PLUS

PROFESSIONAL LIABILITY UNDERWRITING SOCIETY

Preventing and Insuring Cyber Risk and Claims Management

Thursday, November 20, 2014

PLUS

PROFESSIONAL LIABILITY UNDERWRITING SOCIETY

Presenters:

Randy Krause, e-Place Solutions

Winston Krone, Kivu Consulting

Mark Mao, Kaufman Dolowich Voluck

Jenny Soubra, ACE

Susan Young, Marsh

Moderator:

Geoffrey Anello, AXIS Pro

PLUS

PROFESSIONAL LIABILITY UNDERWRITING SOCIETY

Current Significant Cyber Security Risks

Current Significant Cyber Risks

Targeted Damage

- **Malware (Retail)** **PCI**
- **Spear Phishing** **PCI, PII, PHI, $**
- **Trade Secrets** **???**
- **Network Damage** **???**

Collateral Damage

- **Healthcare Data** **PHI, PII, $**
- **Public Servers** **PCI, PII, PHI**
- **Web Applications** **PCI, PII, $**
- **Cloud Accounts** **???**

Targeted Damage #1 - Retail/ PoS

BACKOFF MALWARE

Retail/ PoS – 2014 Q3

BACKOFF MALWARE

Targeted Damage #2 - Spear Phishing

UNSTRUCTURED & CLOUD DATA

Stolen email and network passwords provide access to unlimited data

Data incredibly difficult (and costly) to quantify

Full of surprises (e.g. healthcare and credit card information buried in HR files)

Collateral Damage

Healthcare Data

- Usually NOT target of attack
- PHI enumeration (50% of forensic costs)
- CEs cracking whips on BAs

Public Facing Servers

- Automated attacks

Web Applications

- Errors by third party?

Cloud Accounts

- Don’t know breach occurred?

The Cyber-World

- Cyber Liability and related risks
  - Any liability arising predominantly from computerized operations or communications
  - Third party liability
  - First party exposures

Data Privacy and Network Security: A Multi-Threat Environment

Technology

- **Viruses, SQL Injections, DDoS attacks, etc.**
- **Structural vulnerability**
- **Social Media/Networking**
- **Phishing**

External

- Business Associates
- Vendors/Suppliers (contractors, outside counsel, cloud providers)
- Foreign and domestic organized crime
- Hackers/Hacktivists

Internal

- Rogue employees
- Careless staff
- BYOD

Regulatory

- HHS, HIPAA & HIPAA HITECH
- Identify Red Flags
- SEC, FTC, state attorney generals
- 47 State breach notification laws (Except AL, SD, and NM (proposed))
- PCI Compliance

Old School

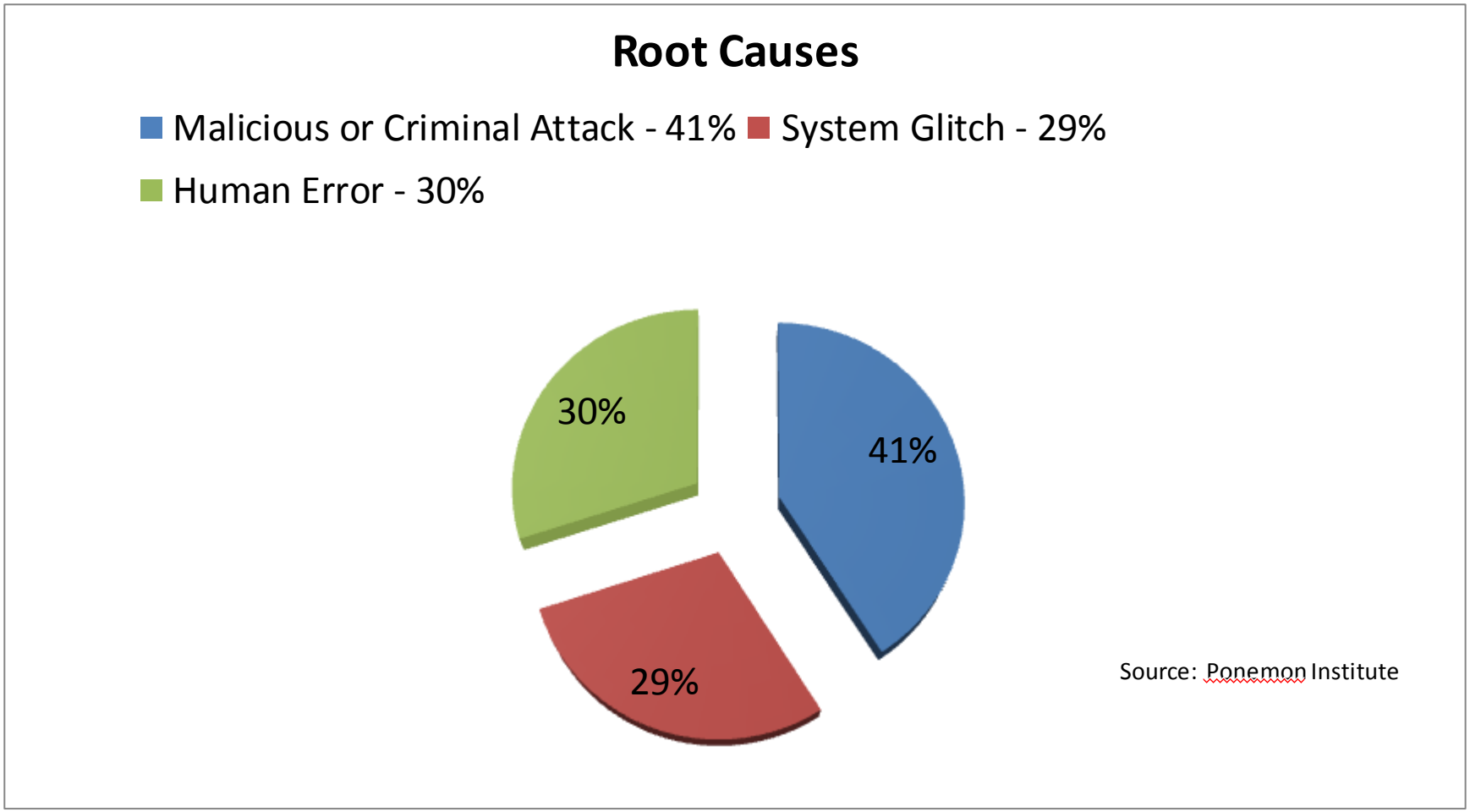
- Laptop theft
- Dumpster diving
- Photocopier

Data Breaches by the Numbers

- Average number of records involved– 29,087
- Average organizational cost - $5.85 Million
- Average detection and escalation costs - $417,700
- Average notification costs - $509,237
- Average post breach costs - $1,599,996
- Average lost business costs - $3,324,959

Source: Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis

Data Breach Causes



Sources of Liability

- Tort theories
  - Invasion of Privacy
  - Expectations
  - Cognizable damages
- Contractual obligations
  - Website Privacy Statements
  - Company Privacy Policies
  - Services Contracts
  - PCI DSS
- Regulatory
  - Fair Credit Reporting Act/Red Flag Rules
  - Gramm Leach Bliley
  - Notification Legislation
  - HITECH/HIPAA
  - Consumer Protection Acts (various)
  - Federal Trade Commission Act

Derivative Actions

- Derivative actions may be brought by shareholders concerning the manner in which a business' officers and directors manage data security and breaches
  - In re Heartland Payment Systems, Inc. Securities Litigation, Civ No. 09-1043
    - United States District Court, District of New Jersey
    - Heartland acted as a processor for credit card and ATM transactions
    - In 2007, hackers breached the Heartland payroll manager application, which did not contain customer data, only information of Heartland's employees
    - The attack also installed malicious software on Heartland's computer network, which resulted in the theft of 130 million credit and debit card account numbers
    - Heartland soon became aware of the payroll manager application breach, but did not discover the account data compromise until January 2009
    - In 2008, Heartland did not reveal the payroll manager application breach to the shareholders when asked about network security incidents
    - In January 2009, Heartland discovered and disclosed the account data compromise, resulting in the stock price dropping from more than $15.00 to $5.34 per share
    - Shareholders brought suit against Heartland alleging that, in 2008, its officers and directors concealed the attack on the payroll application, and misrepresented the general state of its security despite knowledge of the attack
    - The Court found that the Heartland officers and directors did not need to reveal the payroll attack because it did not result in compromised customer data
    - This demonstrates, however, that derivative actions may be brought by shareholders concerning the manner in which a business' officers and directors manage data security and breaches.

Top 5 Risk Management Recommendations

In order of difficulty:

- Assign ultimate responsibility to one person
- Prepare and test an incident response plan
- Train your employees
- Manage your vendors
- Perform a risk assessment (and implement mitigation measures)

PLUS

PROFESSIONAL LIABILITY UNDERWRITING SOCIETY

Questions from the Audience

Thank You 2014 Annual Sponsors

Thank You 2014 Annual Sponsors

Gold

beazley

WS&Co
WOODRUFF SAWYER & COMPANY

Silver

Berkley Asset Protection

Burnham Brown

Cavalry Wholesale Insurance Services

Hays Companies

Hudson Insurance Group

Monitor Liability Managers

RIC Insurance General Agency, Inc.