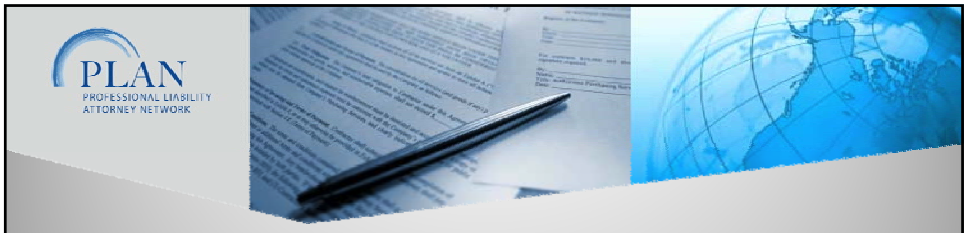


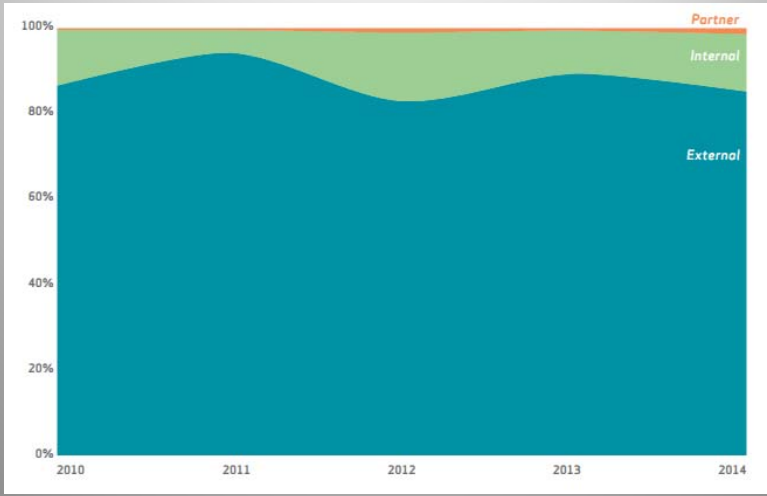
CYBER LIABILITY:

TRENDS AND DEVELOPMENTS: WHERE WE ARE AND WHERE WE ARE GOING

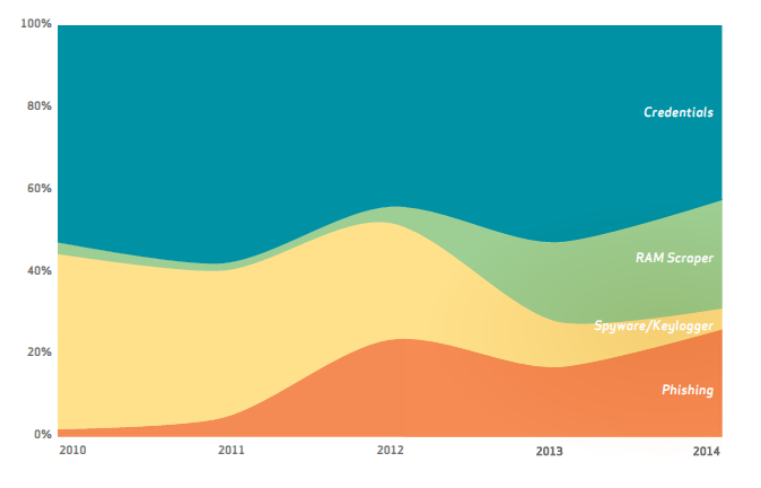
2015 Verizon Data Breach Report

- 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

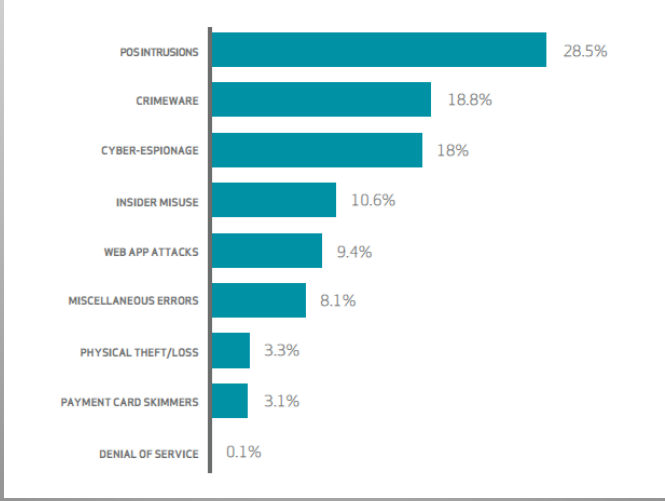
Verizon Report: Threat Actors



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/Data Privacy Products

First Party Coverage

- Breach Response
  - Forensics
  - Notification
  - Legal representation
- Crisis Management
- Reconstitution of electronic records
- Property coverage
  - Computer systems
  - Machinery
  - Business interruption
  - Lost profits

Third Party Coverage

- Response to regulatory investigation
- Defending against lawsuits

Cyber Market Issues

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

Underwriting Cyber

- What were the major underwriting concerns regarding cyber threats in 2014?
- Have they changed?
- How are those concerns being addressed in the underwriting process?
- Where was the underwriting data coming from?

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?

Types of Data Breach Cases

- Stolen or lost computer cases
  - Big factor: was data encrypted
  - How stolen or what happened with it afterwards
- Hacking incidents
  - Payment cards systems
  - Password theft
  - Theft of financial data
- Publication of personal information
  - Often arises in medical context
  - Non-profit posting of tax records

Applicable Law

- Federal law
  - HIPAA/HITECH
  - The Stored Communications Act (SCA)
  - The Fair Credit Reporting Act (FCRA)
  - The Gramm-Leach Bliley Act (GLBA)
- State law
  - Consumer protection or unfair trade practices
  - Negligence
  - Breach of express or implied contract
  - Invasion of privacy
- Self regulation: PCI DSS

Standing and Theories of Harm

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

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

Willingham v. Global Payments, Inc., 2013 WL 440702 (N.D. Ga. 2013)

- SCA claim: GPI not an ECS and did not "knowingly divulge" data to hackers
- FCRA claim: GPI not a CRA and did not "furnish" data to hackers – it was stolen
- Georgia UDTPA: injunctive relief to prevent future injury is sole remedy, but data already stolen
- Negligence: no duty of care and no evidence of what would be "commercially reasonable methods to safeguard" data
- Contract: plaintiffs not third party beneficiaries

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."

Today's Cyber Threats

- Malicious activity by hack-tivists
- Website defacements
- Denial of service (DDOS) attacks
- Destruction of information and systems
- Financial crimes and other frauds
- Theft of confidential business information and proprietary technology

Looking Forward – Current Trends

- 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?

Looking Forward – Current Trends

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

Looking Forward – Current Trends

- *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
- Baker Hostetler report: regulators investigated 31% of breaches; AG offices investigated 5%; and OCR investigated 100% of medical breaches

Target and Home Depot Litigation

- U.S. Dist. Court for Minnesota certified class action of banks and credit unions for restitution in Target data breach litigation
- But Home Depot recently filed motion to dismiss lawsuit by banks, arguing “The banks are sophisticated financial institutions asking the court to shift to Home Depot expenses they allegedly incurred as a result of their commercial decisions following a criminal's theft of data from Home Depot."

Other Issues on Horizon

- Chip and PIN transition effective Oct. 1
- Internet of Things litigation
  - Technology getting ahead of regulation
  - FTC and State AG focus
- Cyber security meets product liability
  - 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?

The Future of Cyber Crime

- More elaborate and more sophisticated
- Attacks that are industry-wide and impact our economy
- Theft of trade secrets and intellectual property
- National security implications
- Terrorism

Closing Questions

- Will a federal notification statute be enacted?
- Will uniform policy language and definitions be developed?
- What direction are we heading?