BOARD OF GOVERNORS *of the* FEDERAL RESERVE SYSTEM

Oversight of Cybersecurity in the Financial Regulatory System

Seminar for Senior Bank Supervisors from Emerging Economies

Matthew Hayduk, Manager, Federal Reserve Board

October 26, 2018

Disclaimer

The views expressed in this presentation are my own and do not represent the official positions of the Federal Reserve Board of Governors. The presenter makes no representation or warranty, express or implied, with respect to the accuracy, reasonableness or completeness of any of the information contained herein, including, but not limited to, information obtained from third parties.

Frequently Asked Questions

- How are Information Technology, cybersecurity, information security and operational risk different?
- Which international standards and regulations are preferred for evaluating cybersecurity?
- Is the preference to create a new cyber risk management regulation or incorporate into current IT risk management regulations?
- What methodology is best to conduct a cybersecurity evaluation?
- What tools do you use in a cybersecurity evaluation?
- What is your opinion of outsourcing to the cloud?
- Apart from a monitoring capability, what are the most important areas supervised entities should establish to manage the risk of cyber attacks?
- What responsibility does the supervisory body have regarding cyber attacks that have impacted their supervised entities?

Agenda Topics

- Cyber Landscape
- Risk Mitigation
- Regulatory and Supervisory Practices
- Looking Ahead

Cyber Landscape

Current State of Cybersecurity

- Cyber Security – Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

  Source: Adapted from ISO/IEC 27032:2012

- Cyber Risk – The combination of the probability of cyber incidents occurring and their impact.

  Source: Adapted from CPMI-IOSCO, ISACA Fundamentals (definition of "Risk") and ISACA Full Glossary (definition of "Risk")

- Cyber Threat – A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security.

  Source: Adapted from CPMI-IOSCO

Source: Financial Stability Board Draft Cyber Lexicon

Current State of Cybersecurity

- The rise in frequency and sophistication of cyber threats can be attributed to various types of threat actors.
- Retail financial institutions and their customers are primary targets for financially-motivated cybercriminals.
- Existing vulnerabilities continue to be exploited while new variants are becoming more prevalent.
- Lack of basic cyber hygiene is a large contributing factor in successful cyber breaches and incidents.

Technology and Financial Services

- Supply and demand factor are affecting an increasing range of activities in banking and finance.
  - Mobile banking
  - Cloud computing
  - Shadow IT
  - Outsourcing

- Hyper-connected ecosystem – New capabilities enabled by these technologies are driving new products and services for customers.

- FinTech and BigTech – New firms and business partnerships with firms not traditionally part of the financial services ecosystem are offering financial products and services.

The New Digital Ecosystem and Cybersecurity

- Accelerated evolution of technology (e.g., cloud, IOT, AI, blockchain, quantum computing, …) combined with legacy technology.
- Increased importance and visibility of data.
- Disappearance of boundary between the enterprise and the “outside” world.
- Increased interconnectivity and interdependencies.

Innovation and Cybersecurity

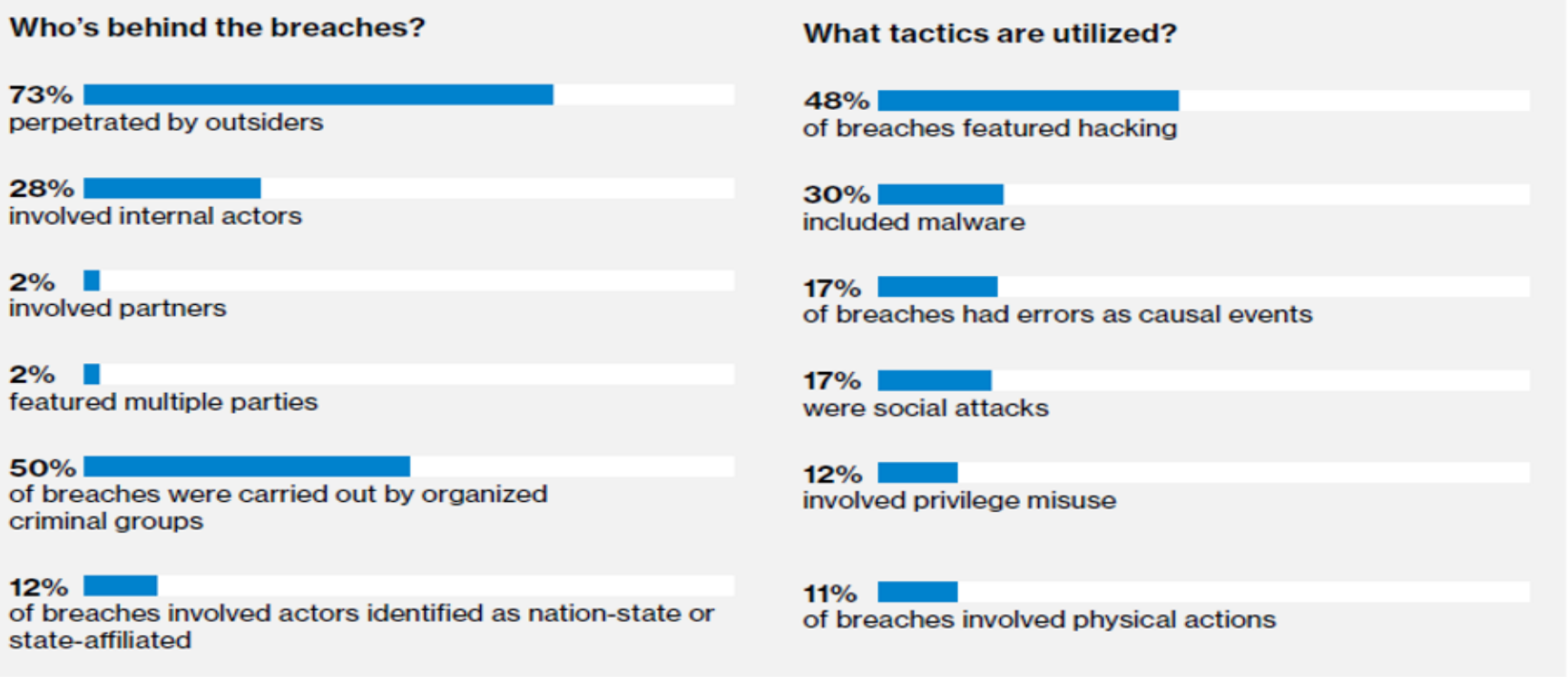
- Technology advances can increase a financial institution's customer base and bottom line but also increases risks associated with cyber theft, fraud, and potential impacts of disruptions.
- New platforms create new risks and vulnerabilities.
- Cyber incidents may result in financial, legal and reputational costs.
- Increased reliance on technology impacts the interconnectedness and interdependencies between institutions, which increases the potential for systemic risk to the financial system.

Cyber Incidents and Breaches Across Sectors

	Incidents				Breaches			
	Large	Small	Unknown	Total	Large	Small	Unknown	Total
Accommodation (72)	40	296	32	368	31	292	15	338
Administrative (56)	7	15	11	33	5	12	1	18
Agriculture (11)	1	0	4	5	0	0	0	0
Construction (23)	2	11	10	23	0	5	5	10
Education (61)	42	26	224	292	30	15	56	101
Entertainment (71)	6	19	7,163	7,188	5	17	11	33
Financial (52)	74	74	450	598	39	52	55	146
Healthcare (62)	165	152	433	750	99	112	325	536
Information (51)	54	76	910	1,040	29	50	30	109
Management (55)	1	0	1	2	0	0	0	0
Manufacturing (31–33)	375	21	140	536	28	15	28	71
Mining (21)	3	3	20	26	3	3	0	6
Other Services (81)	5	11	46	62	2	7	26	35
Professional (54)	158	59	323	540	24	39	69	132
Public (92)	22,429	51	308	22,788	111	31	162	304
Real Estate (53)	2	5	24	31	2	4	14	20
Retail (44–45)	56	111	150	317	38	86	45	169
Trade (42)	13	5	13	31	6	4	2	12
Transportation (48–49)	15	9	35	59	7	6	5	18
Utilities (22)	14	8	24	46	4	3	11	18
Unknown	1,043	9	17,521	18,573	82	3	55	140
Total	**24,505**	**961**	**27,842**	**53,308**	**545**	**756**	**915**	**2,216**

Source: 2018 Verizon Data Breach Investigation Report

Breaches in the Financial Sector



Source: 2018 Verizon Data Breach Investigation Report

Cyber Threats and Vulnerabilities

- Advanced Persistent Threats (APTs) – Cyber Crime / Large Scale Cyber Attacks
- New and Evolving Malware
- Social Engineering – Identity Theft / Data Breaches
- Software Development Vulnerabilities
- End-Point Security / Chip Vulnerabilities
- Interconnectedness Risks – 3rd and 4th Party Risks / Broader Infrastructure Failures

The Increasing Role of Threat Intelligence

- Financial regulators and supervisors require a Security Operations Center (SOC), Security Incident Response Team (CSIRT) and Cyber Analytics capabilities, as appropriate, to monitor, assess and respond to cyber threats in their regulated community.

- Financial institutions, depending on their size and complexity, should consider establishing internal threat intelligence teams that monitor the cyber threat landscape and share with their peer groups.

- Since smaller banks sometimes lack internal resources to maintain awareness of cyber threats, they can participate in cyber information sharing efforts such as the Financial Services – Information Sharing and Analysis Center (FS-ISAC).

- While it is sometimes hard to get actionable information declassified, government agencies often work with the sector to disseminate actionable intelligence to the sector.

Risk Mitigation

Cyber Risk Mitigation

- 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.

Identify, Protect and Detect

- Know Your Connections
  - Identify critical functions, activities, products and services, including interconnections, dependencies and third parties.
  - Prioritize their relative importance and assess their respective cyber risks. Identify and implement security controls – including systems, policies, procedures and training – to protect against and manage those risks within the tolerance set by the governing authority.

- Adopt Layered Security Defenses
  - Identify, classify and protect critical assets, systems and data.
  - Establish systematic infrastructure, systems and data monitoring capabilities to rapidly detect cyber incidents.
  - Periodically evaluate the effectiveness of controls, including enterprise architecture, network and infrastructure monitoring, secure software development, infrastructure configuration testing, audits and exercises.

- Leverage Threat Intelligence Capabilities
  - Institutions are increasingly leveraging threat intelligence built on peer relationships and public-private partnerships to remain responsive to emerging threats.

Response and Recovery

- Engage in Public-Private Collaboration
  - Engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector) on threats, vulnerabilities, incidents and responses to enhance defenses, limit damage, increase situational awareness and broaden learning.

- Respond Quickly
  - Assess the nature, scope, and impact of a cyber incident; contain the incident and mitigate its impact; notify internal and external stakeholders (such as law enforcement, regulators and other public authorities, as well as shareholders, third-party service providers and customers as appropriate); and coordinate joint response activities as needed.

- Resume Operations Responsibly
  - Allow for continued remediation, including by eliminating harmful remnants of the incident; restoring systems and data to normal and confirming normal state; identifying and mitigating all vulnerabilities that were exploited; remediating vulnerabilities to prevent similar incidents; and communicating appropriately internally and externally.

Regulatory and Supervisory Practices

Governance and Preparedness

- Strengthen Cybersecurity Governance:
  - Establish clear and effective 3 lines of defense risk management structure.
  - Clearly define roles and responsibilities for staff implementing, managing and overseeing the effectiveness of the cybersecurity strategy and cybersecurity framework to ensure accountability.
  - Provide adequate resources, appropriate authority, and access to the governing authority (e.g., board of directors or senior officials at public authorities).
  - Establish a clear separation of concern along the 3 lines of defense model for risk, audit and operations.

- Ensure Cyber Resilience Readiness
  - Review the cybersecurity strategy and framework and controls regularly and when events warrant — including cybersecurity governance, risk and controls assessments, monitoring, response, recovery and information sharing components — to address changes in cyber risks, allocate resources, identify and remediate gaps and incorporate lessons learned.

- Test Cyber Resilience Readiness
  - Assess cyber resilience readiness by executing cybersecurity incident drills, business continuity and disaster recovery exercises and tabletop exercises to stress-test organizational cyber resilience readiness.
  - Based on risk, consider the use of Threat Led Penetration Testing (TLPT) where appropriate.

Standards, Regulations and Guidance

- ISO/IEC 27001 family of standards
- National Institute of Standards Cybersecurity Framework (CSF) and Special Publications
- U.S. Federal Banking Agencies Advanced Notice of Proposed Rulemaking for Enhanced Cyber Risk Management Standards
- Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO) Guidance on Cyber Resilience for Financial Market Infrastructures
- G-7 Fundamental Elements of Cybersecurity for the Financial Sector
  - Fundamental Elements for Threat-led Penetration Testing and Third Party Cyber Risk Management
  - G-7 Cyber Incident Response Protocol, Cross-Sector Coordination and Cross-Border Coordination Exercise

Additional Regulations and Guidance

- 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.

- Bank Service Company Act (BSCA)
  - Provides U.S. Federal Banking Agencies authority to examine services provided to banking institutions.

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

Supervisory Approaches

Portfolios	Approach
Smaller, less-complex financial institutions	• Incorporating cybersecurity risk management practices, controls, and response protocols into elements of our IT examination framework. • Heavy emphasis placed on business continuity, vendor risk management, and information security programs – including incident response, training, and issue escalation.
Larger, more-complex financial institutions	• Addressing cybersecurity through horizontal targets across various portfolios and activities. • Still a consideration in other IT and broader Risk Management examinations, but targets are more prominent given risk profile. • Also focus on business continuity, incident response, vendor risk management, and information security programs. • Other considerations in this portfolio include Enterprise Risk Management, new product/service deployment programs, operational and compliance risk focused examinations, and even Corporate Governance.

Examination Guidance

- Uniform Rating System for IT
  - Interagency rating system used to assess financial institutions on IT audit,, 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 Examination Handbook
  - Risk-Based Assessment Process
  - Demonstrate appropriate oversight and controls of cyber risk governance; cyber risk management; internal dependency management; external dependency management; and incident response, resilience, and situational awareness.

- IT Examination Procedures and Work Programs
  - Management
  - Information Security
  - Operations, Infrastructure and Architecture
  - Development and Acquisition
  - Outsourcing Technology Services
  - Retail and Wholesale Payment Systems
  - Business Continuity Planning
  - Audit

Tools and Best Practices

- FFIEC Cybersecurity Assessment Tool
- Financial Services Sector Cybersecurity Profile
- Public / Private Partnerships
  - Cybersecurity Exercises with Government and Industry Stakeholders
  - Education of Boards of Directors, Management, Business Partners, Vendors, Customers and Consumers
  - Staff and Examiner Training

Looking Ahead

How should we think about Cyber?

Cybersecurity transcends other supervisory areas

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

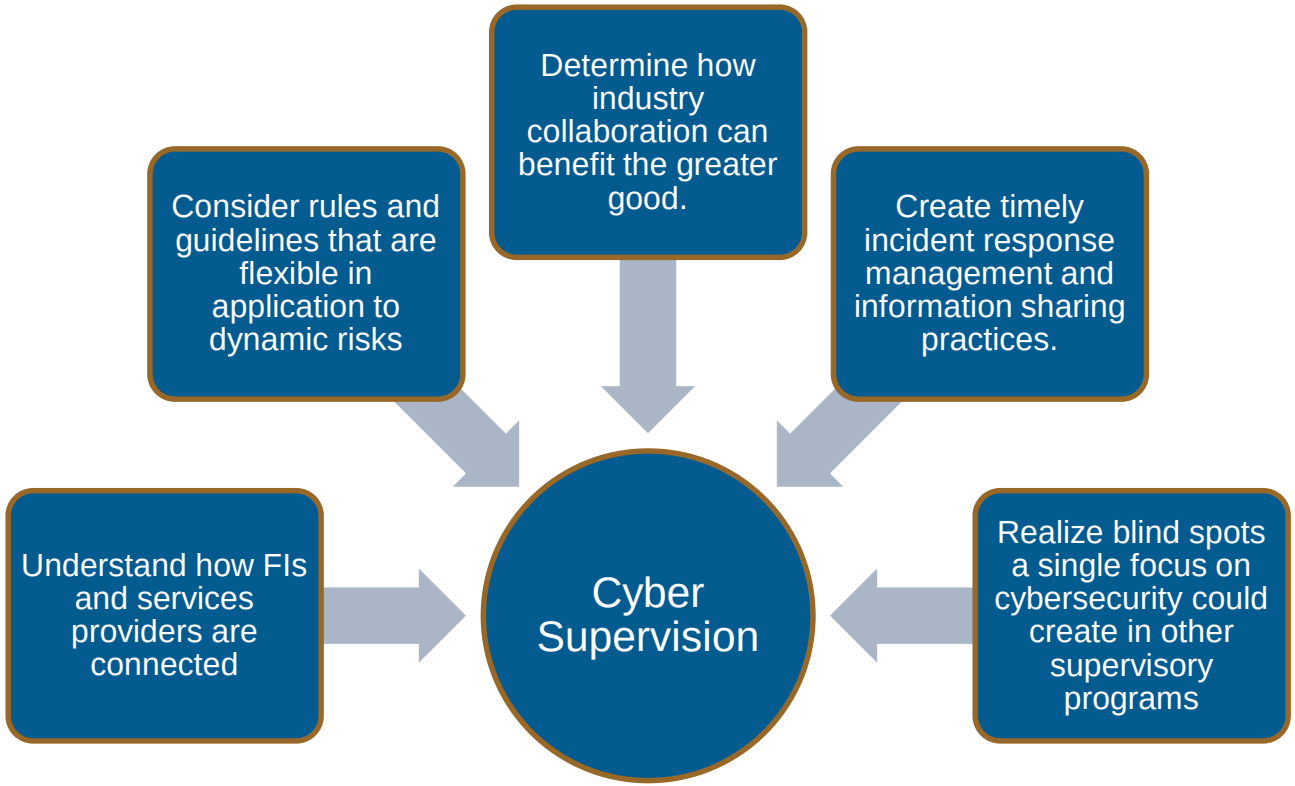
- Review risk identification and aggregation practices to see how they account for potential interplay between cyber and other risk stripes.
- Understand escalation protocols and reporting lines for cyber events and ongoing risk management.

Audit

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

Supervision

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



Cyber Resilience

The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

Source: Adapted from CERT Glossary (definition of "Operational resilience"), CPMI-IOSCO and NIST (definition of "Resilience")

Operational Resilience

+ Reliability
+ Redundancy
+ …

= Resilience

Global Trends 2030 – Alternative Worlds

"Extrapolations of the megatrends would alone point to a changed world by 2030—but the world could be transformed in radically different ways. We believe that six key game-changers—questions regarding the global economy, governance, conflict, regional instability, ***technology****, and the role of the United States—will largely determine what kind of transformed world we will inhabit in 2030. Several potential Black Swans—discrete events—would cause large-scale disruption…"*

https://www.dni.gov/files/documents/GlobalTrends_2030.pdf

Financial Services and Public Policy

"This industry is evolving at a sometimes breathtaking pace. The resulting changes require all of us to frequently revisit our assumptions, views and policies and sometimes to revise those assumptions, views and policies in order to continue to achieve the unchanging objectives of a sound and competitive financial system."

-- Governor Mark W. Olson, 2002

Contact Information

Matthew Hayduk
Manager, Systems & Operational Resilience Policy
Division of Supervision & Regulation
Federal Reserve Board of Governors
Washington, DC

Matthew.E.Hayduk@frb.gov