Superintendencia de Bancos
Guatemala, C. A.

Cybersecurity in the Financial Services Sector

Matthew Hayduk, Manager
Division of Supervision and Regulation
Federal Reserve Board of Governors – Washington, D.C.

The views and opinions expressed in this presentation are my own and do not represent the official positions of the Federal Reserve Board of Governors. The Federal Reserve and the speaker make 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.

Cyber Landscape

The new digital ecosystem

- 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.

Cyber Landscape

Technology in financial services

- Supply and demand factor are affecting an increasing range of activities in banking and finance.
  - Mobile banking
  - Cloud computing
  - Shadow IT
  - Outsourcing
- New capabilities enabled by these technologies are driving new products and services for customers.
  - Hyper-connected ecosystem
- New firms and business partnerships with firms not traditionally part of the financial services ecosystem are offering financial products and services.
  - FinTech and BigTech

Cyber Landscape

Innovation in the financial ecosystem

- 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 Threats

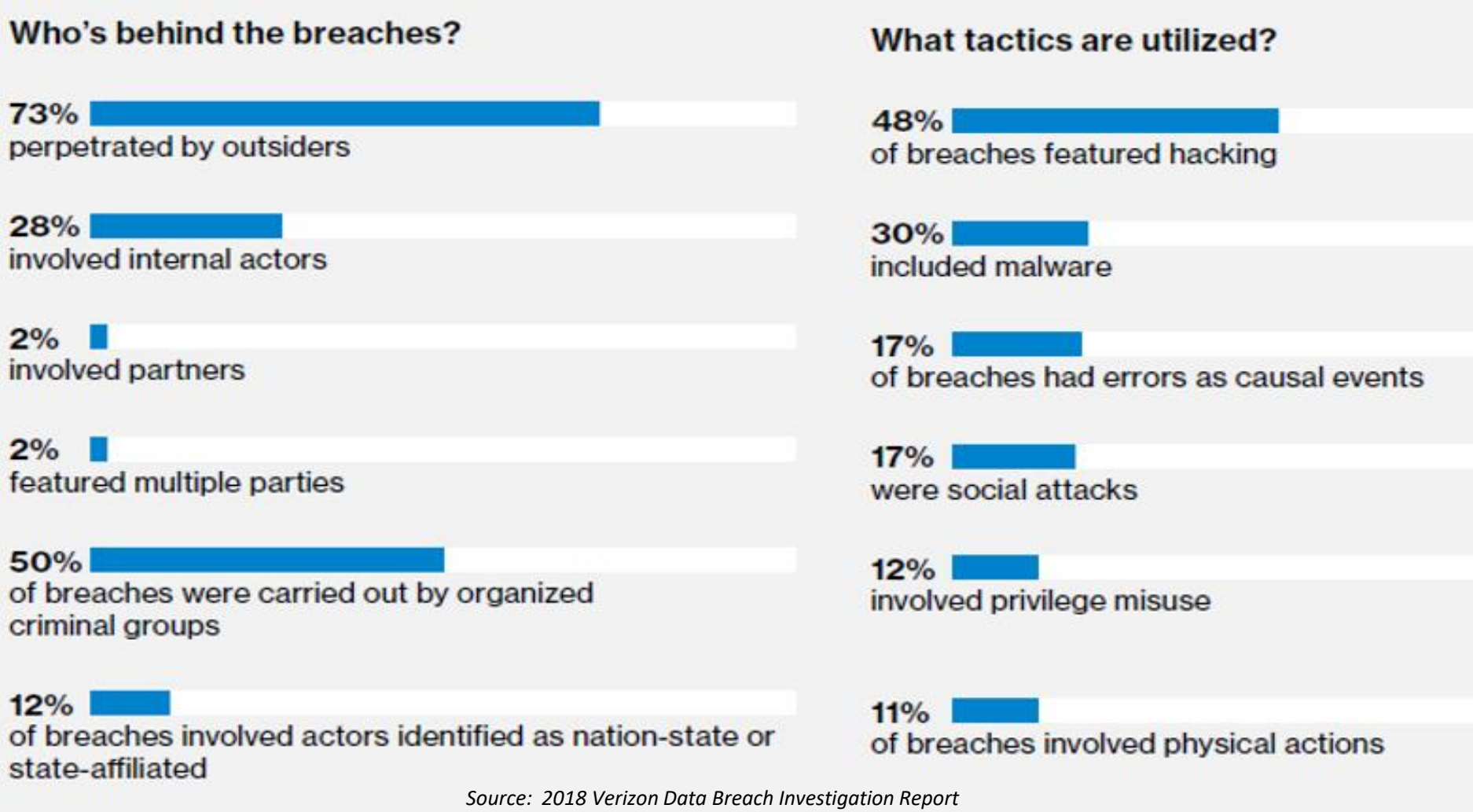
Incidents and breaches across sectors

	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

Cyber Threats

Breaches in the financial sector



Source: 2018 Verizon Data Breach Investigation Report

Cyber Threats

The 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.
- Lack of basic cyber hygiene is a large contributing factor in successful cyber breaches and incidents.

Cyber Threats

Threats, risks and vulnerabilities

- **Advanced Persistent Threats (APTs) – Cyber Crime / Large Scale Cyber Attacks**
  - Sophisticated hackers, hacktivists, and nation state groups that display a high level of technical expertise.
  - Highly coordinated and well resourced.
  - Longer dwell time in network increases ability to cause damage while going undetected.*
- **New and Evolving Malware**
  - Threat actors and malware developers are constantly developing new malware and developing new variants of known malware to increase capabilities and tailor for specific targets.

** Dwell time represents the number of days that a threat "lives" in a system before detection or ultimate remediation*

Cyber Threats

Threats, risks and vulnerabilities

- **Social Engineering – Identity Theft / Data Breaches**
  - A tactic, often relying on human interaction, to bypass cyber security standards.
  - Often non-technical and allow threat actors to gain authorized access to network.
- **Software Development Vulnerabilities**
  - Threat actors are constantly developing new tactics, techniques, and processes to exploit security flaws in poorly developed software.

Cyber Threats

Threats, risks and vulnerabilities

- **End-Point Security / Chip Vulnerabilities**
  - Proliferation of end-point devices (IoT) whose security is not well understood, not well configured, or not well-hardened.
  - New class of chip vulnerabilities that exploit the fundamental design of processors.
  - Fileless attacks are growing at an alarming rate (malware is stored in the RAM to evade detection).
  - *Meltdown* and *Spectre* were the first identified chip vulnerabilities, but new chip vulnerabilities are being discovered regularly.

- **Interconnectedness Risks – 3rd and 4th Party Risks / Broader Infrastructure Failures**
  - Multiple vendors, business partners and other parties (e.g., software developers) create more opportunities for threat actors and malware to gain access.
  - Supply chain compromises throughout the value chain.
  - Cross sector dependencies increasing risks.

Cyber Mitigation

The role of boards of directors and management

- Maintain investments in IT infrastructure to ensure that systems are fully supported by vendors and that they incorporate effective security and resiliency solutions.
- Ensure there is a complete inventory of applications and connections to the Internet and incorporate these dependencies into operational resiliency plans that are tested regularly and as threats change.
- Stay informed and act on timely information regarding vulnerabilities and mitigations.
- Enhance oversight of outsourced service providers and vendors, including their cybersecurity risk management programs and tests of contingency plans and operations.

Cyber Mitigation

The expanding role of the CISO

- **Assess Cybersecurity Risks:** Keep senior leadership and the board of directors updated regularly on cybersecurity risks and ensure effective cybersecurity measures are a top priority.
- **Implement Cybersecurity Programs:** Implement effective cybersecurity risk management programs and frameworks. Although there is no authoritative framework for cybersecurity in the financial sector, 91% of all companies that have adopted a standard security framework have either adopted NIST CSF or ISO/IEC 27001/27002.*

** Source: Survey conducted by FS-ISAC of CISOs of member organizations in 2018.*

*"The role of the modern day CISO is to provide the leadership and guidance necessary for an organization to manage the risks to the confidentiality, integrity and availability of the organization's intellectual property and information technology assets."***

Source: Infosec Today

Cyber Mitigation

The expanding role of the CISO

- **Promote Cybersecurity Awareness Culture:** Establish cybersecurity training programs and promote cybersecurity awareness.
- **Balance Competing Priorities:** CISOs surveyed were split on their top priorities for securing their organizations against cyberattacks.*
  - 35% said that employee training is a top priority for improving security posture in the financial sector.
  - 25% said that infrastructure upgrades and network defense are the top priority.
  - 17% said that breach prevention is the top priority.

** Source: Survey conducted by FS-ISAC of CISOs of member organizations in 2018.*

*"The role of the modern day CISO is to provide the leadership and guidance necessary for an organization to manage the risks to the confidentiality, integrity and availability of the organization's intellectual property and information technology assets."***

Source: Infosec Today

Cyber Mitigation

The increasing role of threat intelligence

- 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.

Cyber Risk Management

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.

Cyber Risk Management

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.

Cyber Risk Management

Respond and recover

- **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:** Timely (a) assess the nature, scope, and impact of a cyber incident; (b) contain the incident and mitigate its impact; (c) 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 (d) coordinate joint response activities as needed.

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

Cyber Resilience

Addressing growing cyber risks

- Basic cyber hygiene is fundamental in protecting an organization's assets and detecting cyber incidents.
- Sound risk management practices set the foundation and enable institutions to be better prepared when impacted by a cyber attack.
- Information sharing with other institutions across the financial services industry and with other critical infrastructure is a crucial component of effective cyber defense.
- Increased emphasis on cyber resiliency is needed, which is a key component of an institution's cybersecurity preparedness.

Cyber Resilience

Preventing or minimizing disruptions

Operational Readiness which includes an assessment of an institution's cybersecurity controls and governance is an important step towards improving its ability to identify, detect, respond, recover and reduce the impact of cyber incidents.

- ✓ Establish clear operational availability and operational readiness objectives.
- ✓ Set and communicate operational readiness objectives, manage expectations and establish operational readiness processes at all levels of the organization.
- ✓ Develop well defined cybersecurity incident management and response procedures and communication plans (playbooks / protocols).
- ✓ Maintain and continue to update a diverse set of operational resilience best practices to ensure operational readiness capabilities that include people, processes and culture.
- ✓ Report early, clearly and objectively operational disruption findings caused by cybersecurity incidents, and formulate concrete remedial actions.
- ✓ Ensure cybersecurity operational readiness assessments are reliable and fair.
- ✓ Develop an after action plan and ensure follow up and implementation of mitigating controls.
- ✓ Report cybersecurity incidents to your regulator and law enforcement agencies.

Cyber Resilience

Implementing a layered security approach

- **Layered security controls include but are not limited to the following:**
  - ✓ **Access and Identity Management:** Implement the principle of least privilege, including protection of administrative privilege, to combat compromise of administrative credentials and establishment of persistence.
  - ✓ **Multifactor Authentication:** Implement rigorous authentication and authorization processes for high value assets to combat credential theft.
  - ✓ **System and Network Segmentation**: Implement the principle of least access to combat lateral movement.
  - ✓ **Endpoint Security:** Implement detection and mitigation of anomalous system behavior to help combat malware.
  - ✓ **Data Encryption:** Implement data encryption at rest and in transit to reduce the risk of data theft.
  - ✓ **Secure Software Assurance:** Implement a secure software assurance program to mitigate the threat of exploitation of software vulnerabilities.

Cyber Resilience

Mitigating growing cyber risks

- **Advanced Persistent Threats (APTs)**
  - Monitoring for application & infrastructure changes, data access attempts and data transfers.
  - Early identification is key to minimize damage (suspicious connections, emails, traffic, etc.).
  - Data encryption at rest and in transit.
  - Robust incident management planning.
  - Proactive threat intelligence / monitoring of alerts.
  - Backups (online and offline).
  - Emergency response and recovery readiness

- **Insecure 3rd / 4th Party Services**
  - Legal agreements with clear SLAs and NDAs governing 3rd party services, including the use of 4th party service providers.
  - Cybersecurity assurance prior to establishing integration of 3rd party services.
  - Testing and patch management.
  - Proactive threat intelligence before compromise.
  - Robust incident management planning.
  - Backups (online and offline).

Cyber Resilience

Mitigating growing cyber risks

- **Social Engineering**
  - Training and testing for awareness and prevention.
  - Layered defense coupled with identity and access management.
  - Threat intelligence for informing users about current social engineering lures and tactics, techniques and procedures (TTPs).
- **End-Point Security (IoT) / Chip Vulnerabilities**
  - Asset management to ensure awareness of hardware and software components and weigh the risks of the components appropriately.
  - Patch management.
  - Vulnerability assessment and penetration testing.
  - Threat intelligence and vulnerability management.

Cyber Resilience

Mitigating growing cyber risks

- **New and Evolving Malware**
  - Prevention through user training and up to date anti-virus software.
  - Patch management.
  - Proactive threat intelligence.
  - Robust incident management planning.
  - Monitoring Cyber alerts.

- **Software Development Vulnerabilities**
  - Prevention through secure coding programs.
  - Penetration testing and scanning for software vulnerabilities.

Superintendencia de Bancos
Guatemala, C. A.

XXI CONFERENCIAS SOBRE
SUPERVISIÓN FINANCIERA

Muchas gracias

Questions?