Fourth Annual Latin America Privacy & Cybersecurity Symposium

KPMG FORTINET OneTrust Privacy Management Software ICC MEXICO INTERNATIONAL CHAMBER OF COMMERCE The world business organization iapp EGADE Business School Tecnológico de Monterrey JONES DAY

CYBERSECURITY IN THE FINANCIAL SECTOR

Presented by

Mauricio Paez, Partner, Jones Day- Cybersecurity, Privacy and Data Protection
Alejandro Clares, S21SEC

JONES DAY

IMPACT OF NEW TECH TO FINSERV COMPANIES

- New technology and services continue to influence the industry
- These transformative technologies have, such as AI, IoT payments, big data, and blockchain present significant opportunities and cyber risks
- The most prevalent cybersecurity risks are in the deployment of multi-party connected platforms
- The view is that small, startup FinTech companies present the greatest risks

CIBERSEGURIDAD Y PRESTACIÓN DE SERVICIOS FINANCIEROS

País	Leyes Vigentes	Resumen
Argentina	**1.** Ley 21.526 – Ley de Entidades Financieras. **2.** Ley 25.326 – Ley de Protección de Datos Personales. **3.** Ley 26.733 - Código Penal **4.** Resolución 30/2017 - emitida por la Unidad de Inteligencia Financiera. **5.** Comunicación "A" 6375.	**1.** Establece requisitos mínimos que deben cumplir las entidades financieras que operan para efectos de asegurar la confidencialidad y seguridad de sus operaciones. **2.** Adopción de medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos personales que permitan detectar desviaciones, de información. **3.** Regula la intermediación financiera no autorizada y otros delitos financieros. **4.** Establece los lineamientos para la para gestionar de acuerdo con sus políticas, procedimientos y controles, el riesgo. **5.** Señala la gestión y controles de riesgos relacionados con la tecnología informática y recursos asociados.
Brasil	**1.** Ley 10214 – 27 marzo de 2001. **2.** Resolución 4,282/2013. **3.** Resolución 4283/2013. **4.** Circular 3681/2013.	**1.** Establece mecanismos y salvaguardas que deberán incluir seguridad de equipos y reglas de control de riesgos en contingencias para efectos de as operaciones realizadas. **2.** Señala las reglas que deben ser observadas para la regulación, monitoreo y supervisión de las instituciones financieras. **3.** Prevé la prevención de riesgos transaccionales y regula la prestación de servicios de instituciones financieras. **4.** Establece el manejo de riesgos, requerimientos de equidad y gobernanza de las instituciones de pagos, así como la preservación de valores y liquidez y otras medidas.

JONES DAY

CIBERSEGURIDAD Y PRESTACIÓN DE SERVICIOS FINANCIEROS

País	Leyes vigentes	
Chile	Recopilación Actualizada de Normas (“RAN”) – Capítulo 1 – 13 y 20 – 8.	-Establece especial atención en la gestión de la infraestructura crítica, como parte de la Evaluación de Riesgo Operacional dirigida a bancos. - Prevé contenidos para la generación y gestión de una adecuada base de incidentes de Ciberseguridad. - Incorpora la Ciberseguridad como contenido de educación financiera.
Colombia	Circular Básica Jurídica C.E. 029 de 2014 Capítulo V.	- Señala las obligaciones en materia de ciberseguridad con las que deben cumplir las entidades reguladas (instituciones financieras), asimismo, establece las políticas, procedimientos y recursos humanos necesarios para gestionar los riesgos de la ciberseguridad.
México (FinTech)	**1.** Ley para Regular las Instituciones de Tecnología Financiera. **2.** Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera. **3.** Circular Única de Bancos.	**1.** Señala de una manera general las medidas y políticas para controlas riesgos relacionados con la seguridad de la información, confidencialidad y soporte tecnológico seguro, confiable y preciso. **2.** Complementando a la Ley, Establece de una manera detallada los estándares mínimos de seguridad que aseguren la confidencialidad, disponibilidad e integridad de la información y prevención de fraudes y ataques cibernéticos. **3.** Señala los órganos que deben instaurarse al interior de la organización para atender incidentes de ciberseguridad. Asimismo, establece los procedimientos que deberán seguirse ante la autoridad correspondiente.

ELEMENTOS COMUNES EN LAS DIVERSAS JURISDICCIONES

NY DFS CYBERSECURITY LAW

- **NY Department of Financial Services - Cybersecurity Regulations:** The NYDFS Cybersecurity Regulation requires New York insurance companies, banks, and other regulated financial services institutions—including agencies and branches of non-US banks licensed in the state of New York—to assess their cybersecurity risk profile.

  - Risk-based minimum standards for information technology systems, including data protection and encryption, access controls, and penetration testing.

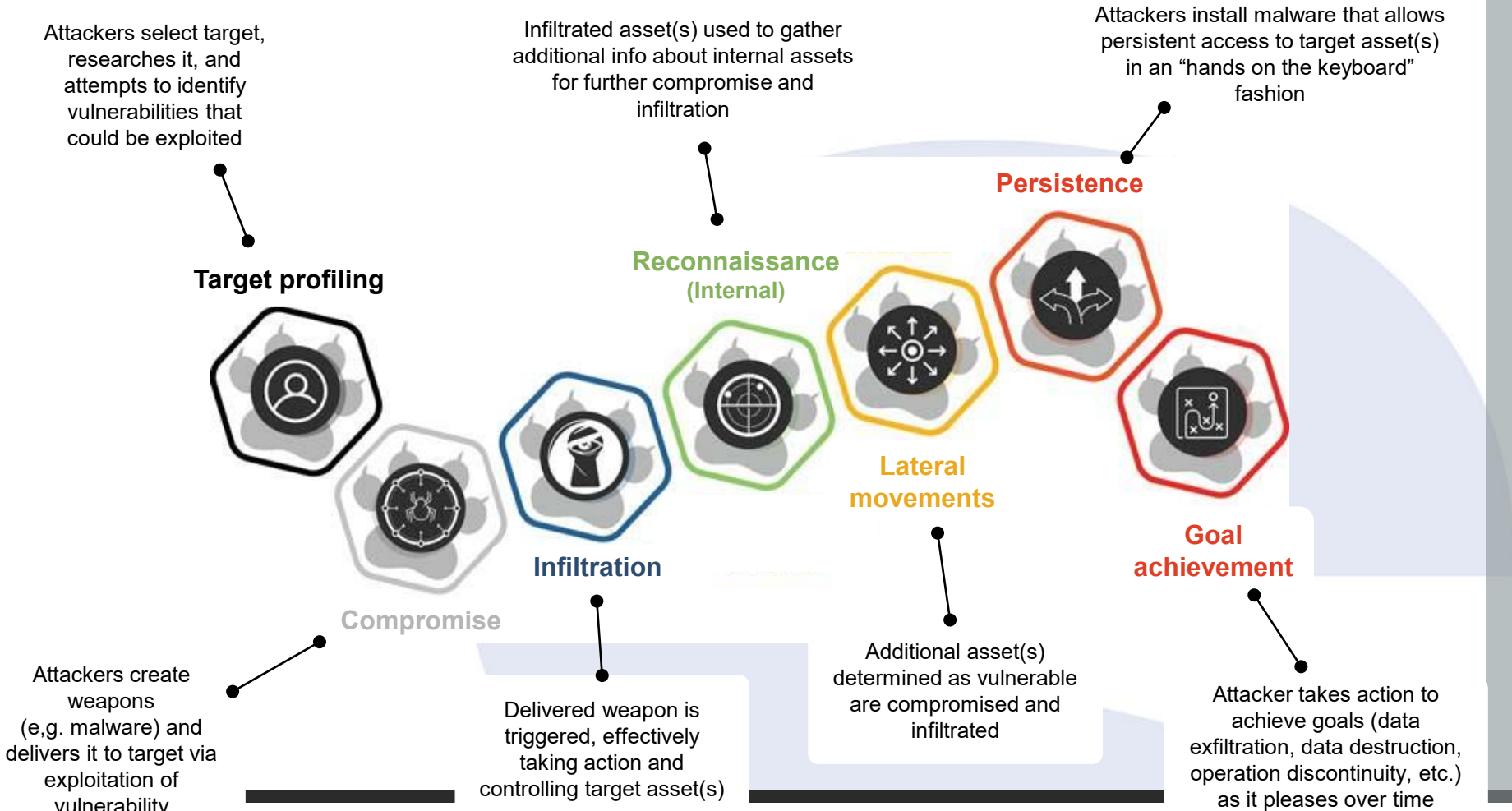
  - Requirements that a program is adequately funded, overseen by a chief information security officer, and implemented by qualified cybersecurity personnel.

  - Effective incident response plans that include preserving data in order to respond to data breaches and timely notice to the NYDFS of material events.

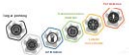
  - Accountability provided by identification and documentation of deficiencies, remediation plans, and certifications of compliance on an annual basis.

ADDRESSING CONCERNS AND REQUIREMENTS

- How do you effective respond to financial cyber threats and incidents?


Attackers select target, researches it, and attempts to identify vulnerabilities that could be exploited
Target profiling
Infiltrated asset(s) used to gather additional info about internal assets for further compromise and infiltration
Reconnaissance (Internal)
Attackers install malware that allows persistent access to target asset(s) in an “hands on the keyboard” fashion
Persistence
Lateral movements
Additional asset(s) determined as vulnerable are compromised and infiltrated
Goal achievement
Attacker takes action to achieve goals (data exfiltration, data destruction, operation discontinuity, etc.) as it pleases over time
Infiltration
Delivered weapon is triggered, effectively taking action and controlling target asset(s)
Compromise
Attackers create weapons (e,g. malware) and delivers it to target via exploitation of vulnerability

WHITE & BLUE TEAM (DEFENSIVE TEAM)

Category	Modular service CAT coverage					
Target profiling	Vulnerability Assessment 			Exposure Analysis 		
Pen Testing	Attack to Web Apps & Sites 		Intrusion Test 		Attack to Wi-Fi Infrastructures 	
Mystery Hacker	Mystery Hacker “Vertical” 			Mystery Hacker “New Employee” 		
Real life exercises	Volumetric DoS 	Technical DoS 	Social Engin. 	Spear Phishing 	APT Simulation 	Armageddon 
Real life training	War Gaming 			SOC Technical Training 		

Best practices (1)

- Establish the firm’s cybersecurity goals and objectives, taking a risk-based and principle based approach that defines specific operational risk controls.
- Establish a strategic, forward looking, fluid and proactive approach to cybersecurity risk management and compliance that take into consideration evolving threats.
- Conduct a cybersecurity resilience assessment, but avoid being divorce from business operations, risk, and compliance.

Best practices (2)

- Develop and implement a governance framework with Board involvement, reporting and communication cadence.
- Develop a testing and monitoring methodology that takes into consideration the complexity of the firm's operations, third party provider risks, industry accepted standards, and regulatory guidance (penetration testing, continuous monitoring, assurance and tabletops).
- Prepare for the inevitable: cyber incident preparedness assessment and response framework.

Best practices (3)

- Develop and implement an effective third party risk management framework that extends the cyber risk management program to third party providers in all phases: pre-contract, contract, and post contract.
- Participate in threat information sharing organizations.
- Develop a cybercrime law enforcement engagement and investigation coordination program, communications, and reporting approach.

Jones Day presentations should not be considered or construed as legal advice on any individual matter or circumstance. The contents of this document are intended for general information purposes only and may not be quoted or referred to in any other presentation, publication or proceeding without the prior written consent of Jones Day, which may be given or withheld at Jones Day's discretion. The distribution of this presentation or its content is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of Jones Day.