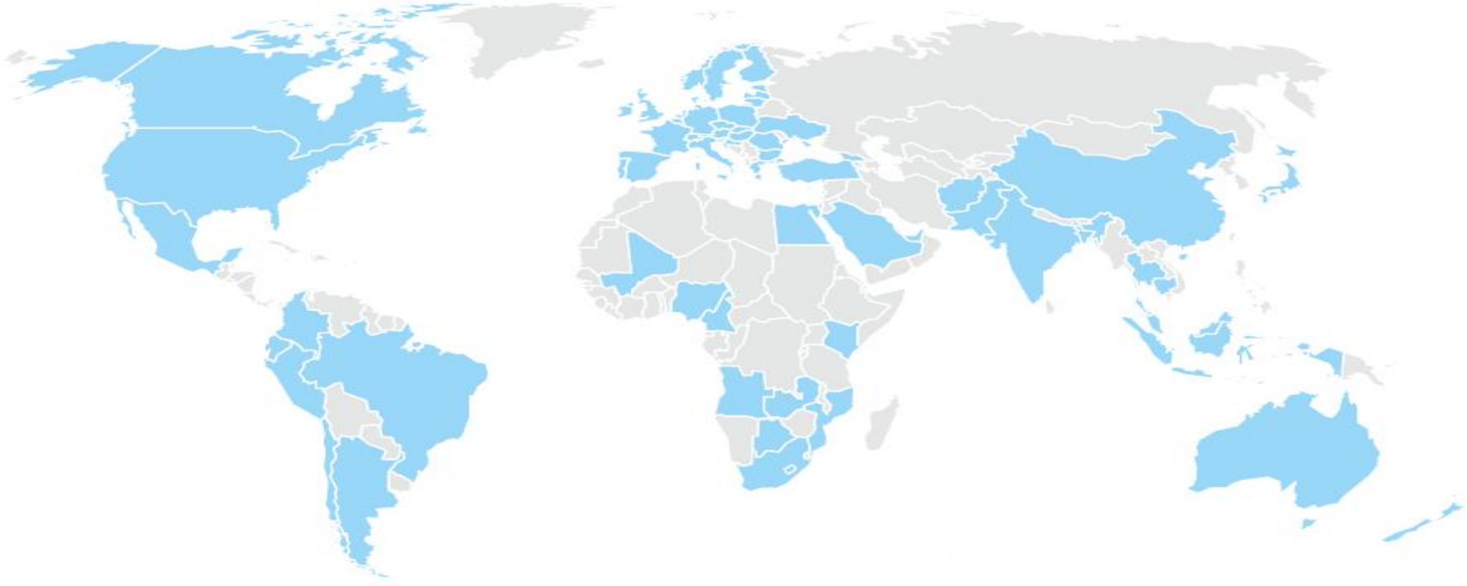


Image: A threat becomes an incident when there are violations of computer security policies, acceptable use policies, or standard computer security practices.

What makes Cyber Risk Challenging?

No locale, industry or organization is bulletproof when it comes to the compromise of data.



2016 Data Breach Investigations Report by Verizon captured incidents affecting organizations in 82 countries and across a myriad of industries.

What makes Cyber Risk Challenging?

Some of the biggest Security Breaches reported so far in 2016 target personal information that could be used fraudulently in the banking sector.

FACC

- $54.5 million

University of Central Florida

- 63,000 records

US Dept. of Justice

- 30,000 employee records

Internal Revenue Service

- 700,000 records

UC Berkeley

- 80,000 records

Snapchat

- 700 records

21st Century Oncology

- 2.2M patient records

Premier Healthcare

- 200,000 patient records

Verizon Enterprise Solutions

- 1.5M customer records

Yahoo!

- 500M accounts

Dropbox

- 68M accounts

LinkedIn

- 117M accounts

Oracle

- Source of data for other POS attacks

Philippine Commission on Elections

- ~55M voter records

Wendy's

- Malware on POS

Newkirk Products

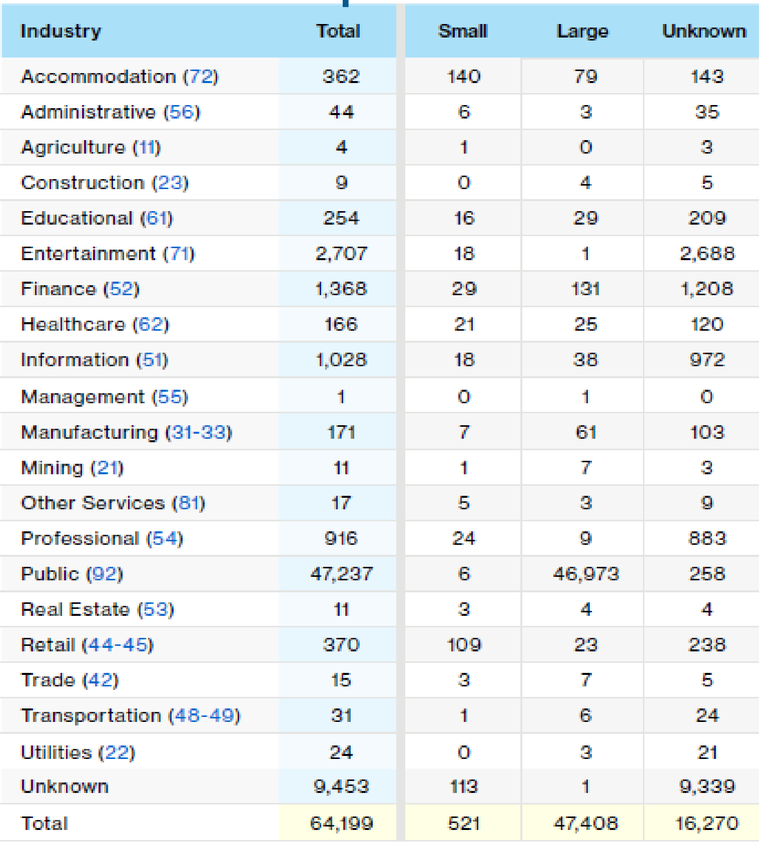
- 3.3M healthcare IDs

Source: https://www.identityforce.com/blog/2016-data-breaches

What makes Cyber Risk Challenging?

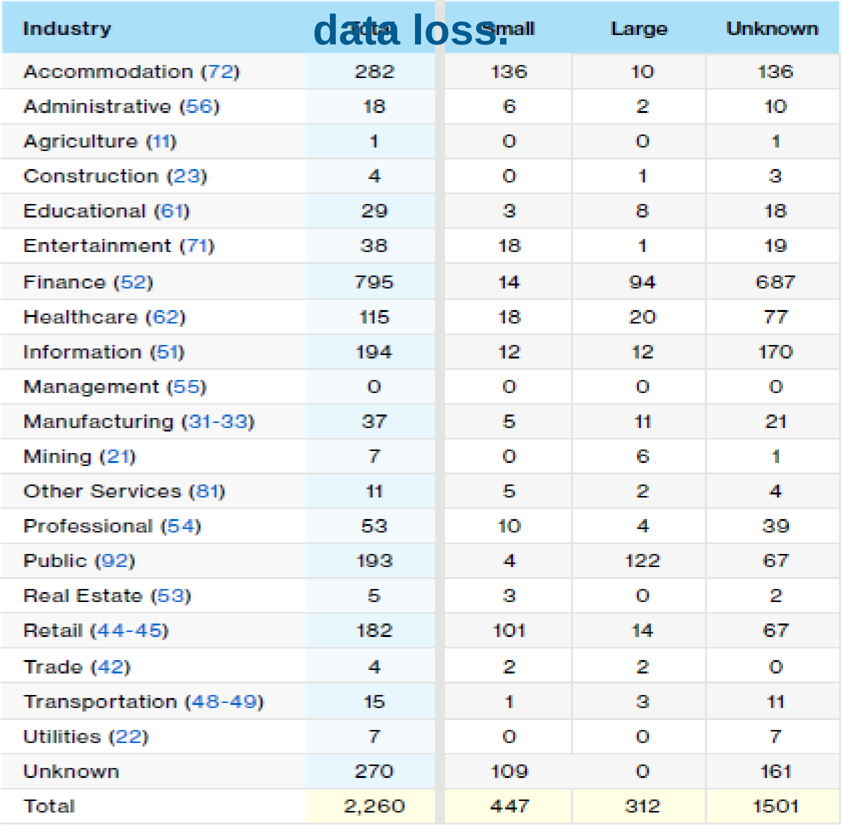
The Financial Services industry continues to be a major target.

Finance industry accounted for 8% of private industry incidents reported in 2016.



Industry	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31-33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (44-45)	370	109	23	238
Trade (42)	15	3	7	5
Transportation (48-49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

Finance industry accounted for 35% of all reported incidents with a confirmed data loss.



Industry	Total	Small	Large	Unknown
Accommodation (72)	282	136	10	136
Administrative (56)	18	6	2	10
Agriculture (11)	1	0	0	1
Construction (23)	4	0	1	3
Educational (61)	29	3	8	18
Entertainment (71)	38	18	1	19
Finance (52)	795	14	94	687
Healthcare (62)	115	18	20	77
Information (51)	194	12	12	170
Management (55)	0	0	0	0
Manufacturing (31-33)	37	5	11	21
Mining (21)	7	0	6	1
Other Services (81)	11	5	2	4
Professional (54)	53	10	4	39
Public (92)	193	4	122	67
Real Estate (53)	5	3	0	2
Retail (44-45)	182	101	14	67
Trade (42)	4	2	2	0
Transportation (48-49)	15	1	3	11
Utilities (22)	7	0	0	7
Unknown	270	109	0	161
Total	2,260	447	312	1501

Source: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

What makes Cyber Risk Challenging?

Motivations for generating new threats are varied, but a majority are financially driven.

Motivations could include….

Financial

Espionage

Fun

Ideology

Grudge

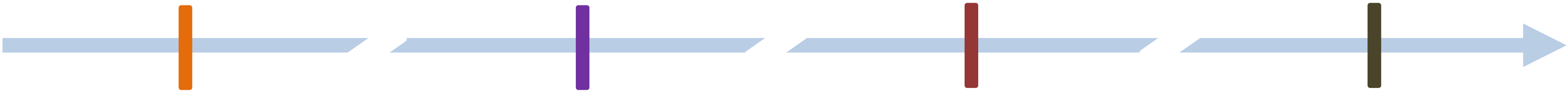
Other

Secondary Motive:
Aid in or distract from a different attack

What makes Cyber Risk Challenging?

Attackers motives also continuously evolve, making it a challenge to anticipate threats before they occur.

Threats evolve with attackers motives…



Blackmail Executives

Attacker breached executive email to **blackmail** against the release of *The Interview*, and published **humiliating** emails after the movie's release.

Sony Pictures Breach

Disrupt Infrastructure

Attacker infiltrated Ukraine's power grid using multiple attack methods in order to **stop electricity delivery to citizens** as retribution during a political conflict.

Ukraine Breach

Accelerate Espionage

Attacker stole federal background checks to construct a **massive database of individuals** with access to sensitive government information for espionage purposes.

OPM Breach

Expose World Leaders

Attacker breached documents and emails of a law firm and used them to expose **personal financial dealings** of world leaders and high-net-worth investors to pressure financial reform.

Mossack Fonseca Breach

How have FIs responded to Cyber?

How Are Financial Institution’s Responding to Cyber?

What trends are you seeing in terms of response?

Have trends been more cultural, financial, organizational, or practical ?

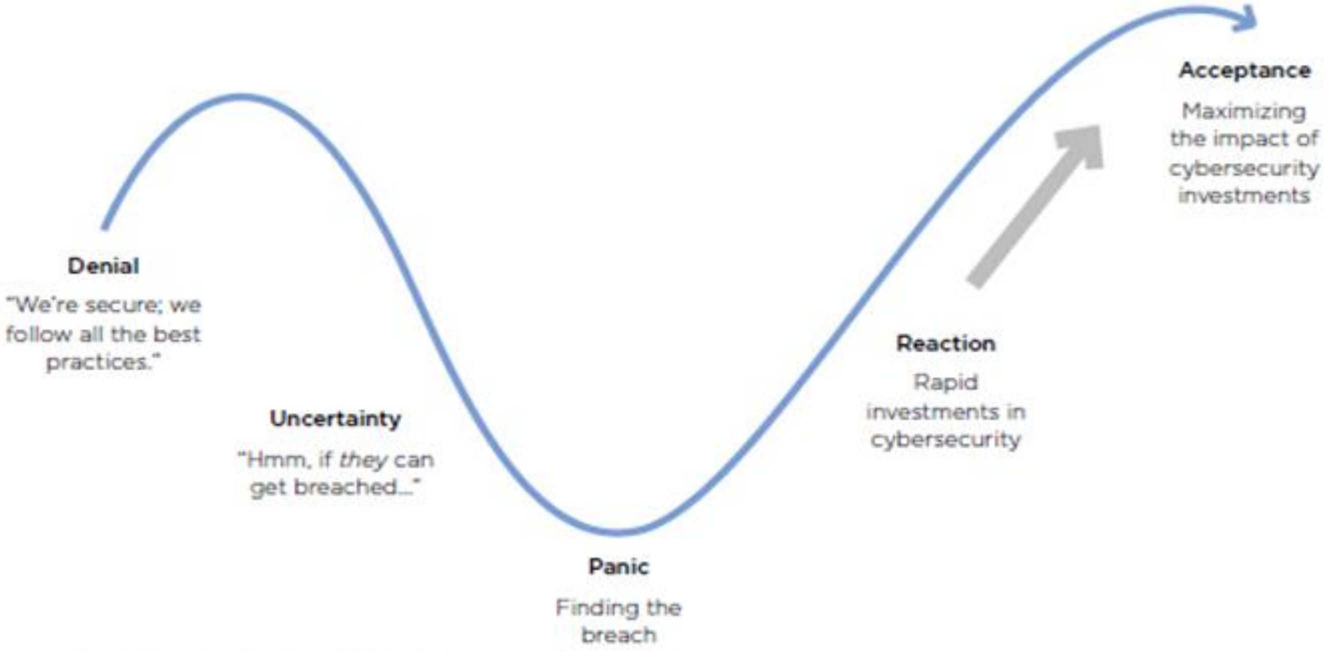
Where is improvement noted?

Where is improvement needed?

How have FIs responded to Cyber?

Culturally

Most financial institutions have accepted that cybersecurity risk can be managed, but never eliminated.


Acceptance
Maximizing the impact of cybersecurity investments
Denial
"We're secure; we follow all the best practices."
Uncertainty
"Hmm, if *they* can get breached..."
Reaction
Rapid investments in cybersecurity
Panic
Finding the breach

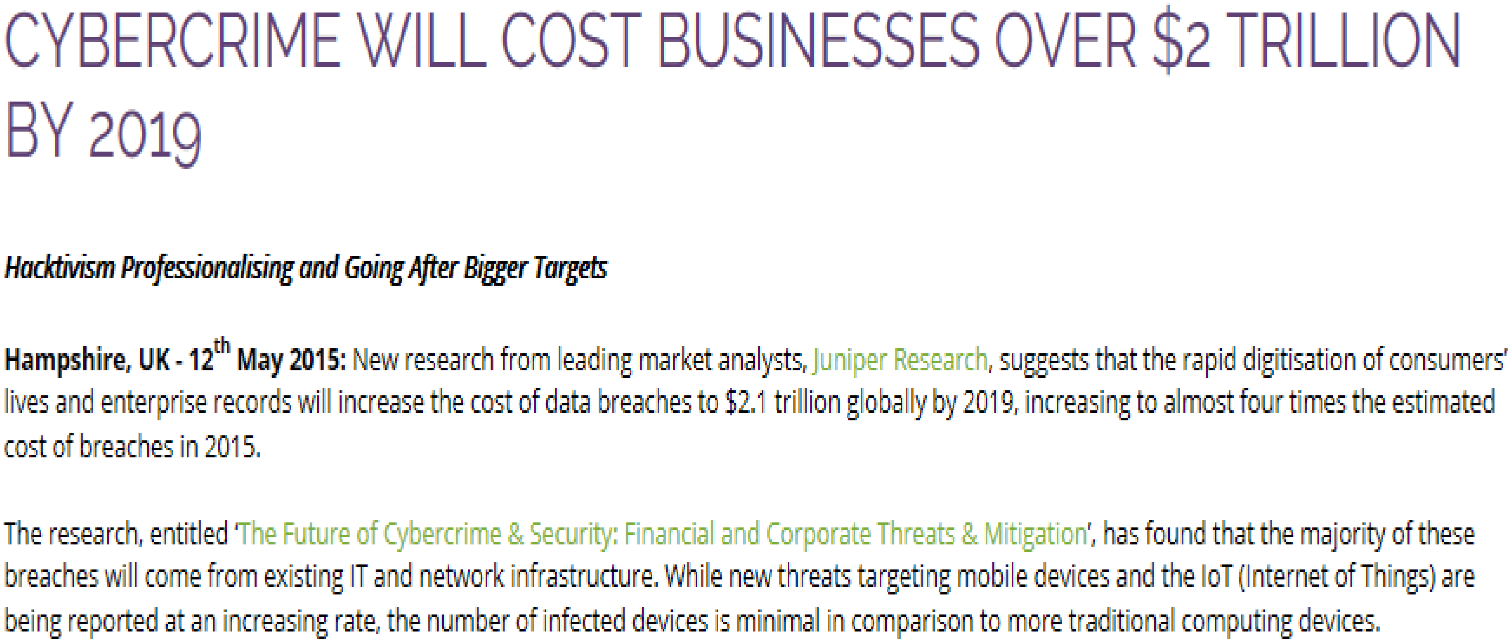
Source: CEB analysis; loosely adapted from the Kübler-Ross Model for Five Stages of Grief

Board discussions, top risk reports, strategic plans, and budgets are now showing recognition of the significant threat cybersecurity is to the financial services industry.

How have FIs responded to Cyber?

Financially

Financial institutions of all sizes and complexities are spending more on information security and all indications show that this trend will continue.



CYBERCRIME WILL COST BUSINESSES OVER $2 TRILLION BY 2019

Hacktivism Professionalising and Going After Bigger Targets

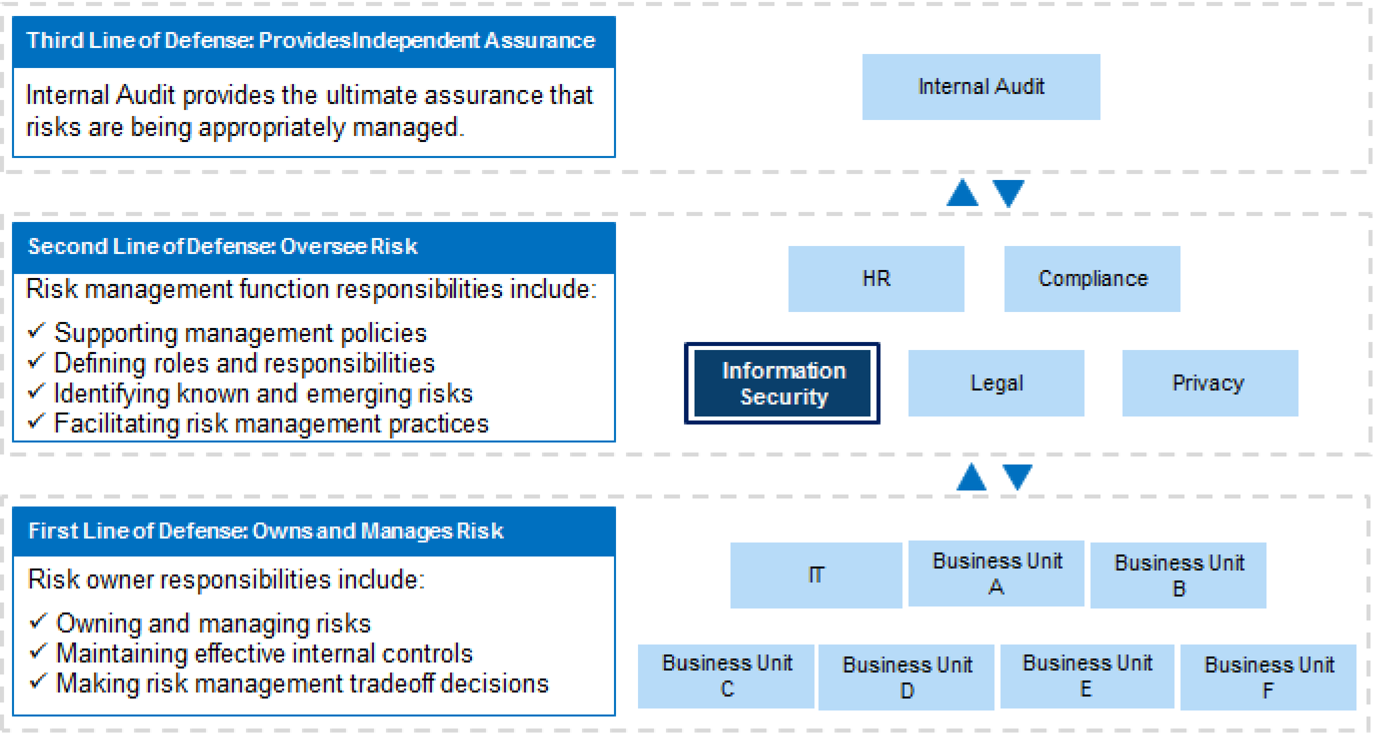
Hampshire, UK - 12th May 2015: New research from leading market analysts, Juniper Research, suggests that the rapid digitisation of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015.

The research, entitled 'The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation', has found that the majority of these breaches will come from existing IT and network infrastructure. While new threats targeting mobile devices and the IoT (Internet of Things) are being reported at an increasing rate, the number of infected devices is minimal in comparison to more traditional computing devices.

How have FIs responded to Cyber?

Organizationally

Some firms are changing their organizational structures, especially within risk and operations, to provide stature and support to cybersecurity risk management.



Third Line of Defense: Provides Independent Assurance

Internal Audit provides the ultimate assurance that risks are being appropriately managed.

Second Line of Defense: Oversee Risk

Risk management function responsibilities include:

- ✓ Supporting management policies
- ✓ Defining roles and responsibilities
- ✓ Identifying known and emerging risks
- ✓ Facilitating risk management practices

First Line of Defense: Owns and Manages Risk

Risk owner responsibilities include:

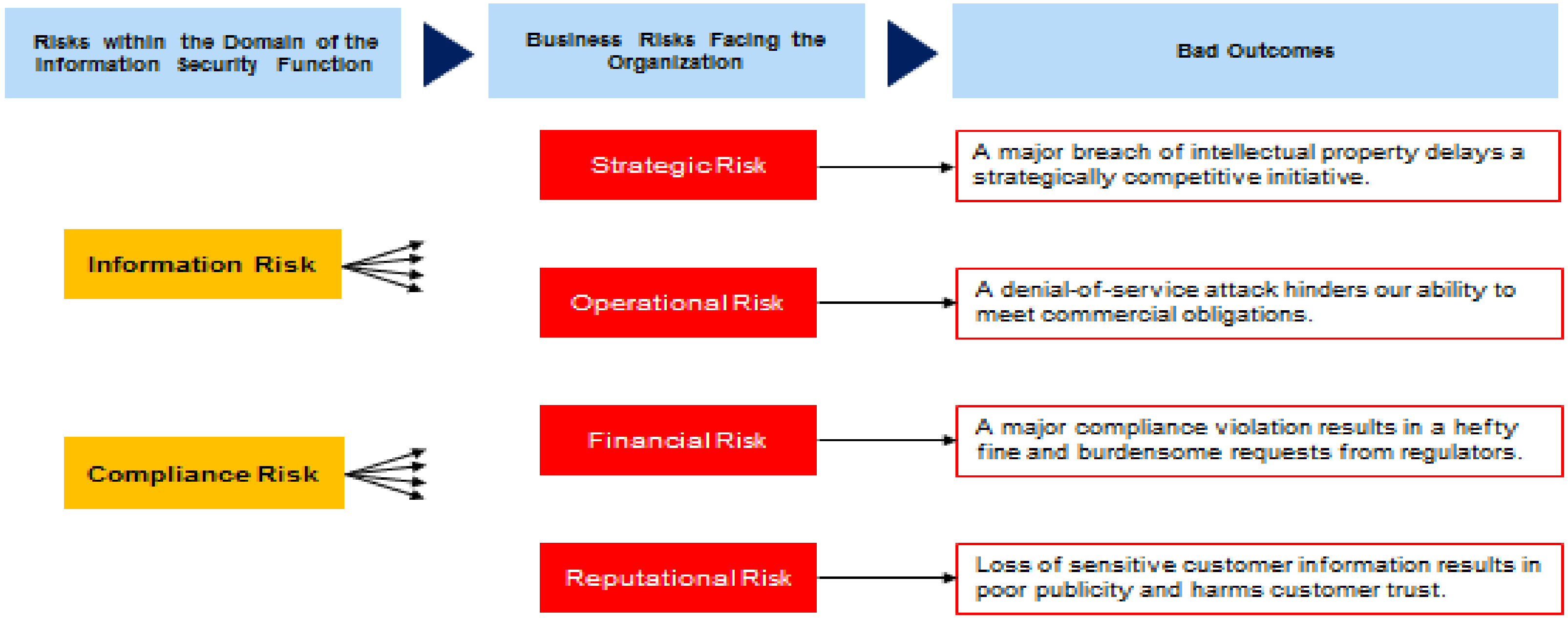
- ✓ Owning and managing risks
- ✓ Maintaining effective internal controls
- ✓ Making risk management tradeoff decisions

IT (operations) and Information Security (risk) are more commonly divided

How have FIs responded to Cyber?

Practically…

Cybersecurity risks are being considered not only from an information security or IT Risk perspective, but also through the lens of other major risk categories.



Risks within the Domain of the Information Security Function

Business Risks Facing the Organization

Bad Outcomes

Information Risk

Compliance Risk

Strategic Risk

A major breach of intellectual property delays a strategically competitive initiative.

Operational Risk

A denial-of-service attack hinders our ability to meet commercial obligations.

Financial Risk

A major compliance violation results in a hefty fine and burdensome requests from regulators.

Reputational Risk

Loss of sensitive customer information results in poor publicity and harms customer trust.

Uncontrolled cybersecurity risk can hinder a firm's ability to achieve its strategic objectives.

How have FIs responded to Cyber?

While change has been observed, the industry has room for improvement

KPMG’s 2016 Banking Outlook Survey found that 12% of the 100 Bank Executives Surveyed still do not have insight into whether their information security has been compromised by cyber attacks over the last two years.

Results from executives one or two tiers below the C-suite were even more disconnected from their institution’s cybersecurity history.

The full report: ***“The Need For Speed,”*** can be accessed at: http://www.kpmg.com/us/2016bankingindustryoutlooksurvey.

What Supervisory Tools Apply?

What tools exists that can be applied to cybersecurity supervision?

What has hindered development of more supervisory guidance in this space?

How do you currently push your institution's to employ greater cybersecurity risk management practices?

Does the nature and pervasiveness of cybersecurity risk push the industry to react without formal guidance?

What and who should drive supervisory guidance for cybersecurity?

What Supervisory Tools Apply?

Today’s Domestic Tools with Broad Applicability:

URSIT

- Interagency rating system used to assess financial institutions on IT audit, management, development and acquisition, and support and delivery.
- Focused on data security and other risk management factors ensuring quality, integrity, and resiliency of IT

FFIEC IT Handbooks

- Guidance for financial sector on IT risk, including business continuity , retail payments, and information security, which have been updated to incorporate cybersecurity expectations

Gramm-Leach-Bliley Act (GLBA)

- Act required each agency to establish controls for safeguarding of financial institution’s customer information.
- Interagency Guidelines established in 2000 outline administrative, technical, and physical control program expectations.

Sound Practices

- Intended to minimize immediate systemic effects of wide scale disruption by wide-scale disruption to critical financial markets by setting expectations for recovery capacity

What Supervisory Tools Apply?

Today’s Domestic Tools with Cyber Focus:

NIST Cybersecurity Framework

- Industry agnostic, voluntary framework to understand, manage, and reduce cybersecurity risk.
- Intended to provide a broad framework that can be customized for business sectors and organizations from any industry
- This framework also encourages better communication and awareness between business leaders and IT functions.

FFIEC Cybersecurity Assessment Tool

- Interagency, voluntary self-assessment tool that is applicable to all size institutions
- Intended to help assess cyber risk and determine preparedness of an organization
- Provides repeatable and measurable processes to determine if appropriate controls and risk management practices have been implemented relative to the firm’s risk profile.
- The CAT incorporates key concepts from NIST’s Cybersecurity Framework

What Supervisory Tools Apply?

International Guidance:

Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO)

Guidance on Cyber Resilience for Financial Market Infrastructures

- First internationally agreed guidance on cyber security for financial industry.
- Intended to add momentum and instill international consistency to industry's ongoing efforts to enhance FMI's ability to pre-empt cyber attacks, respond rapidly and effectively to them, and achieve faster and safer target recovery objectives
- The purpose was "not intended to impose additional standards on FMIs beyond those in the Principles for Financial Market Infrastructures, but provide greater detail on preparation and measures that should be taken to enhance cyber resilience to minimize the escalating threats on financial stability.

How can we supervise Cyber?

How can we supervise Cybersecurity?

- What makes you most uncomfortable about cybersecurity supervision?
- What challenges do you see in applying traditional supervisory practices?
- What risk areas do you see this impacting?
- How do you think resource and training issues can be tackled?

How can we supervise Cyber?

Broad Supervisory Considerations

Cybersecurity should be part of an institution’s ongoing ability to:

identify and manage salient risks;

maintain operations and services;

protect its customer information, safety and soundness, and reputation;

maintain public confidence;

limit, where applicable, contagion risks to the rest of the industry

These abilities should be an input into risk assessments, supervisory plans, examination procedures, and ongoing supervision programs.

How can we supervise Cyber?

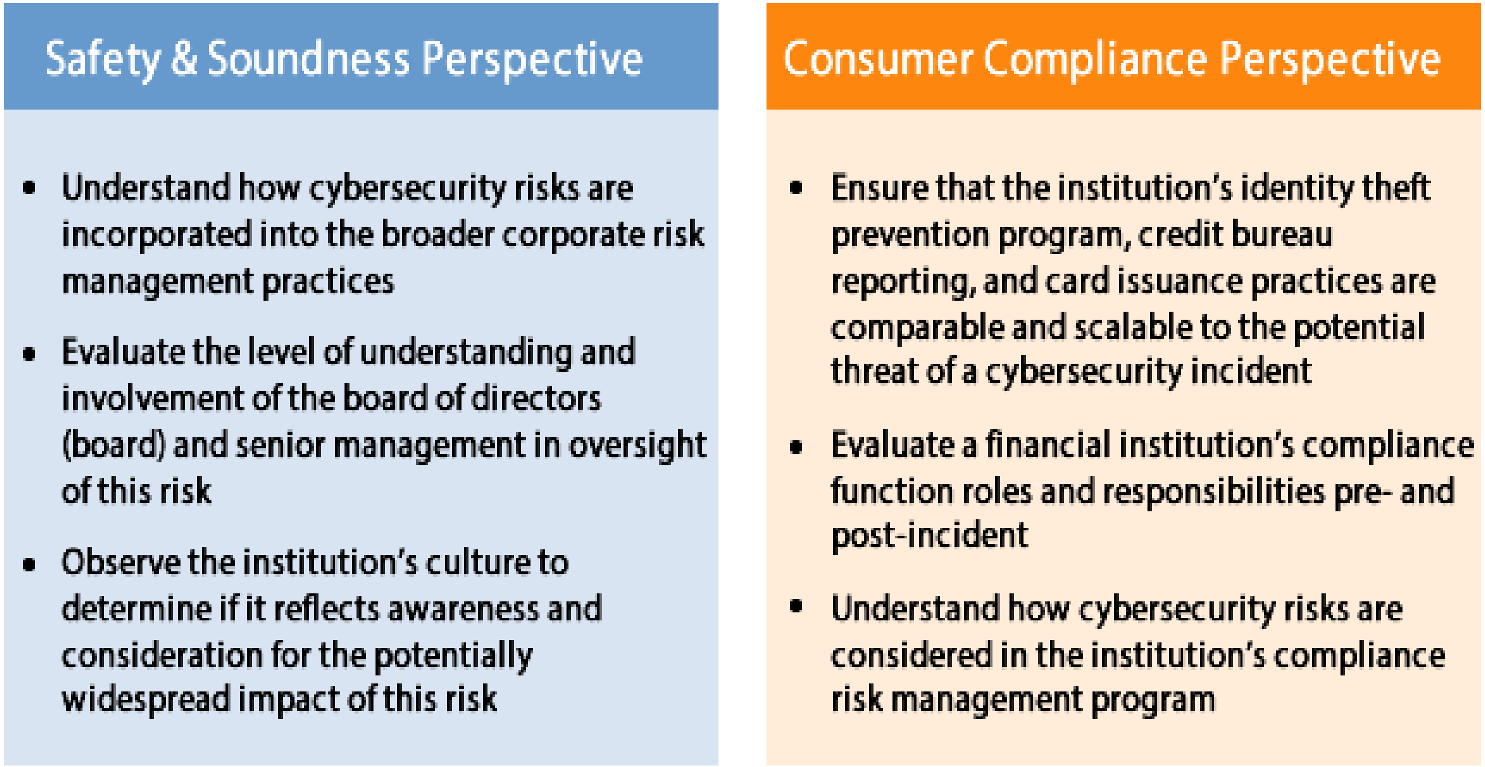
Cybersecurity/IT Focused Supervision

Portfolios	Approach
Smaller, less-complex financial institutions	• Incorporate cybersecurity risk management practices, controls, and response protocols into elements of IT examination work. • Emphasize use of risk management programs like business continuity, vendor risk management, and information security programs – including incident response, training, and issue escalation.
Larger, more-complex financial institutions	• Consider targeted work against specific topics or risk factors • Incorporate into other IT and broader Risk Management examinations • Emphasize impact on risk management programs like business continuity, incident response, vendor risk management, and information security programs and incorporate into reviews of such programs. • Remain cognizant of how cybersecurity could impact other banking programs like Enterprise Risk Management, new product/service deployment programs, operational and compliance risk focused examinations, and even Corporate Governance.

How can we supervise Cyber?

Cybersecurity in scope of integrated supervision

Cybersecurity perspectives vary, but are important across portfolios and supervisory perspectives.



Safety & Soundness Perspective

- Understand how cybersecurity risks are incorporated into the broader corporate risk management practices
- Evaluate the level of understanding and involvement of the board of directors (board) and senior management in oversight of this risk
- Observe the institution's culture to determine if it reflects awareness and consideration for the potentially widespread impact of this risk

Consumer Compliance Perspective

- Ensure that the institution's identity theft prevention program, credit bureau reporting, and card issuance practices are comparable and scalable to the potential threat of a cybersecurity incident
- Evaluate a financial institution's compliance function roles and responsibilities pre- and post-incident
- Understand how cybersecurity risks are considered in the institution's compliance risk management program

How can we supervise Cyber?

Cybersecurity transcends many other supervisory topics

Capital Planning

- Determine if the risk profile necessitates consideration of cyber events as Idiosyncratic risk or stress scenarios

Compliance

- Recognize the extensive legal and reputational impacts of a cyber events
- Understand implications of consumer compliance laws for reissuance of and restitution for credit cards, identity theft monitoring, and customer notification protocols
- Consider how vendor risk management especially where customer information resides with a 3rd party are managed.

Liquidity Management

- Recognize cybersecurity events have the potential to paralyze clearing and settlement systems, delete or corrupt client data, or simply make websites unavailable.
- Determine if contingency funding plans account for events of sizable scope and duration

Enterprise Risk Management

- Review risk identification and aggregation practices to see how they account for potential interplay between cyber and other risk stripes
- Understand escalation protocols and reporting lines for cyber events and ongoing risk management

Audit

- Evaluate and understand how audit incorporates new and emerging risks and technologies.

How can we supervise Cyber?

Ongoing Supervision Considerations

- **ERM reporting**: Risk reports to the board and senior management highlighting top risks may provide insight into the institution's awareness, level of concern, and approach/actions to mitigate cybersecurity risk.

- **Board discussions**: Information conveyed to the board often influences budget and strategic decisions. The inclusion of cybersecurity in such discussions can be an informative perspective into the institution's preparedness and ultimate response.

- **Scenario selection**: Scenarios are a widely used risk management tool across a variety of risk categories and can be a good indication of management's mindset if they include cybersecurity. Regardless of an institution's size or complexity, some forms of scenarios are likely used. Scenarios that might consider cybersecurity could be related to business resumption/disaster recovery, liquidity risk management, capital planning, or even in living wills or recovery/resolution planning.

- **Audit reports**: Whether a broad-based IT audit report from a community bank or a cybersecurity strategy audit from an larger audit department, such reports can provide valuable information on an institution's preparedness for and resilience to cyber attacks that could influence changes to the institution's risk profile.

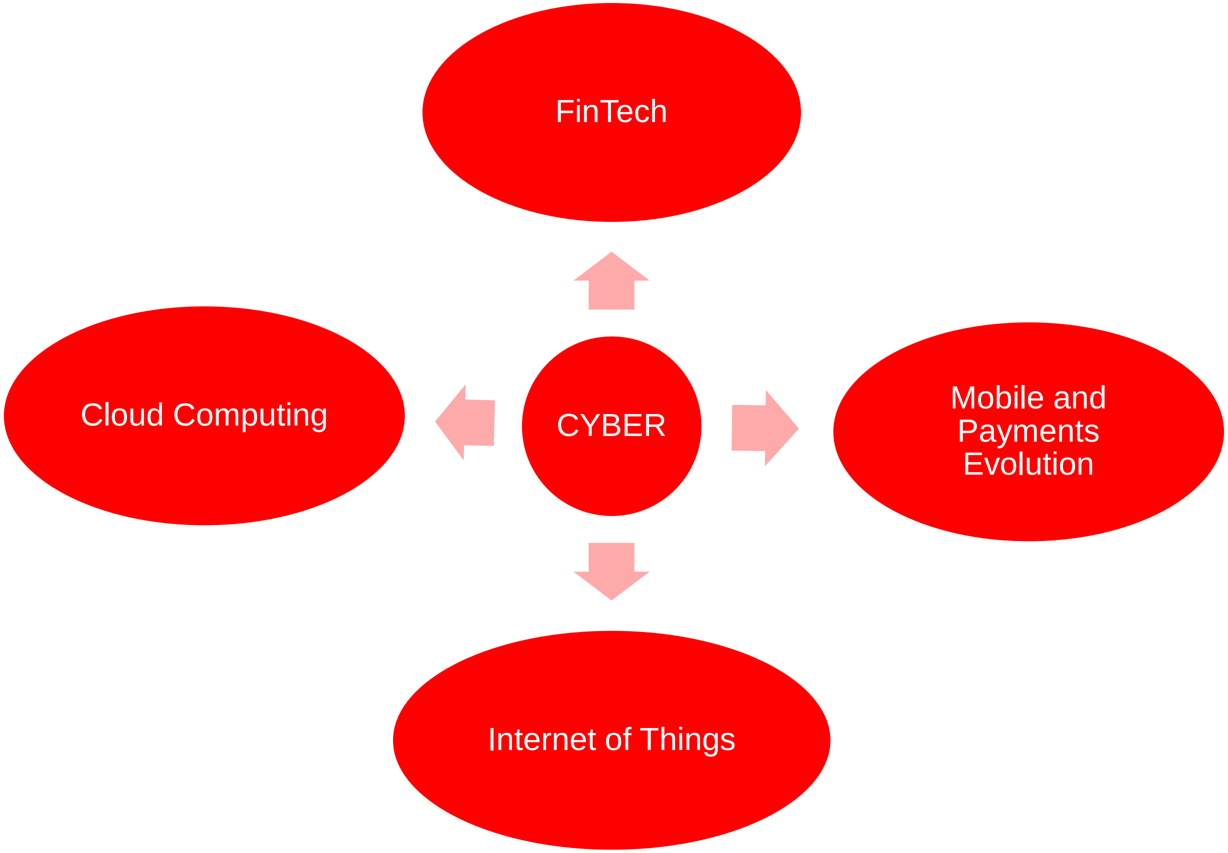
- **Press releases**: Often these could be our first indication that there is an incident that directly or indirectly affects an institution. Publically available information could also provide details to help guide conversations with supervised institutions.

While in no way an exhaustive list, the connections or impact points that cybersecurity risk has across many facets of a financial institution are vast and there are many information sources to consider in the development of an institution's overall risk profile.

How can we supervise Cyber?

Impact of Emerging Technologies and Ventures

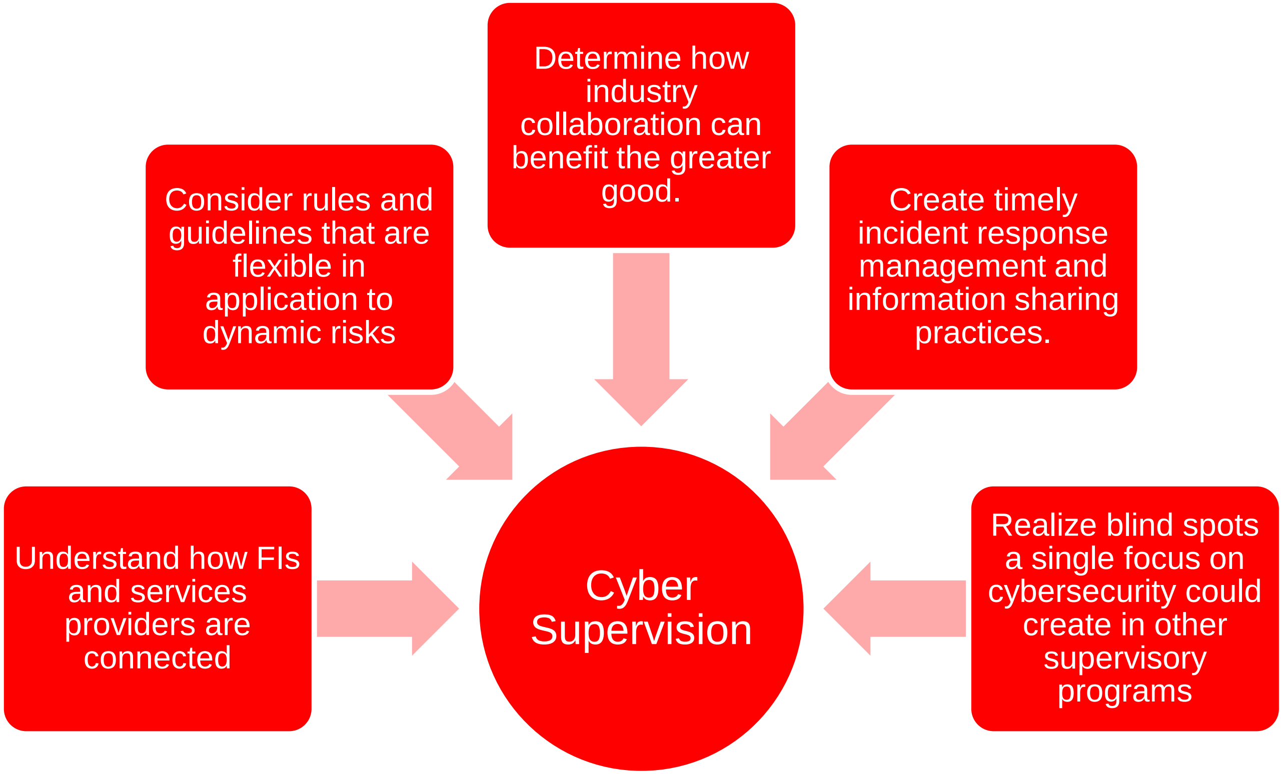
Our supervisory roles will continue to be challenged as cybersecurity risk has a correlation to many of today's financial sector trends.



How can we supervise a moving target?

Supervision of Cybersecurity

Unconventional and unique supervisory practices may need to be considered in order to effectively ensure the safe and soundness of the financial services sector in today's world.



Cyber Supervision

Determine how industry collaboration can benefit the greater good.

Consider rules and guidelines that are flexible in application to dynamic risks

Create timely incident response management and information sharing practices.

Understand how FIs and services providers are connected

Realize blind spots a single focus on cybersecurity could create in other supervisory programs