K&L GATES

CRA Charles River Associates

2017 Consumer Financial Services Symposium

Cybersecurity and the Lifecycle of a Data Breach

Moderator:

David Case, Partner, K&L Gates LLP

Panelists:

Bill Hardin, Vice President, Charles River Associates

Julia Jacobson, Partner, K&L Gates LLP

Soyong Cho, Partner, K&L Gates LLP

James Scheuermann, Partner, K&L Gates LLP

Bruce Heiman, Partner, K&L Gates LLP

Cyberthreat Landscape

Bill Hardin, Vice President, Charles River Associates

Overview

NEUTRAL

Threats


Malicious Insider
Employee Mistakes
Criminal Hackers
Hacktivists
Cloud or 3rd Party Compromise

Extortion Threat Landscape

ENGAGEMENT

AUTOMATION

Automation – We Call It

BTCWare GruxEr vCrypt Merry I love you
Bruce Locky Stampado Zelta

Lockout **SAMSAM** Matrix
Cerberos Cry9 Serpent Troldesh Jigsaw
JeepersCrypt CryptoMix Petya
Erebus **WANNACRY** NotPetya

Legal Landscape

Soyong Cho, Partner, K&L Gates LLP
Julia Jacobson, Partner, K&L Gates LLP

Federal Oversight

Federal Agencies with Oversight Jurisdiction

- OCC
- FDIC
- Federal Reserve
- NCUA
- FTC
- CFPB

Federal Law and Guidance

- Gramm-Leach-Bliley Act
- Fair Credit Reporting Act
- Safeguards Rule
- Disposal Rule
- FTC enforcement actions under Section 5 of the FTC Act for unfair or deceptive acts or practices
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- FFIEC IT Examination Handbook
- Pending – Joint Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management

Possible Consequences of Deficient Programs

- Cease and Desist Orders
- Administrative Consent Orders
- Litigation
- Penalties
- Restitution

U.S. State Landscape

Key Question: what is 'personal information' under the applicable state laws?

- **State Data Security Laws** - Protect the security of personal information that a business collects, uses and stores
  - Strict: Massachusetts Data Security Regulations
- **State Data Destruction Laws**
- **State Financial Cybersecurity Laws** – more prescriptive
  - New York - specific compliance requirements and annual certification by a senior executive or the board
  - Colorado – similar to New York
  - Vermont - written procedures reasonably designed to ensure cybersecurity; evidence of adequate insurance for the risk of cyber security breach; provide post-breach "identity restoration services"

State Data Breach Notification Laws

- **State Data Breach Notification Laws**
  - **Personal information – narrowly defined**
    - common definition: name + SSN; DL or state ID number; financial account number, credit or debit card number
    - form of information – computerized data (e.g., New York) *vs.* all data (e.g., Washington)
  - **Harm to data subject**
    - cause or likely to cause harm/identity theft/fraud
    - "misuse of the information is not reasonably possible" (e.g., New Jersey)

    consider Nevada – not liable for a breach if comply with state data security law and no gross negligence or intentional misconduct

State Data Breach Notification Laws

- **Exceptions**
  - Encrypted, redacted or unreadable
  - Publicly-available information – lawfully made available to the general public from government records or widely distributed media (e.g., Connecticut)
  - "Good faith" acquisition – by employee/agent for legitimate business purpose if not used for unrelated purpose and not subject to further unauthorized disclosure (e.g., Illinois)
- **When to notify varies** - Law enforcement delay
- **Who to notify varies** - Individuals and/or Regulators

General Data Protection Regulation (GDPR)

Three types of "**personal data breach**"

- Confidentiality – unauthorized or accidental *disclosure* of or *access* to personal information
- Availability – unauthorized or accidental *loss of access* to or *destruction* of personal information
- Integrity – unauthorized or accidental *alteration* of personal information

The standard for notification to **supervisory authorities** is a breach that is likely "to result in a **risk** to the **rights and freedoms** of natural persons."

The standard for notification to **data subjects** is a breach that is likely to result in a **high risk** to the **rights and freedoms** of natural persons."

Key Takeaways

- ✓ Document cybersecurity roles and responsibilities.
- ✓ Make cybersecurity a C-Suite/Board issue.
- ✓ Conduct a data inventory – if you collect it, protect it.
- ✓ Ensure cybersecurity policies are appropriate to the risks – one size does not fit all.
- ✓ Address at least regular vulnerability assessments; malware detection and prevention; access controls; incident response (plan, test plan and know how/when to report to regulators; and employee training).
- ✓ Conduct and document review of vendor cybersecurity practices prior to and periodically throughout engagement.

View cybersecurity as a competitive advantage

Best Practices & Risk Mitigation Through Insurance

James Scheuermann, Partner, K&L Gates LLP

Risk Management

Four ways to manage any identified risk:

- Avoid
- Accept
- Mitigate
- Transfer

Avoid

- Don’t enter a market
- Don’t conduct business in some fashion (*e.g.*, online sales)
- Don’t contract with vendor X

Accept

- Passive: by doing little to nothing in any of the other three categories
- Active: by taking all reasonable, cost- and risk- beneficial steps in the other three categories and acknowledging that some risk is ineliminable

Mitigate

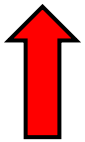
- Technical tools (*e.g.*, encryption of data, backup data, updating and patches, cybersecurity penetration tests, cybersecurity audits)
- Human Resources tools (*e.g.*, training employees, need-to-know access to sensitive data)
- Corporate Governance tools (*e.g.*, focused Board and Directors and Officers, adequate funding for CISO and cyber insurance, post-incident response plan)

Transfer

- Insurance
  - Cyber Insurance and Other Lines (e.g., CGL, Property, D&O, EPLI, E&O, Crime)
- Commercial Contracts (Vendors and Customers)

2016 Cyber Events

- 90% increase in breaches by external actors (vs. 2015)
- 210% increase in ransomware attacks (vs. 2015)



- $221 – average cost per lost/stolen record
- $4M – average cost of data breach

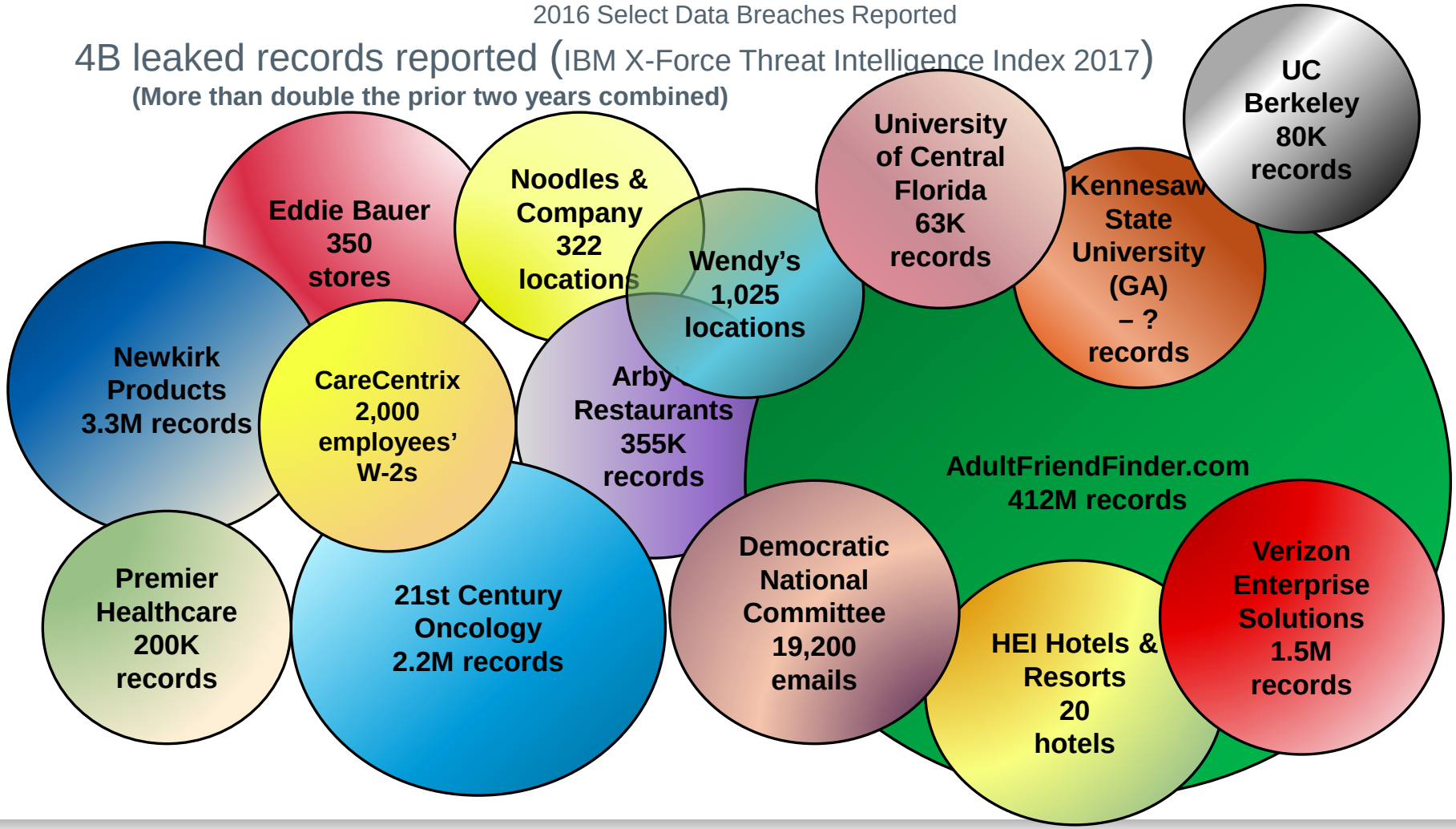
(Sources: Advisen 2016 Cyber Risk Trends, available at www.advisenltd.com/2017/04/05 . . .; Ponemon Institute, June 2016)

Data Breach: Just One of Several Cyber Risks

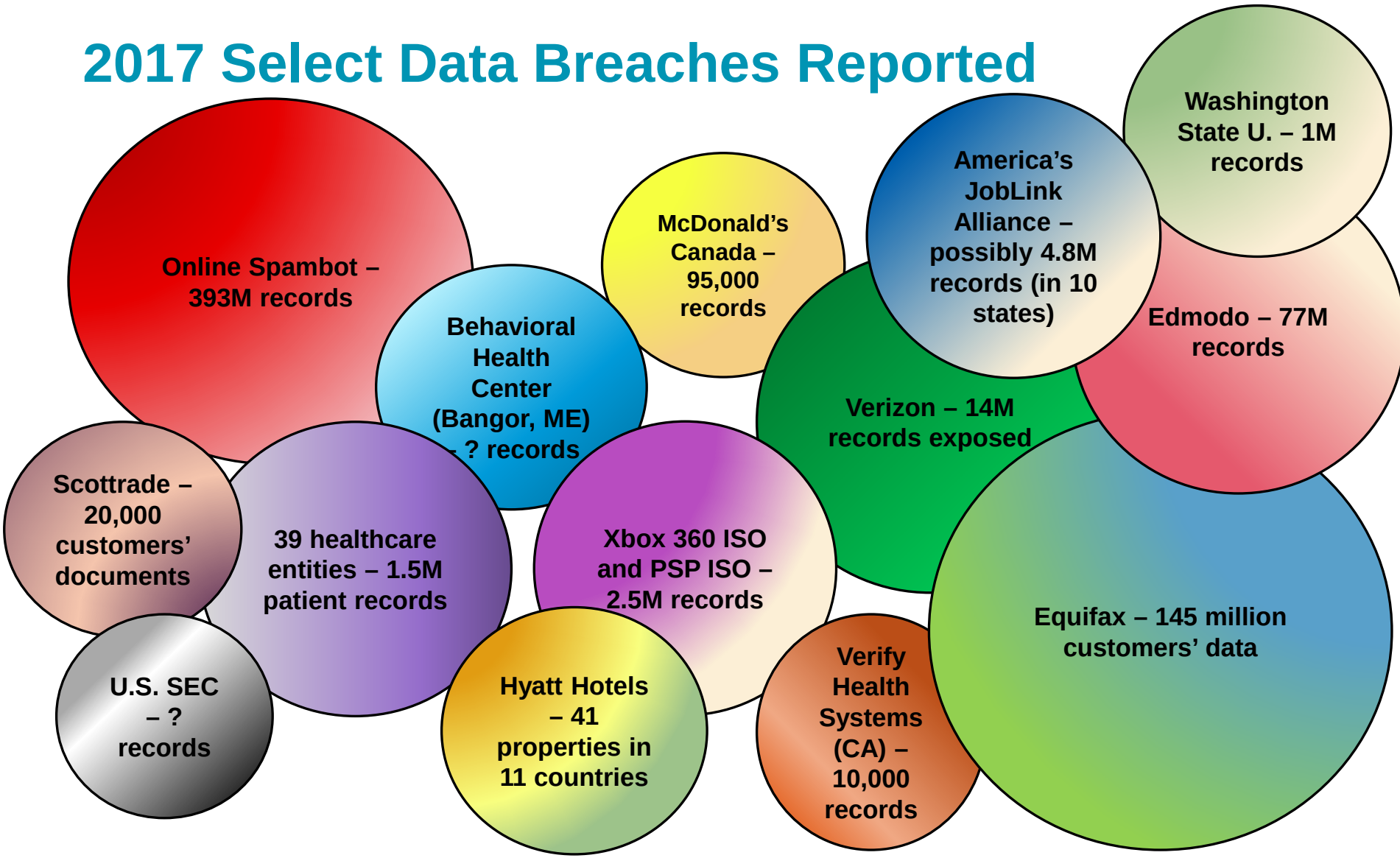
2016 Select Data Breaches Reported

4B leaked records reported (IBM X-Force Threat Intelligence Index 2017)

(More than double the prior two years combined)



2017 Select Data Breaches Reported



Other Cyber Risks

- Cyber extortion/ransomware
  - Substantial increase in 2016
  - 2017 – WannaCry and NotPetya
- Malware – industrial espionage, financial crimes, advanced persistent threats, attacks on computer system's functionality
- Cyber-physical attack
  - Bodily injury
  - Property damage
- DDoS
- Business email compromise schemes (fraudulent funds transfers)
- Media liability (libel, copyright, etc.)

Who "Owns" Cyber Risk & Event Response?

- Board of Directors?
- CEO?
- GC?
- CIO/CISO?
- CFO?
- Risk Manager?

Common Scenarios: Incident vs. Breach

Bill Hardin, Vice President, Charles River Associates
Julia Jacobson, Partner, K&L Gates LLP

Incident vs. Breach

Consider Massachusetts Data Breach Notification Law:

Unauthorized acquisition or unauthorized use of *unencrypted* data or, encrypted electronic data and the confidential process or key that is capable of compromising …*personal information*, … that creates a *substantial risk of identity theft or fraud* against a Massachusetts resident…

Capitol Hill and Press Response

Bruce Heiman, Partner, K&L Gates LLP

"CYCLE OF TERROR"

The New York Times
How to Protect Yourself After the Equifax Breach

The Washington Post
Data of 143 million Americans exposed in hack of credit reporting agency Equifax

POLITICO
Lawmakers: Equifax should be 'shamed'

The Atlantic
How the Equifax Hack Could Hurt Anyone Applying for a Job

THE WALL STREET JOURNAL
Equifax Hack Leaves Consumers, Financial Firms Scrambling

Insurance Coverage Notification and Coverage Disputes

James Scheuermann, Partner, K&L Gates LLP

Cyber Policies and Cyber E&O Policies

Do you need a cyber insurance policy?

Cyber Policies

- First-Party and Third-Party Coverages
  - No standard form policies widely in use
  - Many carriers in market (about 70)
  - Terms and pricing often negotiable
  - *The Take Away*: View cyber policy as a part of your insurance program addressing cyber risks
  - *The Take Away*: Need a hand-in-glove approach
    - match coverages to exposures
    - requires thorough understanding of both
    - participation of: CEO, CFO, GC, CISO, Risk Manager, broker, insurer, coverage counsel

Proposed Legislation

Bruce Heiman, Partner, K&L Gates LLP

K&L GATES

SECURITY INCIDENT SCENARIO

On Sunday afternoon, the information security officer sends you an email asking you to call him immediately. When you call him back, he tells you that the bank suffered a ransomware attack that encrypted all of the bank's electronic data. Although you are aware that a business continuity plan is in the works, the information security officer tells you that back-ups are not available.

After three days of trying, the data is finally decrypted. The forensic team also determines that the ransomware's only functionality was to encrypt the data and no other malware is present in the system. The information security officer did some research through a confidential wiki and found ISOs at three other banks reporting the same problem. He suspects that the hackers gained access through a common third-party service provider.

Do you need to report the malware incident? If yes, to whom?

A few days later, you receive a call from a customer service representative who reports an irate customer accused the bank of negligent data security practices. The customer claims that his savings account at the bank and his brokerage account elsewhere had a total of $50,000 withdrawn without authorization by someone who had initiated wires using his bank and brokerage account numbers.

SECURITY INCIDENT SCENARIO, CONTINUED

You conduct an investigation and learn the following:

1. Two years ago, the customer gave numerous financial and personal data to the bank in connection with a mortgage loan he obtained from the bank. The data included his SSN, tax returns, occupation, salary, bank account numbers and balances and credit card numbers.
2. The customer submitted his information to the bank via email as a PDF document sent to the loan originator's personal email account. The loan originator then forwarded it to the loan department for underwriting.
3. The customer uses the bank's mobile banking products which run on a system that the bank licenses from a third-party vendor.
4. The loan originator is the biggest producer of residential loans at the bank. Although result oriented and effective, he has a reputation at the bank for bending the rules.
5. The bank has a policy prohibiting loan originators from storing personal data collected from customers on their laptops. You know that the bank is implementing some technical controls to limit this, but you suspect that all loan originators store some details about "their" customers and that this is "common practice" in the marketplace.
6. The loan originator frequently works from a local coffee shop with free WiFi.

The bank's president hears about the customer issue and wants your analysis and recommendations about next steps.