WilmerHale Cybersecurity, Privacy and Communications Webinar Series

The Evolving Cybersecurity Landscape: Reviewing Trends in Data Breaches and Incident Response

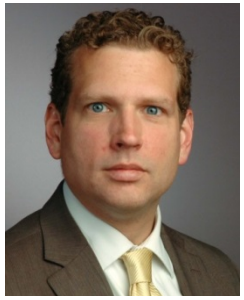
July 28, 2015

Attorney Advertising

WILMERHALE

Speakers

Benjamin A. Powell
Co-Chair Cybersecurity, Privacy and Communications Practice; Defense and National Security



Jason C. Chipman
Cybersecurity, Privacy and Communications; Defense and National Security

Webinar Logistics

- Participants are in listen-only mode
- Submit questions via the Q&A box on the bottom right panel
- Questions will be answered as time permits
- Offering CLE credit in California and New York*
- WebEx customer support: +1 888 447 1119, press 2

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. Texas CLE credit is pending. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Please note that no partial credit will be awarded. Attendees requesting CLE credit must attend the entire program.

Cybersecurity Landscape

Breach Preparation

Breach Response

Case Study

Regulatory Guidance

Cybersecurity Landscape

Threats	Regulatory/Standards	Corporate Response
Criminals	FTC	Board Interest
Hacktivists	State AGs	Cybersecurity Resources
Espionage	SEC	Incident Response Planning
Insiders	DOJ	Vendors and 3rd Party Connections
	NIST	Brand reputation
	Financial Regulators	
	HHS	
	DOD	
	Payment Card Industry	
	Insurers	

Cybersecurity Landscape

Breach Preparation and Response

Litigation

Case Study

Regulatory Guidance

Cybersecurity Lifecycle

Before	Cybersecurity Counseling and Reviews	Incident Response Planning	Corporate Governance
During / After	Investigation: Containment, Remediation, Forensics	Notice / Regulatory Obligations	Communications: Media Law Enforcement Customers
	* * *		
	Litigation	Regulatory Inquiries	Audit

Preparing for an Incident

- **Internal Planning**
  - ✓ Clarity of roles and responsibilities
  - ✓ Type and location of data
  - ✓ Cybersecurity reviews and results
  - ✓ Management and board involvement
  - ✓ Contract terms and conditions on security
- **Forensic Firm(s) Selection**
  - ✓ Engagement terms
  - ✓ Familiar with IT team and systems
- **Engagement of Other Third Parties**
  - ✓ Legal
  - ✓ Media
  - ✓ Notice / Credit Monitoring

Immediate Breach Response

Understand the Incident

- ❑ Stop further exploitation
- ❑ First reports often incomplete
- ❑ Remediation

Communications

- ❑ Board and Audit Committee
- ❑ Suppliers and customers
- ❑ Public Statements / Market

Investigate

- ❑ Forensics
- ❑ Legal Privilege

Regulators / Law Enforcement

- ❑ Coordinate with FBI, Secret Service, state officials, others
- ❑ SEC / Auditors / State AGs / FTC / Others

Cybersecurity Landscape

Breach Preparation and Response

Litigation

Case Study

Regulatory Guidance

Breach Litigation | Common Claims

Consumer and Employee Class Action Suits

- **State Common Law Claims**
  - Negligence
  - Breach of Contract or Express/Implied Covenants
  - Loss of Privacy
- **State Statutory Claims**
  - Data Breach and Breach Notification Statutes
  - Consumer Protection Statutes
  - Workers Compensation Laws

Example Class Action Allegations

- Vendors
  - Segmentation
  - Improper supervision
- Passwords / Encryption
  - Failure to encrypt sensitive data at rest
  - Improper storage of passwords
  - Insufficiently complex passwords
- Notice
  - Insufficient response to past warnings/incidents
  - Insufficient notice to customers
- System Architecture
  - Failure to update anti-virus software in response to recent attacks
  - Failure to deploy purchased tools
  - Improper software matching
  - Poor system monitoring
  - Default accounts

Example FTC Enforcement Allegations

- Wyndham
  - Use of default or insufficiently complex passwords
  - Failure to remedy known vulnerabilities
  - Poor segmentation between independent networks
  - Insufficient monitoring
- Snapchat
  - Failure to configure API properly
  - Failure to restrict serial/automated account creation
- Twitter
  - Poor security for privileged/administrative users
  - Failure to restrict administrative access
- TJX
  - Failure to limit wireless access
  - Weak passwords
  - Failure to patch/update anti-virus software
  - Failure to respond to security warnings

Cybersecurity Landscape

Breach Preparation and Response

Litigation

Case Study

Regulatory Guidance

The OPM Breach: June Announcements

June 4, 2015: OPM announces breach that involves 4.2 million current and former federal government employees.

- Impacts personnel data, including names, birth dates, home addresses, and Social Security Numbers.
- Breach discovered in April

June 12, 2015: Investigators discover a “second breach.”

- Impacts Social Security Numbers and other personal data, such as finger prints and mental health backgrounds, of 21.5 million individuals (19.7 million applicants and 1.8 million non-applicants, such as spouses of applicants).

The OPM Breach: What Happened?

Source of breach not announced but reports suggest:

- ✓ Two-factor authentication not implemented
- ✓ Potential compromise of user credential from third-party contractor
- ✓ Espionage is motive
- ✓ Segmentation issues

Confusion about impact :

June 16, 2015	Media estimates 14 million people affected by the breach.
June 23, 2015	FBI Director estimates 18 million people affected.
June 25, 2015	U.S. Intelligence Chief confirms China is chief suspect.
July 9, 2015	OPM declares 21.5 million individuals affected.
July 10, 2015	OPM Director Katherine Archuleta resigns.

The OPM Breach: Pre-Incident Reviews

Nov 2014 Office of the Inspector General (OIG) audit report identifies several problem areas related to OPM's IT security program, including:

- "Significant deficiency" related to information security governance
- 11 major information systems operating without valid authorization
- Failure to maintain a comprehensive inventory of servers, databases, and network devices
- Multi-factor authentication not required to access OPM systems

March 2015 OIG Semi-Annual Report summarizes IT security deficiencies from prior several years and highlights continuing concerns in light of recent attacks involving OPM and its contractors

The OPM Breach: Notice to Impacted Individuals

ID theft protection for *First Breach*

- ✓ 18 months free credit monitoring
- ✓ Switchboard jammed
- ✓ Problems causing delays in notice for Second Breach

ID theft protection <u>planned</u> for *Second Breach*

- ✓ Announced different, more robust protections (theft insurance, identity restoration, continuous credit monitoring for victim and minor children)
- ✓ Capacity issues

Cybersecurity Landscape

Breach Preparation and Response

Litigation

Case Study

Regulatory Guidance

Guidance on Vulnerabilities / Best Practices

- Federal Trade Commission Guidance
  - ✓ Control access to data
  - ✓ Password security
  - ✓ Secure storage and transmission of sensitive data
  - ✓ Segment network and have intrusion detection system
  - ✓ Secure remote access for employees and third parties
  - ✓ Security of service providers
  - ✓ Patching software
  - ✓ Address security vulnerability reports

Guidance on Vulnerabilities / Best Practices

- White House Post-OPM Guidance
  - ✓ Patch critical vulnerabilities without delay
  - ✓ Tighten policies and practices for privileged users
  - ✓ Dramatically accelerate implementation of multi-factor authentication, *especially for privileged users*
- Department of Justice Guidance
  - ✓ Identify mission-critical assets
  - ✓ Develop an actionable incident response plan
  - ✓ Use appropriate technology / services
  - ✓ Obtain consent for network monitoring
  - ✓ Consult outside counsel
  - ✓ Create information-sharing relationships
- Other Guidance and Best Practices

Thank You and Contact Information

Benjamin A. Powell
Co-Chair Cybersecurity, Privacy and Communications Practice; Defense and National Security

+1 202 663 6770
benjamin.powell@wilmerhale.com

Jason C. Chipman
Cybersecurity, Privacy and Communications; Defense and National Security

+1 202 663 6195
jason.chipman@wilmerhale.com

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. Texas CLE credit is pending. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Please note that no partial credit will be awarded. Attendees requesting CLE credit must attend the entire program.