EPSTEIN
BECKER
GREEN

The Age of Data Breaches:

HOW TO AVOID BEING THE NEXT HEADLINE

MARCH 24, 2015

This presentation has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal, state, and/or local laws that may impose additional obligations on you and your company.

Cisco WebEx can be used to record webinars/briefings. By participating in this webinar/briefing, you agree that your communications may be monitored or recorded at any time during the webinar/briefing.

Attorney Advertising

Presented by

Patricia Wagner

Partner

pwagner@ebglaw.com

Adam Solander

Partner

asolander@ebglaw.com

EPSTEIN BECKER GREEN

Agenda

1. What Not To Do: How Breaches Occur
2. What To Do: Managing Corporate Risk Exposure
3. Response Readiness
   i. Prepare and prevent
   ii. What to do if there's a breach: Response Roadmap
   iii. Organizational Priorities: Getting buy-in
4. Next Steps & Takeaways

EPSTEIN BECKER GREEN

EPSTEIN
BECKER
GREEN

WHAT NOT TO DO:

How Breaches Occur

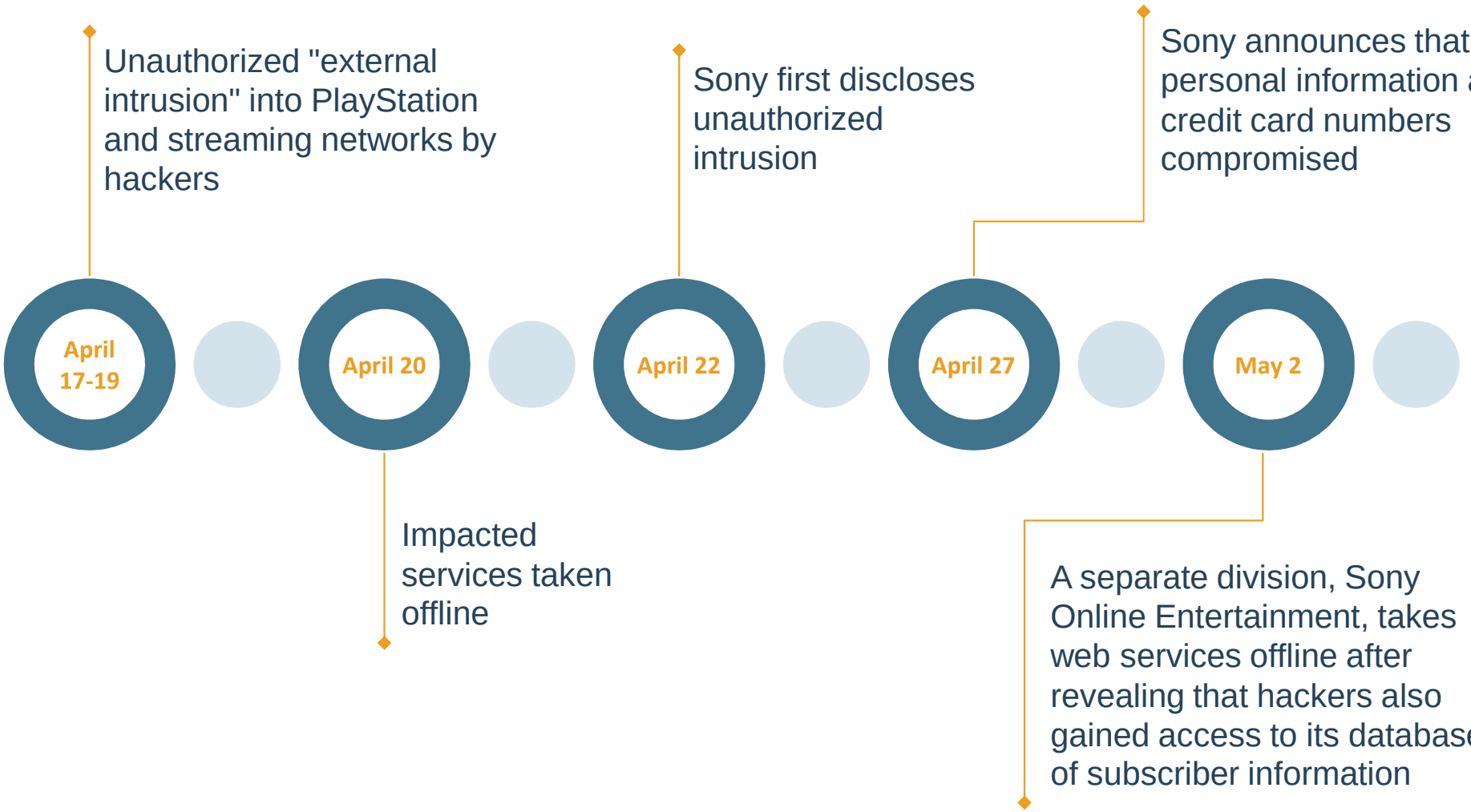
How Breaches Occur

ALL INFORMATION HAS VALUE

- Malicious Actors are targeting personal, payment, and health information that is maintained by all kinds of organizations
- Recent examples include:
  - Sony (2011 & 2014)
  - Stanford
  - TerraCom & YourTel
  - LabMD
- Valuable organizational lessons may be gleaned from each of these examples

How Breaches Occur

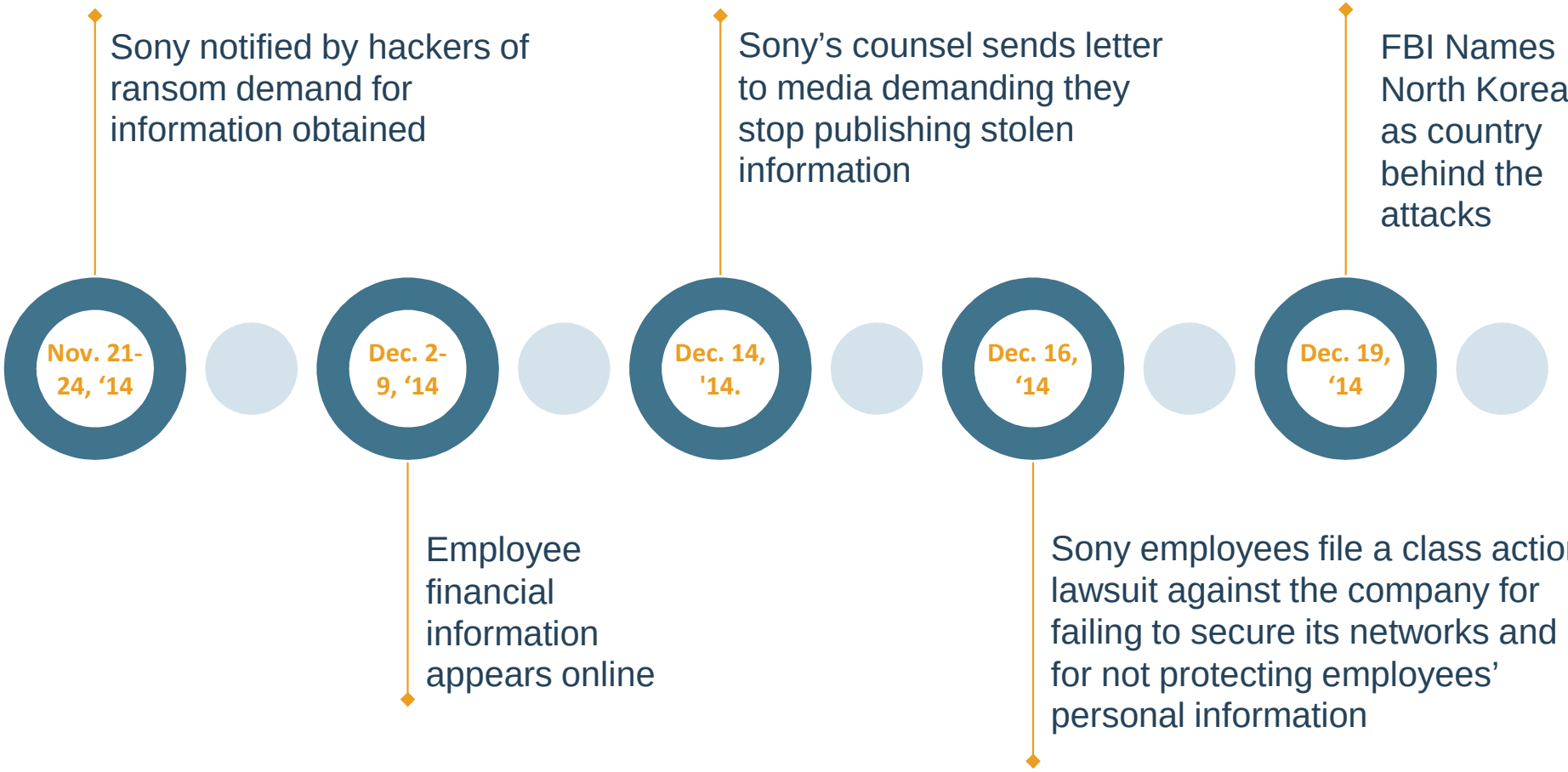
SONY 2011 PLAYSTATION NETWORK: CUSTOMER PAYMENT INFORMATION



EPSTEIN BECKER GREEN

How Breaches Occur

SONY 2014 BREACH: EMPLOYEE PERSONAL INFORMATION



EPSTEIN BECKER GREEN

How Breaches Occur

SONY 2011 & 2014 INCIDENTS

Repercussions…

	2011	2014	TOTAL
Cost of Breach Response	$171 M	$100 M	$271 M
Fines	$250 K GBP	Possible	> $250 K GBP
Lawsuit	$15 M	Pending	> $15 M

EPSTEIN BECKER GREEN

How Breaches Occur

STANFORD & MULTI-SPECIALTY COLLECTION: FAILURE TO SECURE DATA

- Medical information of approximately 20,000 patients treated in the hospital's emergency room between March 1, 2009, and Aug. 31, 2009, was illegally displayed on a public website for nearly a year, beginning on Sept. 9, 2010
- It was identified that this was due to an error by the hospital's Business Associate (Multi-Specialty Collection Services) leading to ePHI being available through Internet
- **Settlement: $4.1 M to settle class-action lawsuit**

One report suggests that as many as 63% of breaches may be caused by improperly vetted outsourcing

Trustwave 2013 Global Security Report, http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

EPSTEIN BECKER GREEN

How Breaches Occur

TERRACOM & YOURTEL: IMPROPERLY CONFIGURED SERVERS

- TerraCom and YourTel collected the names, addresses, Social Security numbers, copies of driver's licenses, and other proprietary information and stored the information in electronic forms on Internet servers without password protection or encryption that could be accessed by anyone
- These improperly configured servers made customer records publicly available (170,000 individuals)
- TerraCom and YourTel were found to have willfully and repeatedly violated the Communications Act and the FCC's rules for for their failure to protect the confidentiality of subscribers' personal information from misappropriation by third parties
- **FCC Fine: $10 M**

How Breaches Occur

LABMD: BILLING INFORMATION SPREAD BY P2P SOFTWARE

- LabMD Inc. is a medical testing laboratory based in Atlanta
- Complaint filed by FTC for allegedly failing to "reasonably protect the security of consumer's personal data" and medical information.
- A spreadsheet containing 9,000 consumers' billing information — including Social Security numbers, dates of birth, health insurance provider information and standardized medical treatment codes — was found on a P2P network.
- FTC stated "Misuse of such information can lead to identity theft and medical identity theft, and can also harm consumers by revealing private medical information."
- **Fine: Case is still pending. LabMD's challenge to the FTC's enforcement authority in this instance was dismissed**

EPSTEIN
BECKER
GREEN

WHAT TO DO:
Managing Corporate Risk Exposure

Managing Corporate Risk Exposure

3 BASIC TENETS

EPSTEIN BECKER GREEN

Managing Corporate Risk Exposure

KNOW YOUR WEAKNESSES

- Security risks to data vary according to the nature of your business
- The Verizon breach report identifies how breaches occur across selected industries

INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

EPSTEIN BECKER GREEN

Managing Corporate Risk Exposure

KNOW YOUR WEAKNESSES: 9 MOST COMMON SHORTCOMINGS

Lack of system activity review	Lack of encrypted offsite data backup	Lack of email encryption
Lack of laptop encryption	Lack of mobile encryption (smartphones / tablets / USB drives, etc.)	Lack of anti-virus on all endpoints and servers
Lack of security patching of servers and desktops	Lack of security penetration and vulnerability testing	Lack of security incident response procedures

EPSTEIN BECKER GREEN

Managing Corporate Risk Exposure

QUANTIFY THE IMPACT

- There are many, many direct and indirect organizational burdens associated with a data breach
- Direct Costs of Breach (Ponemon report)
  - Average cost is $5.9 million per organization
  - Average of $201 per record affected
  - Malicious attacks are the most expensive to resolve: average of $246 per record; human error is least expensive at $160 per record
- Reputational/Customer Fear: Average loss of business is $3.2 million
- Good business continuity management reduced cost of breach
- $1.6 million in post-breach-response costs (i.e., addressing victim, regulator, and plaintiff counsels' concerns)

Source: Ponemon Institute, 2014 Cost of Data Breach: Global Analysis, http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

EPSTEIN BECKER GREEN

Managing Corporate Risk Exposure

REPORT APPROPRIATELY – IGNORING IT DOESN'T MAKE IT GO AWAY!

- Follow the organizational policies and procedures regarding breach response protocol
- Don't fail to report, when appropriate
- Many examples of enforcement actions by state and federal governments for failure to report
  - 2013/2014: A local, Vermont country store settled an enforcement action over its failure to report a 2013 breach compromising online customers' data.
    - According to the Vermont Attorney General, this "send[s] a warning to businesses of all sizes that they need to be aware of their data breach notification obligations"
  - 2010: Lucile Salter Packard Children's Hospital at Stanford University was fined $250,000 by California health officials for failing to report a breach of 532 patient medical records within 5 days of an apparent theft of a hospital computer by an employee

EPSTEIN
BECKER
GREEN

Response Readiness

Response Readiness

PREPARE AND PREVENT

- Implement strong organizational policies
  - Policies should be specific and instructional
  - Procedures should identify core responsibilities and responsible parties
- Be comprehensive
  - Policies & Procedures should be clear, actionable, and reviewed periodically
  - All organizational employees should be aware of and trained to follow policies and procedures
  - Explicitly state sanction policies and disciplinary measure for non-compliance
- Make sure policies address relevant points of law
- Compliance is king

Institute a good compliance program with routine checks and implement feedback mechanisms to measure compliance and update policies

Response Readiness

ORGANIZATIONAL PRIORITIES

Assess Risks ★	Check for Vulnerabilities ★★	Demonstrate Compliance ★★★
▪ Comprehensive and periodic risk assessments are the basis of a reliable compliance program and include • Technical investigations • Organizational inspections • On-site inspections	▪ Perform vulnerability and penetration testing ▪ Ensure IT staff are appropriately qualified and trained ▪ Patching and update IT infrastructure: • Anti-virus, anti-malware • Regular checks are necessary	▪ Demonstrate compliance to internal and external clients as well as enforcement agencies • HITRUST • PCI • ISO, COBIT, NIST

EPSTEIN BECKER GREEN

Response Readiness

EVOLVING LEGAL LANDSCAPE: EXAMPLES

- **FEDERAL:** Obama's focus on cyber security
  - Obama said the prospect of cyber attacks are one of the nation's most pressing national security, economic and safety issues
  - In an executive order signed in February 2015, Obama encourages the development of central clearinghouses for companies and the government to share data and creation of centers where data can be shared across specific geographic regions
  - Obama also pushed for collaboration between the public and private sectors
- **STATE:** New York Data Breach Law Proposed by State Attorney General
  - Independent third-party audits and certifications would offer a rebuttable presumption of having reasonable data security

Source: A.G. Schneiderman Proposes Bill To Strengthen Data Security Laws, Protect Consumers From Growing Threat Of Data Breaches, http://www.ag.ny.gov/press-release/ag-schneiderman-proposes-bill-strengthen-data-security-laws-protect-consumers-growing

Response Readiness

RESPONSE ROADMAP

Disaster recovery and business continuity planning	These should be in place well before any breach; it is important to practice them and follow them when a breach occurs
Investigation and determination of whether a breach has occurred and its scope	Sometimes it turns out information has not been accessed, and thus a breach has not occurred and no reporting requirements kick in
Notification of proper authorities	Different states have widely varying reporting periods and it is critical to ensure compliance with all applicable federal and state laws
Preemptive representation agreements	The best way to get a fast start and prompt breach response and mitigation

Response Readiness

ORGANIZATIONAL PRIORITIES: GETTING BUY-IN

- Top-Down Approach
  - Convince the Board & C-Suite
  - Focus on economics

- Bottom-Up
  - Employee and partner training
  - Rewards & incentive programs
  - Make the “Ground-up” investment in compliance

Organizations with a formal incident response plan in place prior to an incident achieved a lower per record data breach cost of $17 versus $21

EPSTEIN
BECKER
GREEN

Where To Go From Here…

Response Readiness

ORGANIZATIONAL PRIORITIES: GETTING BUY-IN

1. Prepare and prevent

- Put good policies into place
- Review and critically assess your existing policies
- Perform gap analyses and have your policies vetted by third parties

2. Perform regular risk assessments

- Comprehensive and annual assessment are critical

3. Pursue outside certification

- Demonstrate compliance and readiness to internal and external clients

4. Be prepared

- Have adequate disaster recovery and business continuity plans
- Make arrangements for the event of a breach

EPSTEIN
BECKER
GREEN

Questions?

Presented by

Patricia Wagner

Partner

pwagner@ebglaw.com

Adam Solander

Partner

asolander@ebglaw.com

EPSTEIN BECKER GREEN