CyberCrime Symposium 2016

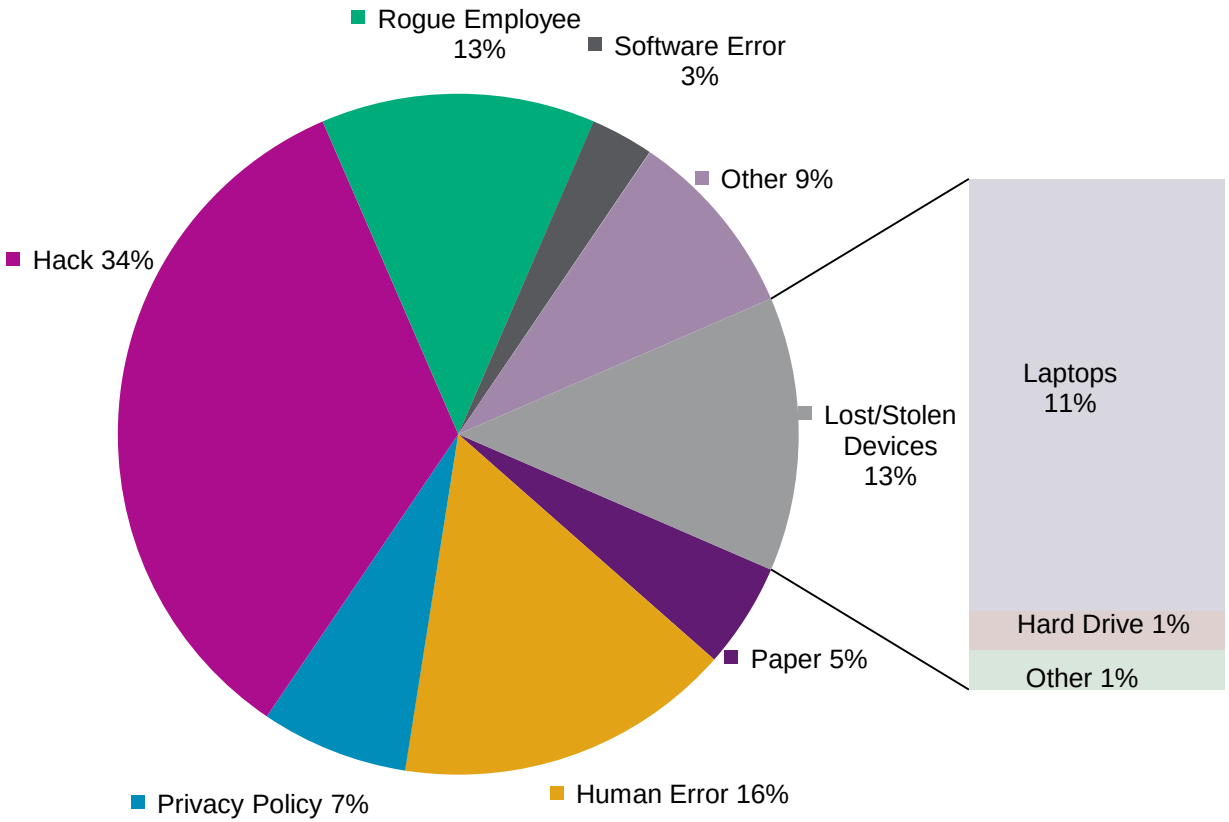
Got Coverage? Cyber-Insurance Realities Revealed

Peter Foster, Executive Vice President, FINEX Cyber/E&O Team

November 4, 2016

Key Trends and Recent Developments

How are Network Breaches Occurring?



Industry Breakout 2013-2015:

- Healthcare – 31%
- Technology – 9%
- Professional Services – 15%
- Retail – 9%
- Financial Institutions – 6%

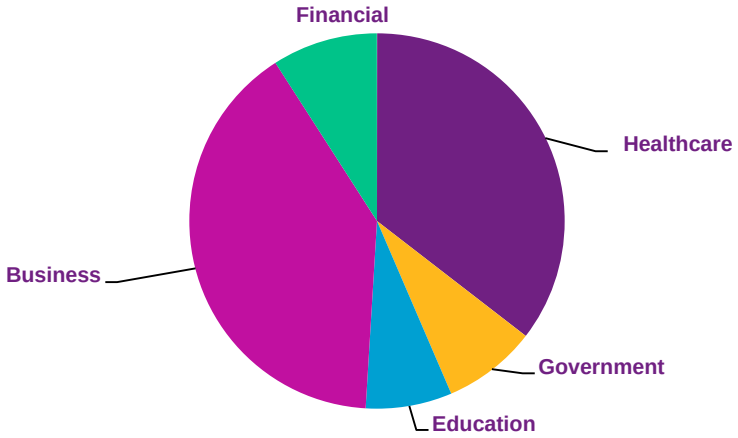
Targeted Attacks for PII:

- Lost/Stolen Devices
  - 2013 – 17%
  - 2014 – 12%
  - 2015 – 11%
- **Hack**
  - 2013 – 29%
  - 2014 – 27%
  - 2015 – 43%
- **Rogue Employee**
  - 2013 – 14%
  - 2014 – 16%
  - 2015 – 11%

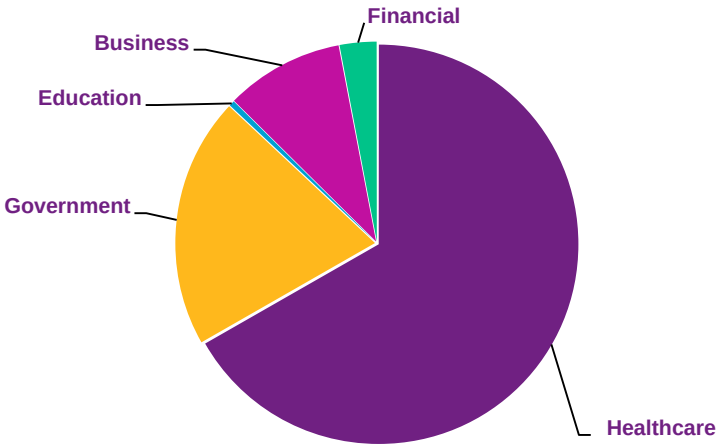
Source: Chubb/Ace Cyber Claims and Industry Trends, 3 Year Trends (October 2015)

Key Trends and Recent Developments

Who is Being Targeted?



Number of	Breaches
Healthcare	277
Government	63
Educational	58
Business	312
Financial	71



Number of	Records Exposed
Healthcare	112,832,082
Government	34,222,763
Educational	759,600
Business	16,191,017
Financial	5,063,044

The Identity Theft Resource Center has been tracking data breaches by sector since 2005. These graphs reflect their 2015 stats of reported data breaches as 1/4/2016.

In 2015, the Healthcare Sector had the highest severity with 12,832,082 records exposed resulting from 277 reported data breaches.

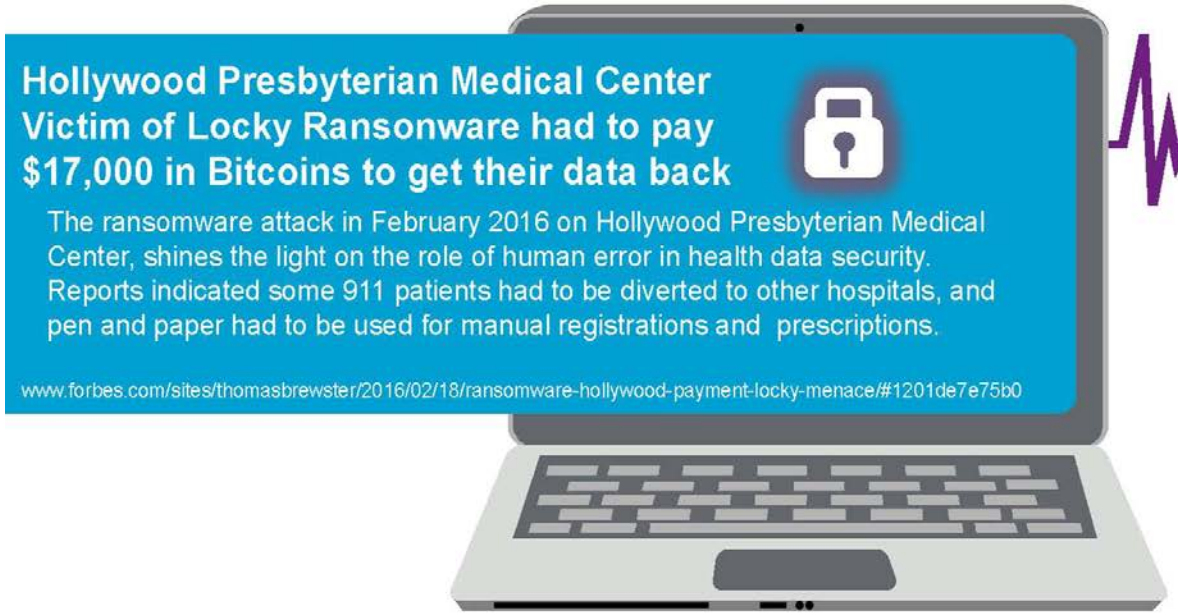
The Business Sector had the highest frequency with 312 reported data breaches exposing 16,191,017 records.

The Ransomware Crisis

Trending

Hackers Taking Hostage

In 2014, **68 percent** of healthcare data breaches were caused by lost or stolen devices containing health information. In 2015, **99 percent** of healthcare data breaches were caused by hacking events. Criminal hackers use social engineering techniques, such as phishing to target heir victims.



Ransomware Flatline

Ransomware is a virus that is typically delivered via phishiing email campaigns. All the target victim has to do is click on a link to immediately become infected. Once infected all their data is encrypted until a ransom is paid to the attacker, typically in Bitcoins, to get the encryption key to restore their data. Locky Ransomware is a fast moving virus, infecting as many as 90,000 victims per day.

https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise/ransomware-on-the-rise

Identifying Key Exposures

Build a Detailed Overview of the Enterprise's Risk

Quantify the particular enterprise risk to the organization, <u>viewed as a financial and operational risk:</u>

- How many records are held/collected by the organization and where are they held - what are the reporting requirements in the event of these records being disclosed?

- How reliant is the organization on 3rd party service providers? What contractual obligations/indemnifications are in place to protect the organization as comprehensively as possible?

- What, and how much of the company operations are reliant on a functioning network?
  - What is the financial loss from a network event?
  - Based on a 50% outage, what is the effect? 100%?
  - How long is the network outage likely to occur?
  - How are backups stored and activated?

Key Benefits of Cyber Risk Insurance

Mitigates Exposure to:

- Third Party claims, e.g., multi-million dollar class action loss due to a data breach, thereby reducing shareholder exposure.
- Breach response costs (Forensics, Legal Compliance, Notification, and Credit Monitoring).
- The increased outsourcing of IT applications (network disruption) and customer information (data breach) to service providers/business associates.
- Increased regulatory scrutiny.
- Meets contractual requirements demanded by many clients and business partners.
- Covers extortion, business interruption loss of income and remediation expense all arising out of ransomware attacks

Cyber Insurance - Core Coverage

Liability Coverage

Privacy Liability	Liability associated with your inability to protect personally identifiable information or corporate confidential information of third parties. The information can be in any format and breached intentionally or negligently by any person, including third party service providers to which you have outsourced information. Third party service providers include, but are not limited to, information holders.
Network Security Liability	Liability costs associated with your inability to prevent a computer attack against your computer network.
Media Liability	Tort liability associated with content you create, distribute or is created and distributed on your behalf , including social media content.

Direct (Loss Mitigation Coverage)

Breach Response Costs	Direct costs expended to mitigate a privacy breach. Costs typically include public relations expenses, notification, identity theft restoration, credit monitoring services and forensic/remediation expenses.

Cyber Insurance - Core Coverage

Direct (First Party) Coverage

Income Loss/Extra Expense	Income Loss/Extra Expense associated with your inability to prevent a disruption to your computer network caused by a computer attack or programming or software failure either: 1. on your network, or 2. at your IT Service Provider hosting your application.
Data Reconstruction	Your costs to recreate, recollect data lost, stolen or corrupted due to your inability to prevent a computer attack against your computer network.
Extortion Costs	Your costs expended to comply with a cyber extortion demand.
Regulatory Fines	Fines assessed by a regulatory body due to your data breach.

Cyber Claims Successes

A client's employee sent wealth management client information to his personal computer. The issue was identified, but not before the PC had the transmission. Our client notified all affected clients and regulatory agencies. Several regulatory bodies investigated the matter. No fraud was ever committed with the compromised data and no actions were brought against our client. Our claims legal group pursued reimbursement of the expense incurred excess of a significant retention prior to the renewal of the Cyber program. The expense to be reimbursed was agreed to before renewal, allowing us to negotiate a renewal for a $300M placement at $20K below the expiring premium. The reimbursed expense exceeded the total premium paid over the five years of the Cyber coverage.

A client's security was breached and 80 million records were accessed just prior to the cyber insurance renewal date. Our claims and broking staff coordinated an effort to review with the client's legal team and Information Security and provide enough information on the incident and the remediation to underwriters in order to renew the Cyber program without compromising the defense of the matter (several class action suits).

The policy limit of $100M was paid five weeks after we provided documented proof of loss.

Underwriting Process

Underwriting Process could include:

- Conference call with InfoSec and insurers.
- Completed, signed, and dated cyber application
- Details on prior losses over the past three years.
- Number of records that could be accessed in one occurrence

Key Primary Markets for Financial Institutions and Healthcare:

- AIG
- Chubb
- Liberty
- Kiln
- Beazley