COUNSEL TO GREAT COMPANIES

Dealing with Data Breaches

June 9, 2016 – Employment Law Seminar

Bellevue, Washington

Presented by:

Todd Hinnen, Partner

Chair, Privacy & Security Practice

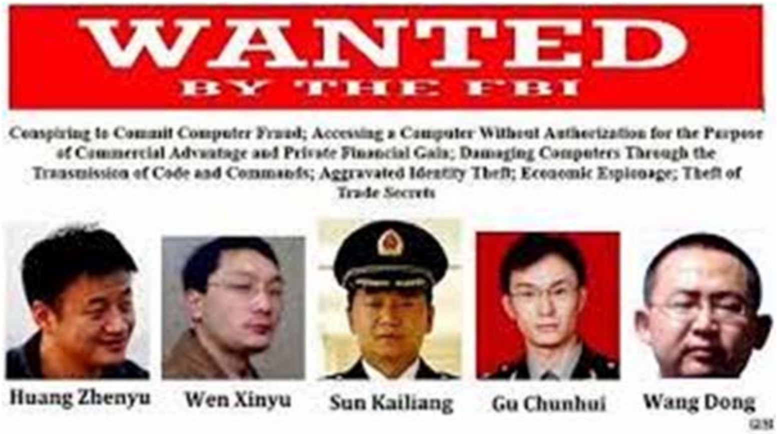
Digitization of HR Content

Ubiquity of Personal Data

Diversification of Threat Actors

Nation-state actors

- Highly resourced, sophisticated
- IP, critical infrastructure, propaganda value
- APT, Las Vegas Sands, Finance, Oil



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

Huang Zhenyu Wen Xinyu Sun Kailiang Gu Chunhui Wang Dong

Organized crime

- Personal information, credit cards
- Supported by black market for stolen data
- Target, Home Depot

Hacktivists, Script Kiddies, White Hats

The Nature of the Threat

In Chinese intrusion cases handled by Mandiant, 94% of the victim companies didn't realize their networks had been breached until someone else told them.

On average, companies' networks had been breached for 416 days before the intrusion was detected.

"Nation-states willing to spend unlimited amounts of money for technology, intelligence gathering, and bribery can overcome just about any defense."

-- Alan Paller, Director of Research, SANS Institute

Proliferation of Laws & Regulations

HIPAA

FTC Section 5

SEC guidance

GLBA

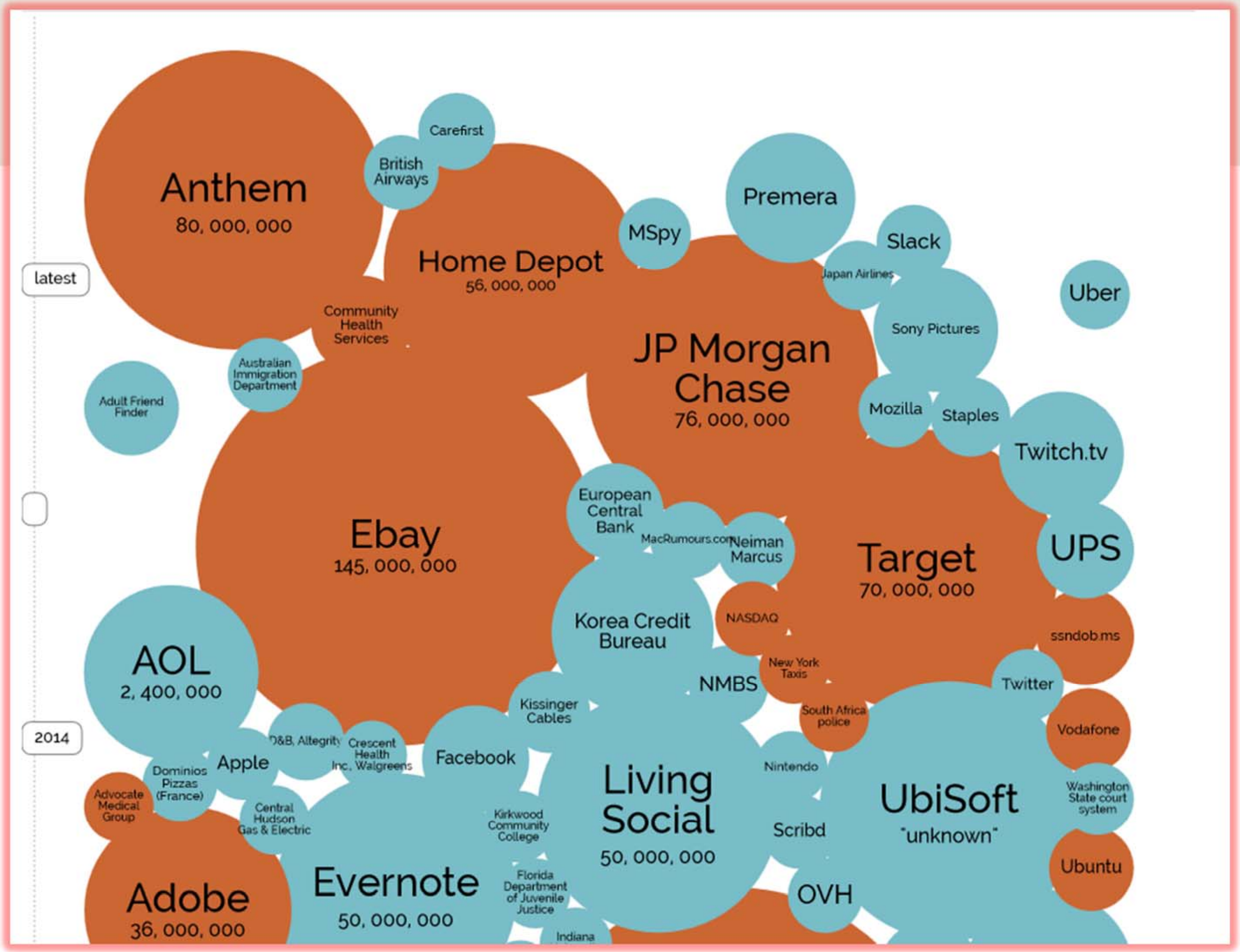
PCI DSS

NLRB Guidance

State Data Security Laws

State Breach Notification Laws

- HHS Settles with Health Plan for Records on Copier for $1.2M
- Mortgage Co. Fined $50K for Tossing PII in Dumpster
- Alaska DHHS Fined $1.7M for stolen unencrypted thumb drive
- WellPoint Fined $1.7M for exposure of PHI online
- CVS Fined $2.25M for disposing of health records in dumpster
- ChoicePoint pays $10M for unauthorized disclosure or PI
- AT&T fined $25M for breach of social security numbers



Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Three Types of Class Actions

Consumer Actions

- High profile recent decisions from Sony Playstation, Adobe, and Target endorsing a **lower bar** for standing
- Negligence, statutory claims surviving

Employee Actions

- Recent Sony Interview decision adopted consumer standing law

Financial Institutions Actions

- Target is settling for $67M with Visa; MasterCard TBD

Shareholder Litigation

Major cases

- Target (2014)
- Wyndham (2014) (since dismissed)
- Home Depot (2015)

Claims

- Breach of fiduciary duty
- Failure of responsible oversight
- Failure adequately to protect corporate assets

Allegations

- Officers, Board failed to devote regular attention and resources to data security
- Failed to heed warning of other prominent data breaches
- Company engaged in *per se* inadequate practices

How Do You Protect Your Company?

Company-wide data security program

- All stakeholders – IT alone can’t secure your data
- Coordinated, high-level engagement across components, business lines
- Written policies and practices -- IRP
- Train, audit, and enforce

Securing data shared with third-parties

- Due diligence
- Effective contracting

Insurance Coverage

- Cyber policy; interaction among policies

Labor & Employment Issues

- Onboarding process
- HR records practices
- Network & Employee Monitoring
  - Employee handbook, logon banners, BYOD registration
- Training
- Internal investigations, employee interviews
- Enforcement and discipline
- Separation, change of roles

Questions?

Todd Hinnen

206-359-3384

thinnen@perkinscoie.com

Additional Resources

Effective Security Controls

Administrative Controls

- Employee background checks, training, discipline, termination
- Network segmentation, device management, and access control
- Incident Response Plan

Physical Controls

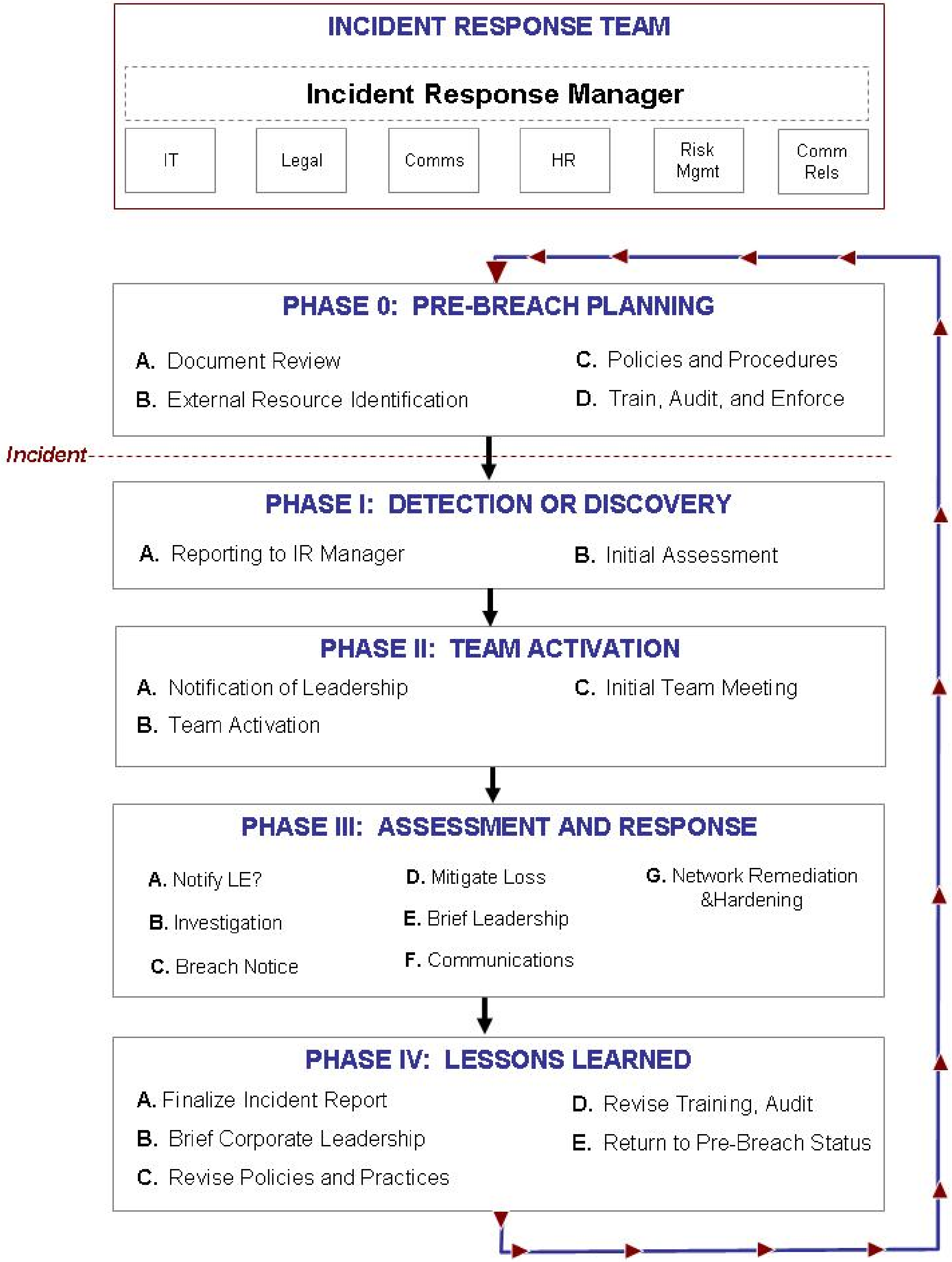
- Building and area access
- Workstation security

Technical Controls

- Firewalls, log aggregation and analysis, encryption, anti-virus
- Passwords, two-factor authentication

Incident Response Plan

Fig. 1 – SCENARIO C INCIDENT RESPONSE
Team Structure and Process



INCIDENT RESPONSE TEAM

Incident Response Manager

IT | Legal | Comms | HR | Risk Mgmt | Comm Rels

PHASE 0: PRE-BREACH PLANNING

A. Document Review

B. External Resource Identification

C. Policies and Procedures

D. Train, Audit, and Enforce

Incident

PHASE I: DETECTION OR DISCOVERY

A. Reporting to IR Manager

B. Initial Assessment

PHASE II: TEAM ACTIVATION

A. Notification of Leadership

B. Team Activation

C. Initial Team Meeting

PHASE III: ASSESSMENT AND RESPONSE

A. Notify LE?

B. Investigation

C. Breach Notice

D. Mitigate Loss

E. Brief Leadership

F. Communications

G. Network Remediation &Hardening

PHASE IV: LESSONS LEARNED

A. Finalize Incident Report

B. Brief Corporate Leadership

C. Revise Policies and Practices

D. Revise Training, Audit

E. Return to Pre-Breach Status

Critical Questions

- What information do you collect?
- Where do you store it?
- How do you use is?
- With whom do you share it?
- How do you dispose of it?
- How is your network configured?
- What servers, clients, and devices are on your network?
- What software and applications do you run?
- How do you manage patches, updates, and antivirus?

Critical Questions - 2

- How do you control access?
- What are your logging practices?
- Who is on your incident response (IR) team?
- When did you last review, exercise your IR plan?
- When was your last security audit?
- When was your last penetration test?
- What 3d parties have access to your network, data?
- How is data security addressed in your hiring, training, and termination policies?
- How are your physical facilities secured?

Resources

- National Institute of Standards and Technology, ***Framework for Improving Critical Infrastructure Cybersecurity*** (Feb. 12, 2014) (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf)
- ISO/IEC 27000 series, ***Information Security Management Systems*** (available on amazon.com)
- The SANS Institute, ***The Critical Security Controls for Effective Cyber Defense*** (https://www.sans.org/media/critical-security-controls/CSC-5.pdf)
- The Center for Internet Security, ***Security Benchmarks*** (http://benchmarks.cisecurity.org/)
- Governance of Enterprise Security: ***CyLab 2012 Report*** (Carnegie Mellon University CyLab, May 2012) (http://globalcyberrisk.com/wp-content/uploads/2012/08/CMU-GOVERNANCE-RPT-2012-FINAL1.pdf)