



Updates within Network Security and Privacy Risk Management

RIMS Minneapolis Meeting

Melissa Krasnow, Partner, Dorsey & Whitney LLP (Minneapolis, MN)

Mario Paez, Midwest Practice Leader for Tech., Privacy, Network Risk, Wells Fargo Insurance (Minneapolis, MN)

Vern Suckerman, Senior Underwriter, XL Catlin

Patrick Tatro, Senior Data Security Manager, Best Buy Corp.

October 20, 2015

This presentation was created by Dorsey & Whitney LLP, 50 South Sixth Street, Suite 1500, Minneapolis, MN 55402. This presentation is intended for general information purposes only and should not be construed as legal advice or legal opinions on any specific facts or circumstances. An attorney-client relationship is not created or continued by sending and/or receiving this presentation. Members of Dorsey & Whitney will be pleased to provide further information regarding the matters discussed in this presentation.

Agenda

- Recent breach statistics
- Legal update and the regulatory environment
- Underwriting insight & trends
- Information security perspective & threat trends

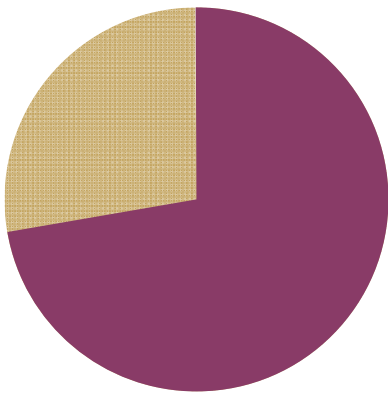
Statistics



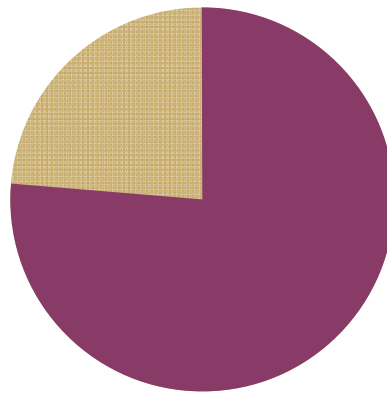
Verizon 2015 data breach investigations report

By the numbers

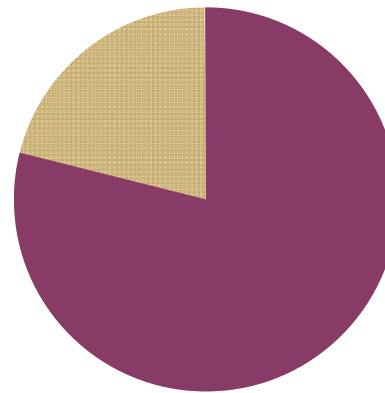
28.5% POS
intrusions



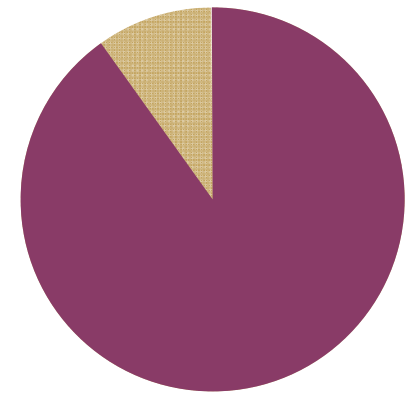
18.8%
crimeware



18% cyber
espionage



10.6% insider
misuse



2,122 confirmed
data breaches
(up from 1,367 in 2014)

79,790 reported
security incidents
(up from 63,437 in 2014)

61 countries
represented
(down from 95 in 2015)

NetDiligence 2015 claims study

Findings

Data type	Cause of loss	Business sectors
<ul style="list-style-type: none">▪ PII - 45%▪ PCI - 27%▪ PHI - 14%	<ul style="list-style-type: none">▪ Hackers - 31%▪ Malware virus – 14%▪ Staff mistakes – 11%▪ Rogue employees - 11%▪ Lost/Stolen Laptop/Device – 10%▪ Paper Records – 5%▪ System Glitch – 5% <p><small>*In 2013, stolen laptops were #1</small></p>	<ul style="list-style-type: none">▪ Healthcare sector - 21%▪ Financial services - 17%▪ Retail – 13%▪ Technology – 9%▪ Professional Services – 8%▪ Hospitality – 4%▪ Restaurants – 4%

Data

- Sample size – 160 insured claims

Company size

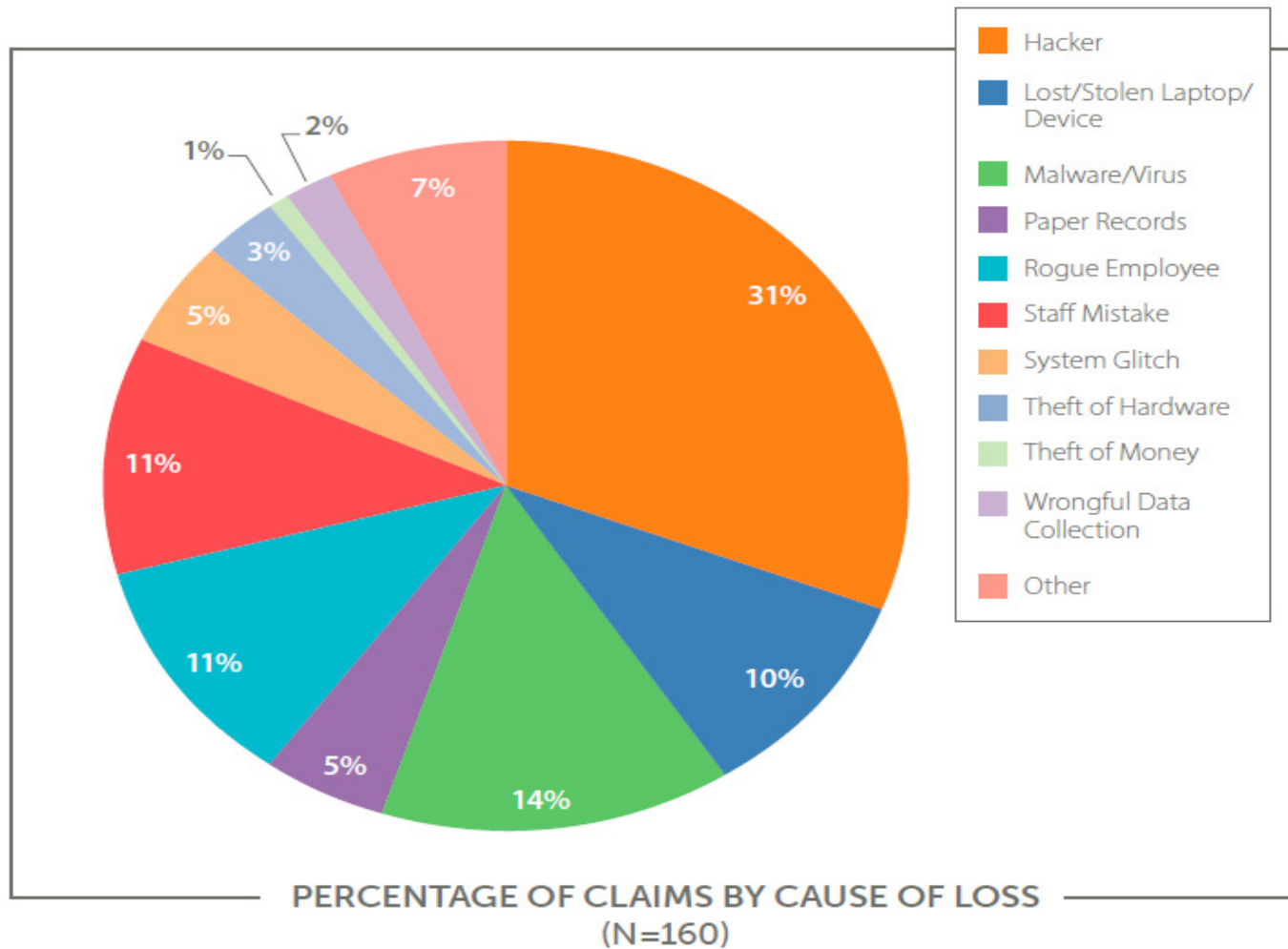
- Nano-cap (under \$50M revenue) & Micro-cap (\$50M-\$300M): 28% & 18% of incidents respectively
- Small-revenue (\$300M-\$2B revenue): 25% of incidents
- Large-revenue (\$10-\$100 billion) lost the most records (60%)(13% of incidents)

Additional notes

- The average cost of a claim was \$673,767
- Average claim for a “large” company was \$4.8 million
- Third parties accounted for 25% of the claims submitted

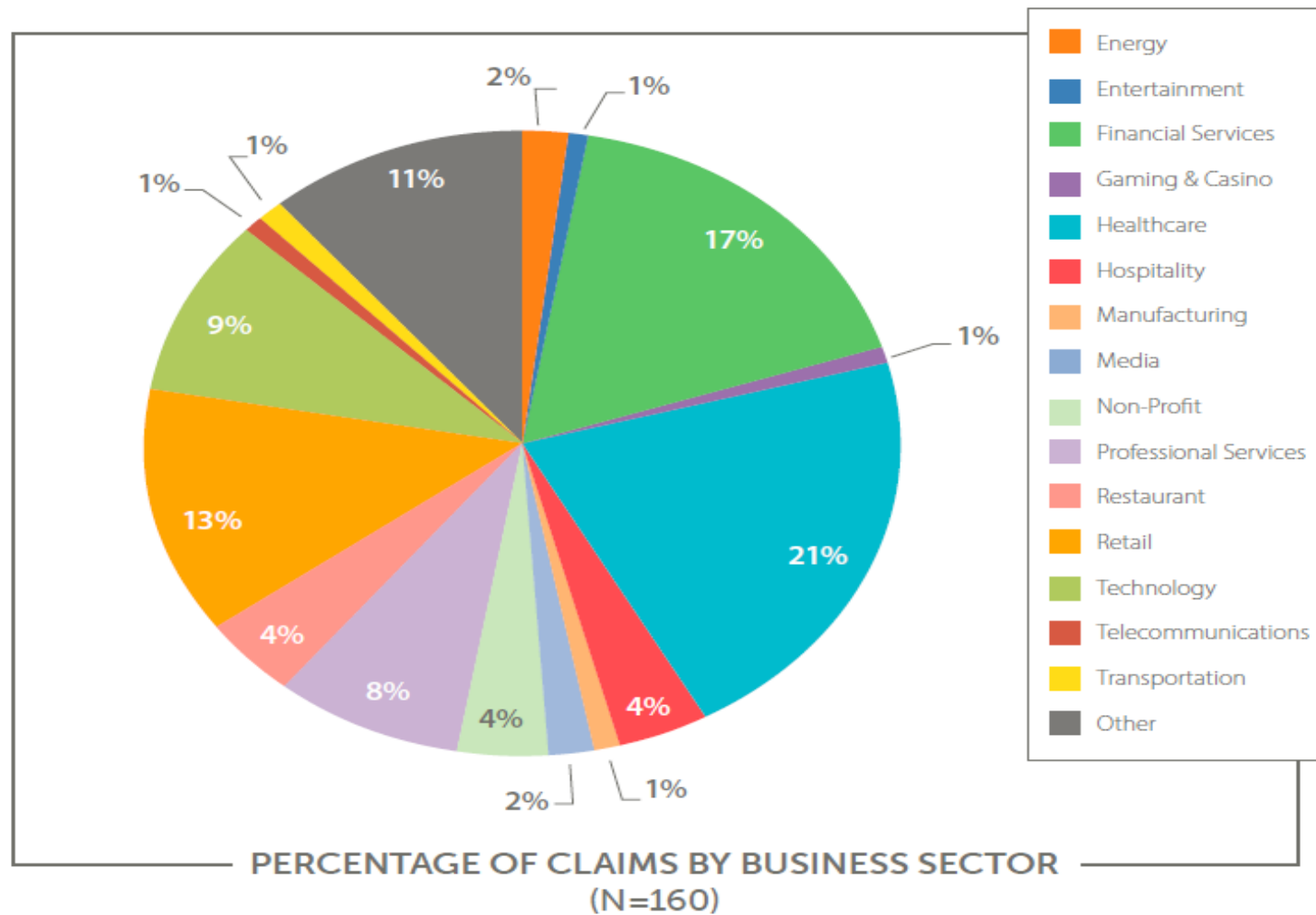
NetDiligence 2015 claims study

Percentage of breaches by cause of loss



NetDiligence 2015 claims study

Percentage of breaches by business sector



RIMS cyber survey 2015

- **51% of RIMS membership purchase stand-alone cyber insurance policies**
 - 58% of RIMS membership carry less than \$20M in cyber coverage.
 - 49% of those with under \$20M in coverage are paying over \$100k in premium.
 - 74% of those without cyber coverage in place are considering procuring coverage in the next 12-24 months.
- **The reported top three first party cyber exposures are:**
 - Reputational harm (79%);
 - Business interruption (77%);
 - Data breach response and notification (73%).



Current Regulatory Environment

2015 developments in state breach notification laws

- 47 states, plus the District of Columbia, Guam, Puerto Rico and Virgin Islands, have breach notification laws requiring breach notification to affected individuals; some of these laws have been amended

<http://www.irmi.com/articles/expert-commentary/state-breach-notification-laws-continue-to-change>

- Alabama, New Mexico, and South Dakota do not have breach notification laws
- Will there be a comprehensive federal breach notification law?

2015 developments in state cybersecurity laws and federal guidance

- Approximately 25% of states with breach notification laws also have security procedures laws; some of these laws have been amended

<http://files.dorsey.com/files/upload/Krasnow-MA-Data-Security-Regulation-mar-2015.pdf>

- Federal Trade Commission's Start with Security guidance

<https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>

2015 developments in incident response plan guidance; tabletop exercises; corporate governance

- Department of Justice's Best Practices for Victim Response and Reporting of Cyber Incidents

http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf

<http://www.irmi.com/articles/expert-commentary/guidance-for-incident-response-plans>

<http://www.irmi.com/articles/expert-commentary/board-oversight-of-cyber-risks-directors-and-officers-litigation>

Insurance Trends



Underwriting due diligence

- Organization of their Information Security Team
- Information Assets / Sensitive Information (including PII, PHI & PCI-DSS)
- Administrative Information Security Controls
- Physical Information Security Controls
- Technology Security (Encryption, VPN, DLP, Monitoring, Scanning)
- POS Security / Controls (Retail/Hospitality/Etc.)
- Vendor Management
- Incident Response Plan
- Business Continuity Plan
- Audits/Testing
- Claims/Breaches
- Future Projects

Cyber underwriting trends / Insurance considerations

- Industry
 - Retail/Hospitality
 - Healthcare
 - Financial services
 - Schools/Public entities
- Understand what is included within the Definitions of the First Party Coverages when evaluating limits provided
- First Party coverage Triggers - Wrongful Act versus Knowledge of Executive Officers
- Notified Individuals versus Dollar Limit Approach (Required Vendor vs Flexibility of Vendors)
- PCI-DSS Coverage:
 - What does it cover?
 - Limits?
 - Carveback of Contractual Liability Exclusion
- Other Coverages to Purchase:
 - Business Interruption (Security failure vs. System failure)
 - Data Loss / Restoration
 - Dependent Business Interruption
 - Network or Systems Failure
 - Reputational Damage (mostly London markets)
- Medial Liability – Electronic Media vs Broad Form Media

Insurance claims takeaways


- Most significant claims activity have been on Healthcare and Retail
 - Healthcare – malware and lost laptops/removable devices
 - Retail – malware on POS network
 - Financials Services
- Frequency of activity on the public entity side (CryptoLocker claims)
- Utilities
- Many Human Error type incidents
 - Lost laptops and other removable devices.
 - Data Loss incidents – inadvertent emails with confidential information
- Media Claims
 - Invasion of privacy (example emails and other communications)
 - Intellectual Property



Threat Landscape



Who's Got Your 6?

A photograph of a group of people playing poker in a casino. The players are seated around a green felt table, which is marked with a yellow line and the words "CASINO". They are dressed in formal attire, including tuxedos and gowns. The background shows other casino patrons and a large, ornate chandelier. The scene is dimly lit, with warm lighting from the chandelier and other sources.

Information Sharing