Debevoise & Plimpton

Cyber Security In Context: Perspectives on Risk Management

Jim Pastore

FIRMA National Risk Management Training Conference
San Diego, CA – April 24, 2018

Our Discussion Today

Setting the Stage:
Threat Actors

Two Perspectives:
Privacy vs. Risk

Implications For Effective Risk Management

Effective Incident Response

Questions


Setting the Stage:
Threat Actors

Faces of Cybercrime

WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

WANG DONG
Aliases: Jack Wang, "UglyGorilla"

SUN KAILIANG
Aliases: Sun Kai Liang, Jack Sun

WEN XINYU
Aliases: Wen Xin Yu, "WinXYHappy", "Win_XY", Lao Wen

HUANG ZHENYU
Aliases: Huang Zhen Yu, "Ivy Ihx"

GU CHUNHUI
Aliases: Gu Chun Hui, "KandyGoo"

DETAILS

On May 1, 2014, a grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army (PLA) of the People's Republic of China (PRC) for 31 criminal counts, including: conspiring to commit computer fraud; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging computers through the transmission of code and commands; aggravated identity theft; economic espionage; and theft of trade secrets.

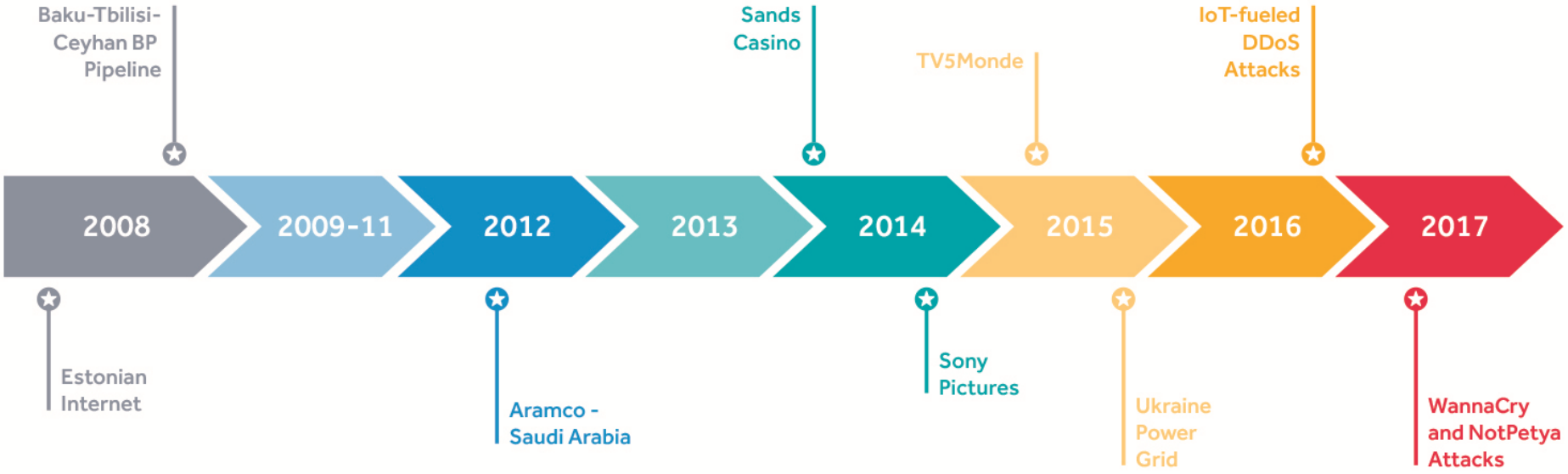
The subjects, Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, were officers of the PRC's Third Department of the General Staff Department of the People's Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398, at some point during the investigation. The activities executed by each of these individuals allegedly involved in the conspiracy varied according to his specialties. Each provided his individual expertise to an alleged conspiracy to penetrate the computer networks of six American companies while those companies were engaged in negotiations or joint ventures or were pursuing legal action with, or against, state-owned enterprises in China. They then used their illegal access to allegedly steal proprietary information including, for instance, e-mail exchanges among company employees and trade secrets related to technical specifications for nuclear plant designs.

If you have any information concerning these individuals, please contact your local FBI office or the nearest American Embassy or Consulate.

An Evolution . . .

Debevoise & Plimpton

Destructive Attacks



Debevoise & Plimpton

Landmark PII Heists

EQUIFAX

Equifax (2017): Full credit data for 148 million customers

UBER

Uber (2017): Exposure of 57 million users' data, including 600,000 driver's license numbers of drivers.

YAHOO!

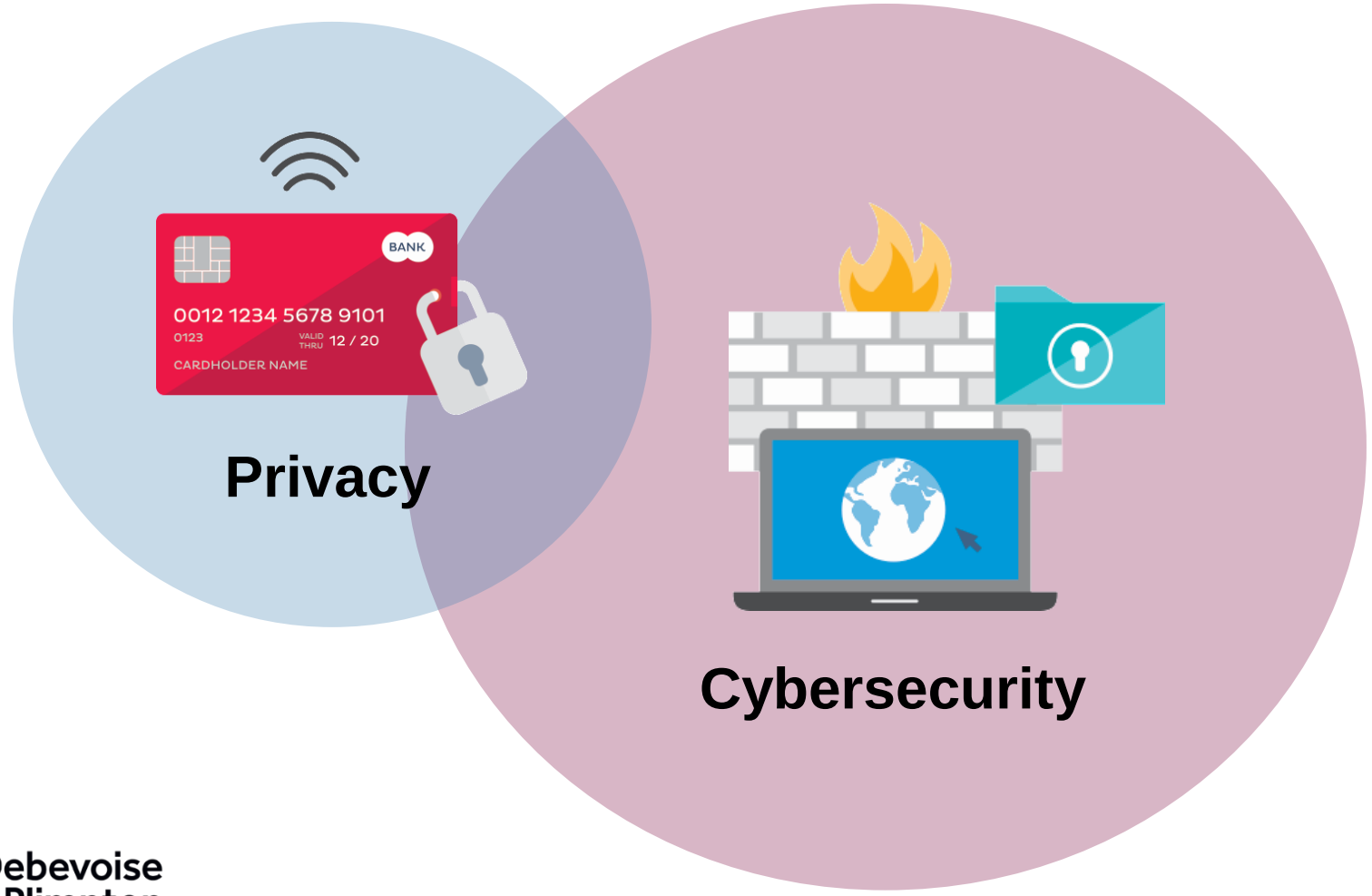
Yahoo! (2016): Two incidents involving 3 billion user accounts

Anthem.

Anthem (2015): PII of almost 80 million customers and employees


Two Perspectives:
Privacy vs. Enterprise
Risk

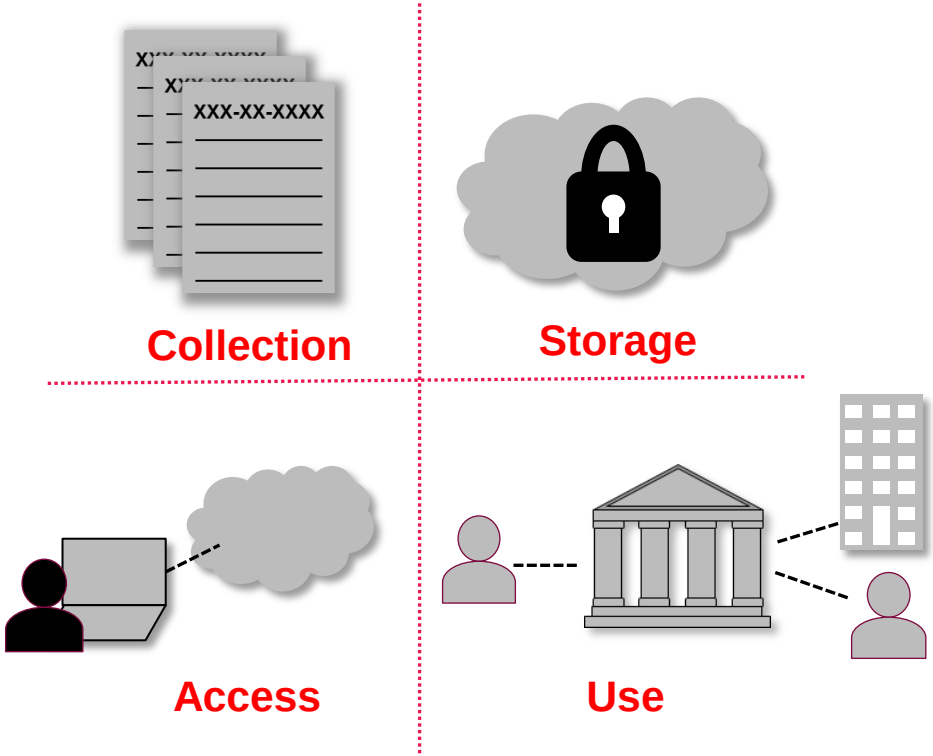
Two Perspectives



Debevoise & Plimpton

Privacy Perspective

Focus on Personally Identifiable Information . . .

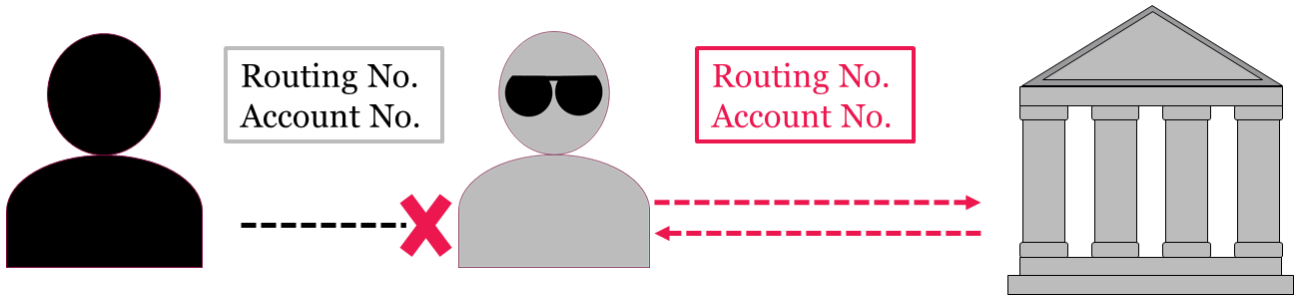


. . . and preventing breaches and data exfiltration.

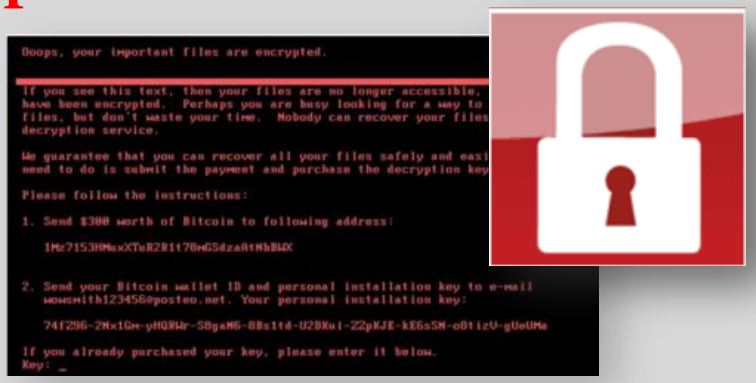
Debevoise & Plimpton

Enterprise Risk Perspective

Incidental Access to PII



Transactional & Operational Risk



Debevoise & Plimpton

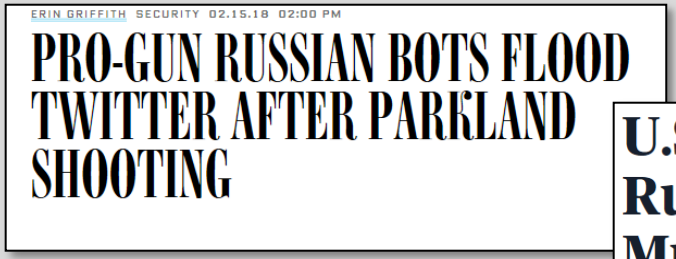
Enterprise Risk Perspective

Intellectual Property

HBO

GAME OF THRONES™

Unintended Network Use


ERIN GRIFFITH SECURITY 02.15.18 02:00 PM

PRO-GUN RUSSIAN BOTS FLOOD TWITTER AFTER PARKLAND SHOOTING


U.S. imposes sanctions on 13 Russians indicted by Robert Mueller

Politics Mar 15, 2018 10:41 AM EDT — Updated on Mar 15, 2018 11:11 AM EDT

Debevoise & Plimpton


Implications for Effective Risk Management

A Baseline of Compliance

NYDFS Cybersecurity Regulation

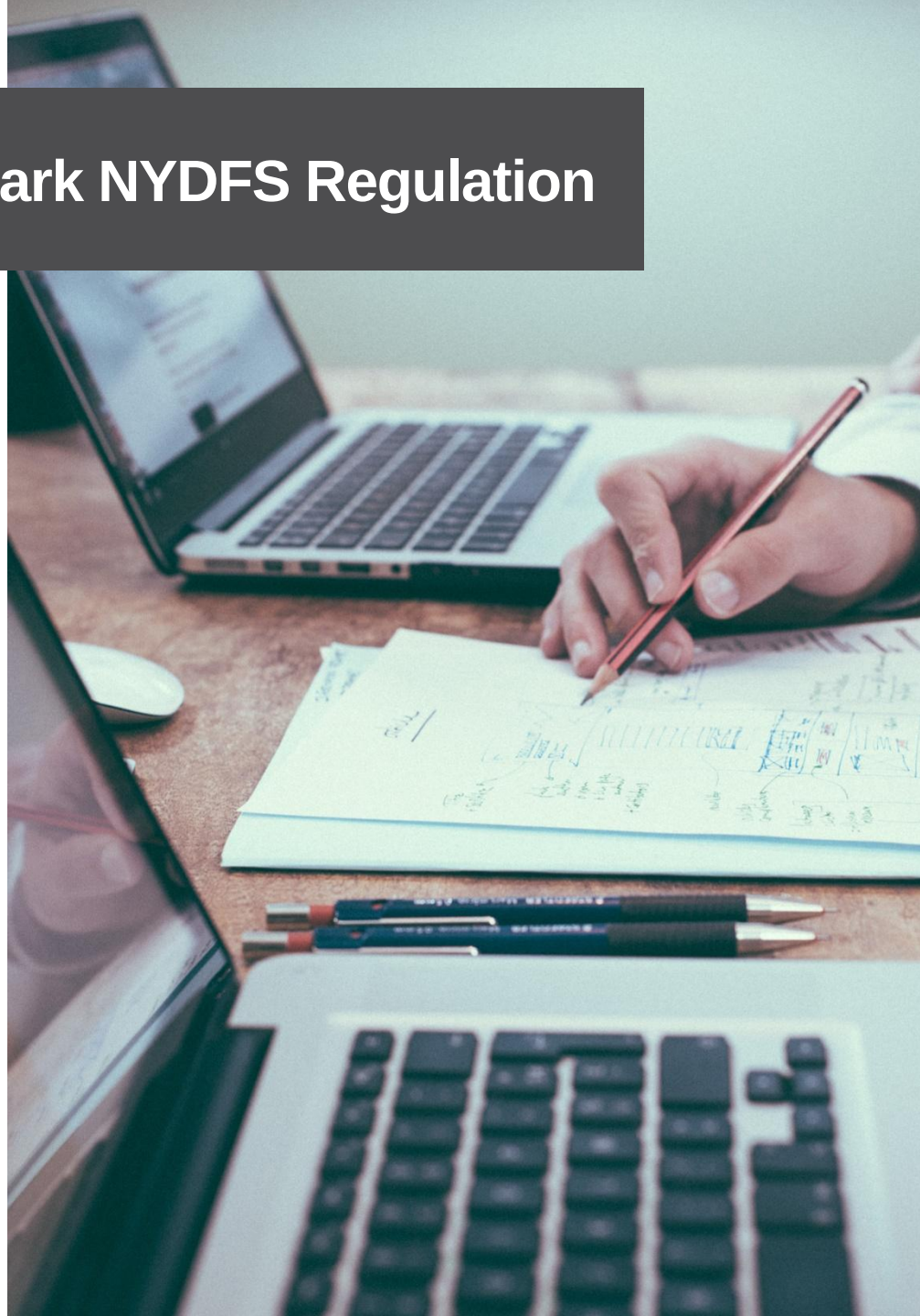
SEC and FINRA: Cybersecurity as an exam priority; recent wave of fines

NAIC's new Model Law closely tracks the NYDFS rule

Updated NIST Cybersecurity Framework

A Closer Look at the Landmark NYDFS Regulation

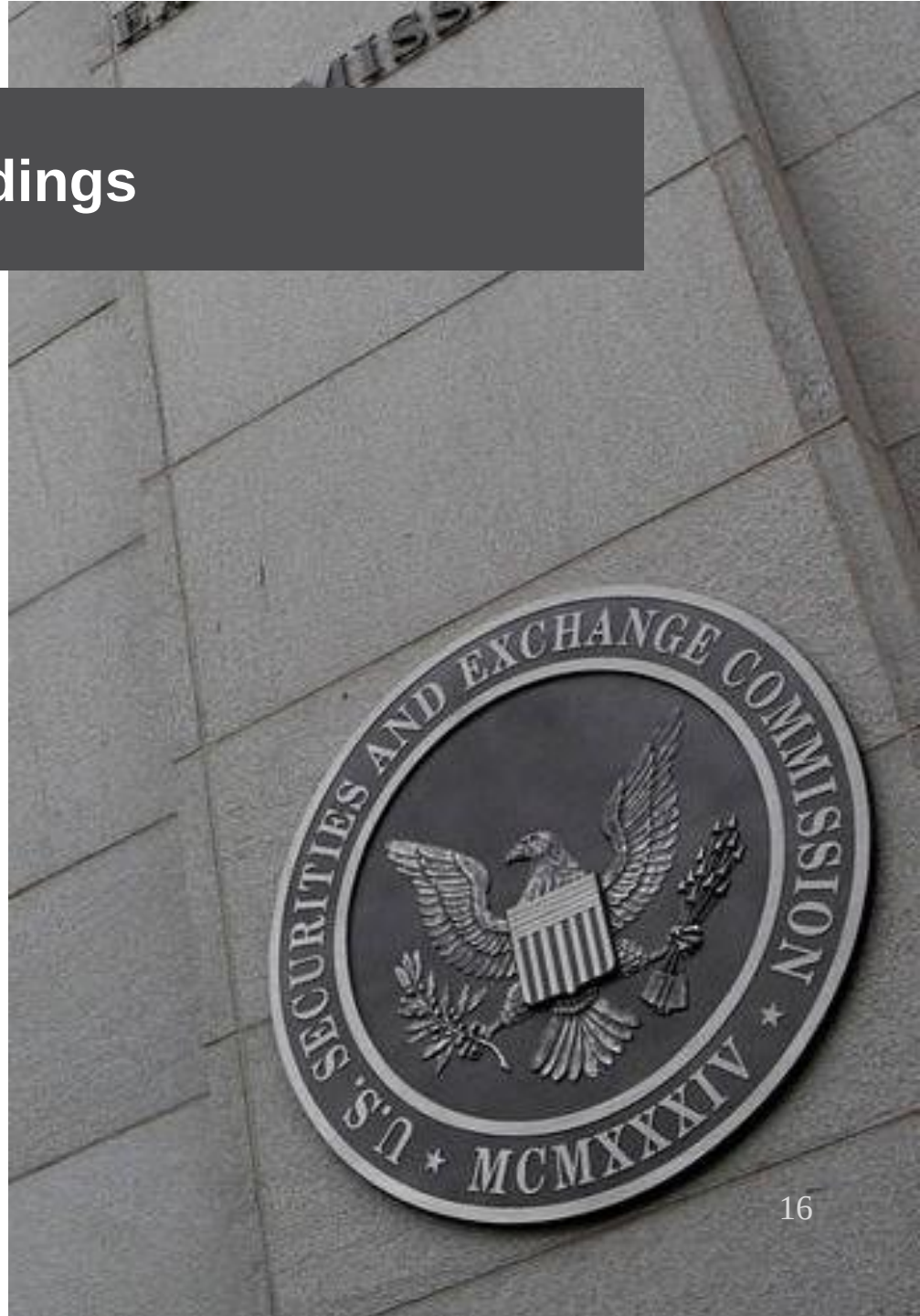
- Initial, prescriptive drafts evolved into risk-based approach
- Heavy emphasis on an enterprise wide risk assessment, and what that means
- Key policy and procedural aspects, including CISO role and board involvement
- Annual certification of compliance
- First certifications of compliance were due February 2018



Debevoise & Plimpton

2017 SEC Cyber Exam Findings

- Policies and procedures not reasonably tailored
- Policies and procedures inconsistent with actual practices
- Stale risk assessments
- Lack of remediation efforts



Debevoise & Plimpton

Elements of Robust Policies and Procedures

- Maintenance of an inventory of data, information, and vendors
- Detailed cybersecurity-related instructions
- Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities
- Established and enforced controls to access data and systems
- Mandatory employee training
- Engaged senior management

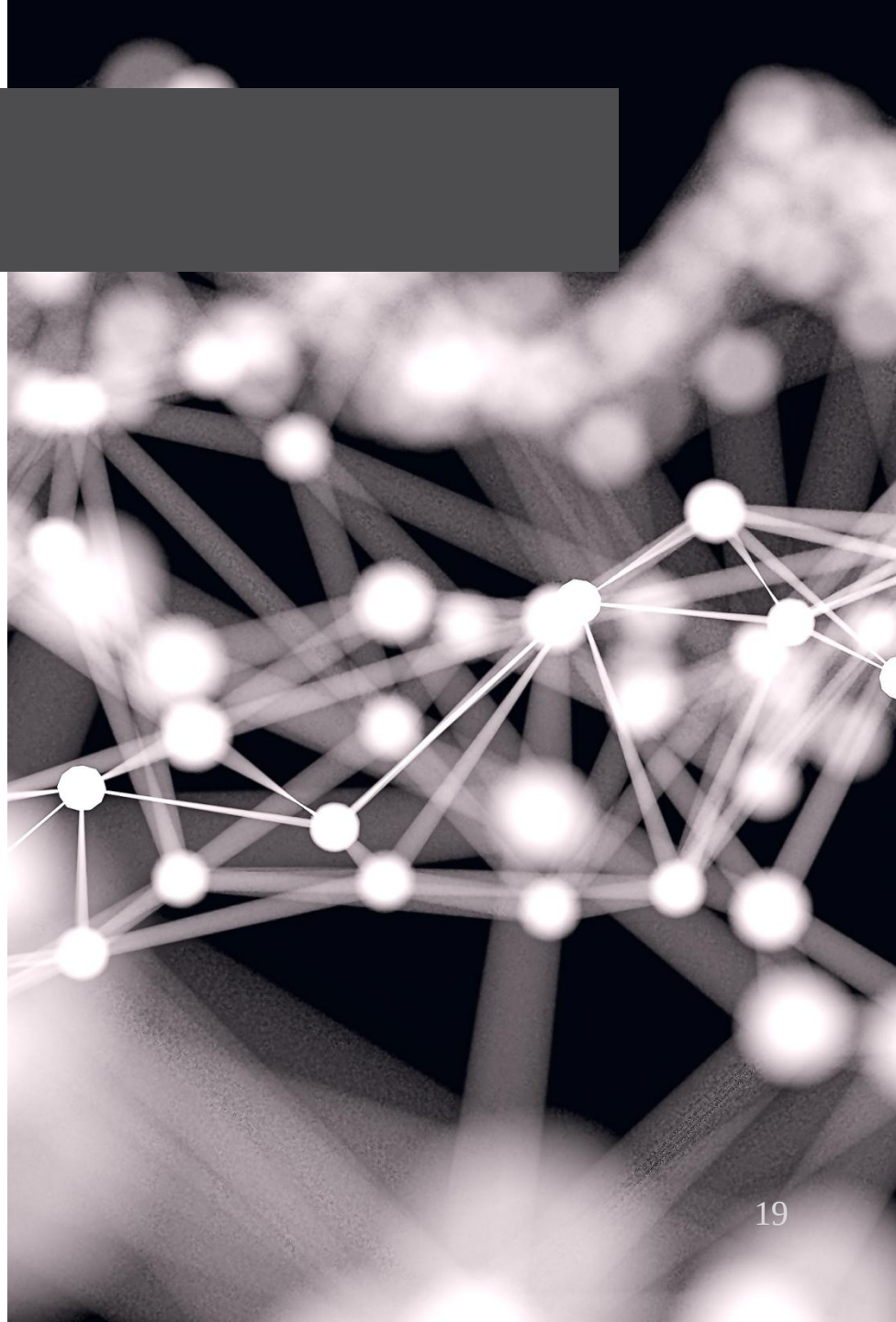
NAIC Model Law

- Tracks DFS
- With a few differences, *e.g.*:

	NY DFS	NAIC
Policies	Written policies covering many topics, including written secure application development practices	Written Information Security Program and Incident Response Plan
CISO	Requires appointment of a CISO	Requires designation of one or more employees, affiliate or outside vendor
Pen Testing	Required – annual penetration tests and bi-annual vulnerability assessments	References testing controls
Multi-Factor Authentication	Required, for any individual accessing internal networks from an external network	Effective controls may include multi-factor authentication

NIST Updated Framework

- Second draft of proposed framework issued December 5, 2017
- Framework remains flexible
- Updates to the self-assessment process to focus on measuring risk along with the cost and benefits of remediation efforts
- New emphasis on cybersecurity in supply chain risk management



Debevoise & Plimpton

Litigation Trends

- Standing arguments gain ground; eye on company statements
- Cases are not getting dismissed as easily; discovery risks
- Plaintiff's Bar is expanding and becoming more aggressive (with both privacy class actions and inter-vendor disputes)
- Push to hold senior management and boards accountable
- Elevated importance of counsel at many key junctures

Industry Pressure:
SWIFT Customer Security Controls Framework

- After suffering several hacks through member banks in 2015 and 2016, SWIFT began enforcing mandatory security controls on its members on April 1, 2017.
- Members were required to self-attest that they have implemented the security controls by the end of 2017 and every 12 months thereafter.
- SWIFT may seek additional information on compliance from members' internal or external auditors and reserved the right to report a member's failure to submit a self-attestation to regulators.

Secure Your Environment

- Restrict Internet access
- Protect critical systems
- Reduce attack surface
- Physically secure environment

Know and Limit Access

- Prevent credential compromise
- Manage identities and segregate privileges

Detect and Respond

- Detect anomalous activity
- Plan for incident response and information sharing

Debevoise & Plimpton

Effective Vendor/Supplier Risk Management

Software: "Zero Days" are highly overrated; the bigger problem is addressing known vulnerabilities

Lack of segmentation and detection often leads to significant damage

Strong contractual protections are necessary but insufficient

Value of due diligence and related practical issues

Area of increasing regulatory focus that will flow down to vendors themselves

Insurance considerations


Effective Incident
Response

Incident Response as Key Component of an Information Security Program

- Information security programs are multifaceted

Policies & Procedures	Data Security	Training & Awareness
Access Control	Logging & Monitoring	Risk Assessments
Identity Management	Incident Response	

- And incident response planning is a critical component:
  - It is a matter of when, not if, a cyber incident will occur
  - A documented and tested incident response plan increases an organization's ability to respond quickly and effectively
  - When organizations begin to expect – and prepare for – a cyber incident, the organizational mindset shifts from worrying solely about adequate defenses to proactive monitoring and prompt response

Debevoise & Plimpton

Essential Steps for Incident Preparation

Monitoring your evolving threat profile

Mapping your network

Layering network defenses and emphasizing detection

Developing an incident response plan (IRP)

Establishing an incident response team

Testing your plan and your team

Building key external relationships with law enforcement and others

Assessing insurance

Debevoise & Plimpton

The Crush of a Major Incident

Debevoise & Plimpton

Lifecycle of an Incident

- Validate breach and preserve evidence, typically with help of outside experts
- Notification of possible breach to senior management
- Possible initial press reports; rapidly prepare messaging
- Possible law enforcement engagement

- Confirm scope of breach; containment; begin remediation
- Initial notifications to internal and external stakeholders
- Legally mandatory disclosures to certain external stakeholders
- Lawsuits and government investigations begin

- Intensive fact gathering around breach and pre-breach security practices
- Complete short-term remediation
- Begin to identify “lessons learned” and plan for broader security improvements
- Additional law suits filed and investigations begun; initial motion practice

- Implement and audit full range of security improvements
- Continued defense of litigation and government inquiries; resolution of same

Debevoise & Plimpton

Key Intangibles in a Major Breach

How the victim's corporate governance works in a crisis

Protocols established in advance and drilled in simulations

Understanding what information can and should be shared with law enforcement and regulators

Understanding how the government will respond

Having an incident response team that can cover all of the technical and legal bases

Ability to leverage external relationships

Debevoise & Plimpton

The Role of Counsel in Managing Cyber Risks

Extending privilege to maximum extent possible before, during and after an incident

Making disclosure and related timing determinations

Translating key technical decisions into business decisions

Ensuring evidence preservation and investigation documentation

Leveraging external relationships with law enforcement and regulators

Vetting public statements to balance brand and liability issues

What can we do proactively? Active defense and related issues

Debevoise & Plimpton

Questions?

Debevoise Cyber Contacts

New York and Washington, D.C.:

Jim Pastore
New York
jjpastore@debevoise.com
+1 212 909 6793

Luke Dembosky
Washington, D.C.
ldembosky@debevoise.com
+1 202 383 8020

Jeremy Feigelson
New York
jfeigelson@debevoise.com
+1 212 909 6230

Maura Kathleen Monaghan
New York
mkmonaghan@debevoise.com
+1 212 909 7459

Christopher Ford
New York
csford@debevoise.com
+1 212 909 6881

London, Frankfurt and Paris:

Lord Goldsmith QC
London
phgoldsmith@debevoise.com
+44 20 7786 9088

Jane Shvets
London
jshvets@debevoise.com
+44 20 7786 9163

Robert Maddox
London
rmaddox@debevoise.com
+44 20 7786 5407

Dr. Thomas Schürrle
Frankfurt
tschuerrle@debevoise.com
+49 69 2097 5000

Fanny Gauthier
Paris
fgauthier@debevoise.com
+33 1 40 73 12 90

Hong Kong and Tokyo:

Mark Johnson
Hong Kong
mdjohnson@debevoise.com
+852 2160 9861

Ralph Sellar
Hong Kong
rsellar@debevoise.com
+852 2160 9860

Naomi Aoyama
Tokyo
naoyama@debevoise.com
+813 4570 6683

Debevoise & Plimpton