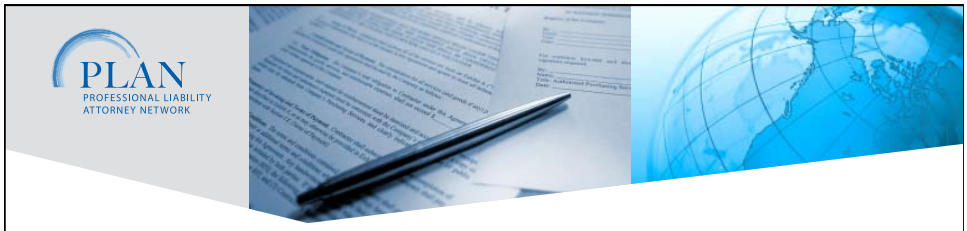
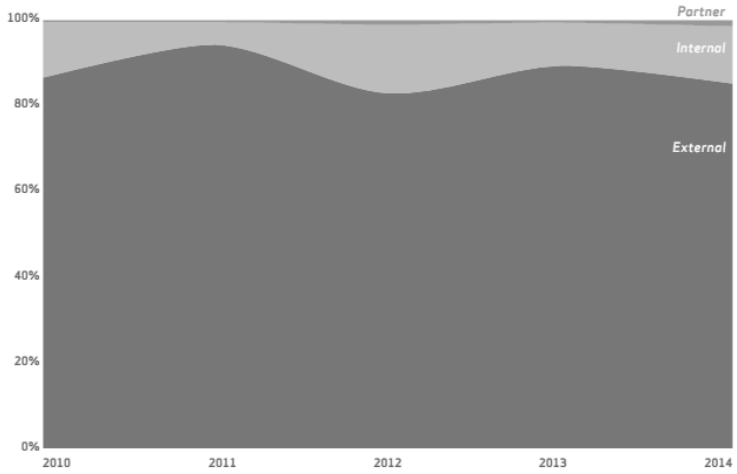



# Trends in Data Security and Privacy Litigation and Insurance

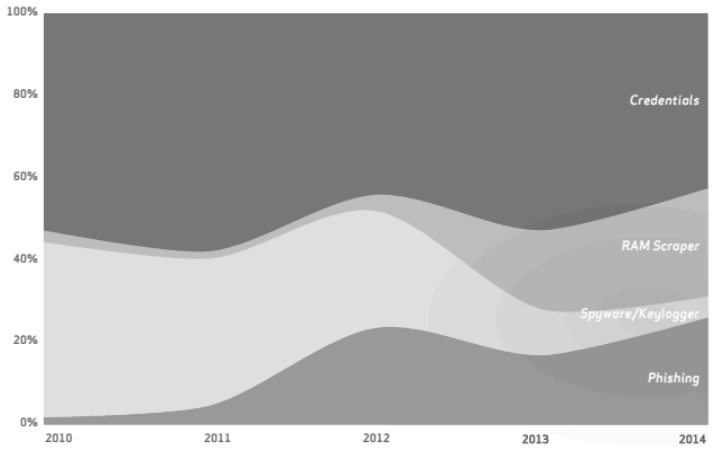
## 2015 Verizon Data Breach Report

- 79,790 security incidents
- 2,122 confirmed data breaches
- Top industries affected: Public, Information, and Financial Services (same as prior years)
- But numbers show that no industry is immune

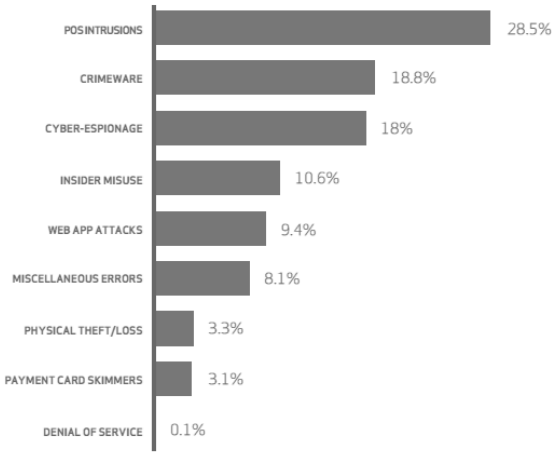
# Verizon Report: Threat Actors




# Verizon Report: Threat Actions



# Verizon Report: Incident Types




# 2015 Ponemon Cost of Data Breach Study

- $217 average cost per lost or stolen record
- Healthcare, pharmaceutical, financial, energy, and transportation, communications and education tend to have higher costs
- Incident response plan, extensive use of encryption, employee training, board-level involvement, and insurance protection had most significant impact on reducing costs

## Cyber Market Issues

- Types of coverage available
- Carriers dropping from the cyber market
- Mergers of insurance carriers
- Varying products by company
- Varying policy language by company

## Who Was Buying Cyber

- Big companies v. small to midsize companies
- Was it industry specific?
- What were the driving forces for the purchasing decisions?
- What products were sold?
- How much is dependent on the agent/broker?
- Stand alone policies v. endorsements
- Is any of this changing?

## Article III Standing

- *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013) - expenditure of money to prevent surveillance was a form of manufactured standing
- Alternate theories of harm
  - Lost time and inconvenience
  - Emotional distress
  - Decreased economic value of PII
  - Denied benefit of the bargain
  - Statutory damages

## Lack of Standing

- *Whalen et al. v. Michaels Stores, Inc.*, No. 14-CV-7006 (E.D.N.Y. Dec. 28, 2015) – court dismissed class action lawsuit based on 2014 payment card breach for lack of standing
- *In re: SuperValu Inc. Customer Data Security Breach Litigation*, No. 0:14-cv-03252 (D. Minn. Jan. 8, 2016) – single incident of fraudulent purchase not fairly traceable to the data breach

## *Resnick v. AvMed*, 693 F.3d 1317 (11th Cir. 2012)

- Two laptops stolen from corporate office with names, SSNs, addresses, and phones
- Injury: plaintiffs were victims of identity theft and suffered monetary damages
  - Bank accounts and credit cards opened
  - Home address changed with USPS
  - E*Trade account opened and overdrawn
- Causation: allegations of negligent care for laptops, no encryption, and timing of ID theft

## Remijas v. Neiman Marcus Grp., LLC, No. 14-3122 (7th Cir. 2015)

- First circuit court *post-Clapper* to confer standing based on possibility of future harm
- "Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing."
- Mitigation costs can support injury-in-fact where harm is imminent, and suggested that offer of credit monitoring and ID-theft protection to all customers was "telling."

# Collection, Use, and Transfer of PII

- Inability to establish injury led to failure of several putative class actions in 2015, most notably in a series of cases alleging that companies allowed PII about customer Internet browsing history to be collected and sent to Facebook
  - *In re: Hulu Privacy Litigation*, — F. Supp. 3d —, No. 3:11-cv-03764 (N.D. Cal. Mar. 31, 2015) (granting summary judgment)
  - *Carlsen v. GameStop, Inc.*, — F. Supp. 3d —, 2015 WL 3538906, at *6 (D. Minn. June 4, 2015) (granting motion to dismiss)
  - *Austin-Spearman v. AARP and AARP Services, Inc.*, — F. Supp. 3d —, 2015 WL 4555098 (D.D.C. July 28, 2015) (same).

# Standing re: Medical Breaches

- *Walker et al v. Boston Medical Center Corp.*, No. 2015-1733-BLS 1 (Mass. Sup. Ct. Nov. 19, 2015) –
  - Medical records inadvertently made accessible through website of an independent medical record transcription service
  - Plaintiffs do not allege that any unauthorized persons actually viewed, accessed or misused their medical information
  - Nonetheless, court denied motion to dismiss, reasoning that pleading a "real and immediate risk" of injury was sufficient for a plaintiff to demonstrate standing.

## Shareholder Derivative Suits

- State laws generally do not to permit shareholders to use the duty of oversight to second-guess well-informed business decisions
- But inadequate oversight can serve as a basis for individual board member liability where:
  - Directors consciously failed to implement any reporting or information system or controls; or
  - Directors, having implemented such system or controls, consciously failed to oversee its operations and thus failed to be informed of risks

## Shareholder Derivative Suits

- In re Home Depot –
  - Alleges that directors and officers breached fiduciary duties of loyalty and good faith by failing to adequately oversee the company's cybersecurity functions
  - Claims data breach damaged company by exposing it to massive consumer litigation, regulatory investigations, and millions of dollars in related fees and costs

## Shareholder Derivative Suits

- In re Target –
  - Alleges the board and executives "knew or should have known that the company had failed to meet industry standards with its security systems and left its technologies unreasonably vulnerable rendering its customers a target of attacks by nefarious third parties"
  - Further claims they "aggravated the damage to customers by failing to provide prompt and adequate notice to customers and by releasing numerous statements aimed to create a false sense of security to affected customers"

## What Should D&Os Do?

- Be educated on cybersecurity risks to understand the company's risks and control measures
- Establish a committee or appoint one director to assume responsibility for cybersecurity oversight
- Perform a cybersecurity risk assessment
- Establish a data security policy and management plan
- Implement a data breach response plan
- Ensure the company has adequate cyber insurance coverage, including D&O coverage for alleged breaches of fiduciary duty in connection with a breach

# Agency Enforcement

- FTC is pursuing alleged failures to provide adequate security or follow promises or policies about use or security of consumer information as unfair and deceptive trade practices under Section 5 of the FTC Act
- *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3rd Cir. 2015) – failure to follow published privacy policies or take reasonable measures to safeguard data can constitute an unfair trade practice

# Agency Enforcement

- Baker Hostetler report: regulators investigated 31% of breaches; AG offices investigated 5%; and OCR investigated 100% of medical breaches involving over 500 records
- Report the Office of the Inspector General (OIG) issued in October 2015 called for stronger, more proactive oversight from OCR.
- OCR agreed with the recommendation that its enforcement action should be increased and noted that it would be implementing Phase 2 of a permanent audit program beginning in 2016

## Cyber Security Meets Product Liability

- Internet of Things
- *U.S. Hotel and Resort Management, Inc. v. Onity, Inc.* (D. Minn. July 30, 2014)
  - Is vulnerability to hacking a "defect"?
  - Is defect alone an injury?
  - Is warranty against hacking implied?

## Online Privacy and Defamation

- SunEnergy1, LLC et al v. Jeffery Brown, No. N14M-12-028 (Sup. Ct. Del. Nov. 30, 2015).
  - "The right to discover the identity of an anonymous author alleged to have made defamatory statements must be balanced against the author's First Amendment right to free speech and to remain anonymous."
  - Statements on Glassdoor.com were statements of opinion only, and no reasonable person could interpret them otherwise. Therefore, not defamation, as a matter of law, and no basis to compel identity of the poster

# Employee Misuse of Data

- Federal circuits are split whether an employee acts "without authorization" under CFAA when he or she steals employer confidential data at or near termination.
  - Second, Ninth, and Fourth Circuits: as long as employee was allowed to access the data, diversion of employer information is "authorized" under CFAA
  - First, Fifth, Seventh, and Eleventh Circuits: allow CFAA claims for employee misuse of employer information that he or she was otherwise permitted to access

# Predictions for 2016

- Products
  - Growth of cyber towers
  - Expansion of coverage afforded
    - First Party
    - Third Party

  In what way will the coverage expand?

  Are there any risks that have become uninsurable?

# Predictions for 2016

- Underwriting
  - Choosing risks
  - Pricing
  - Overlapping coverage and its impact on placement
  - Position in the tower
  - Willingness to manuscript policies
  - Aggregation Issues

# Predictions for 2016

- Courts will continue trend of recognizing alternate theories of harm to find standing; class action suits will increasingly survive summary judgment and become more frequent
- Rise in claims as a result of agency enforcement activity from FTC and OCR in particular

# Predictions for 2016

- State data breach notification requirements will continue to expand
  - Expanded definition of personal information
  - Required reporting to AG or other agency
  - Required data security measures
- Targeted social engineering hacks will be the primary focus
- Ransomware attacks will continue to evolve
- Service provider due diligence will become more stringent and important