The Future of Data Breach Risk Management

“Response and Recovery”

The Cybersecurity Forum | April 14, 2016

If you have integrity matters
nothing else matters

If you DON’T have integrity matters
nothing else matters

Harvey Mackay
Today’s Topics

- About Merchants Information Solutions, Inc.
- About Mark Pribish
- Data Breach Trends
- Identity Theft Trends
- The Threat Landscape
- The Future of Data Breach Risk Management
- Questions and Answers
Merchants Information Solutions

Since 1912
ID Theft Risk Management Solutions Pioneer
Over 10 Million Consumers Covered

Business | Consumer | Data Breach - Identity Theft Solutions
About Mark Pribish

Vice President & ID Theft Practice Leader

- **Gannett/ Arizona Republic guest columnist** for cybersecurity, data breach, identity theft, and personal privacy
- **Member of FBI Citizens Academy** Class of 2012, **FBI InfraGard Public Private Alliance**, Guidepoint Global Advisors, and **Risk Insurance Management Society**
- Certified Identity Theft Risk Management Specialist (CITRMS) and **Arizona P&C License**
- 25 years’ experience in helping consumers and enterprise organizations manage the risks associated with ID Theft and data breach events
- Served in senior sales positions for Aon and AIG
- Graduated from the University of Dayton in 1981
Data Breach Trends
Data Breach Trends

2015 Security and Data Breach Research Reports

- Gartner, Sep 2015 - the forecast for worldwide spending on information security will reach $76.9 billion annually

- Grant Thornton, Sep 2015 - estimates the total cost of cyber attacks to businesses worldwide has reached $315 billion annually

- Trend Micro’s Data Breach Report, Sep 2015 - titled “Follow the Data: Dissecting Data Breaches and Debunking Myths” found that 41 percent of data breaches since 2005 were related to lost devices
Data Breach Trends

Privacy Rights Clearinghouse Data Breach Timeline for 2005 - 2016
April 2016

- Since January 2005 there have been **4,815** data breaches affecting **nearly 1 billion records**

- **Only 25 percent** of these data breaches were impacted by hackers and IT related events

- **The Majority - 75 percent** of these data breaches were impacted by social engineering (the human element)
Data Breach Trends

Privacy Rights Clearinghouse

Types of Data Breaches

- **Hacking/Malware** - electronic entry via outside party, malware and spyware
- **Insider** - someone with legitimate access intentionally breaches information
- **Payment Card Fraud** - fraud with debit and credit cards such as skimming devices at point-of-service terminals
- **Physical Loss** - lost, discarded or stolen non-electronic records
- **Portable Device** - lost, discarded or stolen laptop, smartphone or flash drive
- **Stationary Device** - lost, discarded or stolen stationary electronic device or server not designed for mobility.
- **Unintended Disclosure** - sensitive information posted publicly
- **Unknown** or other
Data Breach Trends

Ponemon Institute Study: Cost of a Data Breach
March 2015

- **Total Costs** - averaged **$217 per lost or stolen record**

- **Direct Incremental Costs** - including free/discounted services, notification letters, legal/accounting fees, etc.

- **Lost Productivity Costs** - including lost time of employees and contractors diverted from other tasks

- **Customer Opportunity Costs** - including cost of lost customers and cost of acquiring new customers
Identity Theft Trends

2015 FTC Consumer Sentinel Network Report
Identity Theft Complaints by Victims’ Age
February 2016

- 19 and Under – 5%
- 20 – 29 years old – 14%
- 30 – 39 years old – 16%
- 40 – 49 years old – 20%
- 50 – 59 years old – 24%
- 60 – 69 years old – 15%
- 70 and Over – 6%
Identity Theft Trends

2015 FTC Consumer Sentinel Network Report
How Victims’ Information is Misused
February 2016

- Government Documents/Benefits Fraud – 45.3%
- Credit Card Fraud – 15.8%
- Phone or Utilities Fraud – 9.9%
- Bank Fraud – 5.9%
- Employment-Related Fraud – 3.3%
- Loan Fraud – 3.5%
- Other Identity Theft – 19.2%
Identity Theft Trends

GAO Tax and Identity Theft Report
January 2015

Taxpayer Identity Theft is on the increase

- 2008 - 51,702 identity theft incidents
- 2009 - 169,087 identity theft incidents
- 2010 - 245,000 identity theft incidents
- 2011 - 1.1 million identity theft incidents
- 2012 - 1.8 million identity theft incidents
- 2013 - 2.9 million identity theft incidents
According to the U.S. Government Accountability Office (GAO), the IRS estimated it prevented $24.2 billion in fraudulent identity theft refunds in 2013.

The IRS also paid $5.8 billion that year for refund requests later determined to be fraud.
Identity Theft Trends

Ponemon Institute 5th Annual Study
February 2015

- Medical ID theft soared 22 percent in 2014
- Ponemon estimates more than 2.3 million adult medical ID theft victims
- Average victim didn’t find out until three months after it happened
- 65 percent of the study’s respondents paid average cost of $13,453
The Threat Landscape

Ponemon Institute 2015 State of Endpoint Report: January 2015

- This annual study identifies trends and changes in endpoint risk in organizations

- An endpoint can include servers, desktops, laptops, smartphones, and even printers, ATMs and PoS devices

- The biggest problem is the negligent or careless employee with multiple mobile devices using commercial cloud apps and working outside the office
The Threat Landscape

SailPoint Study (Identity and Access Management)
April 2016

- 25% of employees will share sensitive info outside their company
- 85% of employees react negatively if personal information were breached
- Yet 1 in 5 employees would sell their passwords to an outsider
- And of those who would sell their passwords, 44% would do so for less than $1,000
- 65 percent of respondents admitted to using a single password among applications
- One-third share passwords with their co-workers
- 40 percent reported having access to a variety of corporate accounts after leaving their last job
The Threat Landscape

According to the FBI
April 8, 2016 - LA Times

- **Ransomware** - disables digital networks but usually don't steal data
- Hacking victims in the U.S. have paid more than $209 million in ransom payments in the first 3 months of this year
- Compared with $25 million in all of 2015
- Paying the ransom does not guarantee the encrypted files will be released
- Decrypting files does not mean the malware infection itself has been removed
- **Train employees** to not open digital attachments or click on unfamiliar weblinks
The Threat Landscape

75% of breaches are to businesses of 100 employees or fewer

83% of SMBs have no formal cybersecurity plan

92% of companies who experienced a data breach didn’t know it…Notified by 3rd party
The Threat Landscape

**Data breach risk factors** include **people**, **processes** and **technologies**:

**People** – the insider threat, whether accidental or malicious, can include current and former employees, customers, associates, vendors, and independent contractors.

**Processes** – including information technology, enterprise risk management, marketing/sales and human resources need to be aligned, defined, and documented.

**Technologies** – that are relied on to conduct and grow your business are also being used to identify vulnerabilities and cyber threats on your business.
The Future of Data Breach Risk Management

Confronting the Widening Infosec Skills Gap - www.csoonline.com
May 15, 2015

- CSO provides news, analysis and research on a broad range of security and risk management topics

- The demand for cybersecurity pros has grown more than 3.5 times faster than the demand for other IT jobs over the past five years

- Cybersecurity jobs have increased more than 12 times faster than the demand for all other non-IT jobs

- The gap between the demand for information security professionals and the supply to grow to **1.5 million by 2020.**
The Future of Data Breach Risk Management

The Emergence of Cybersecurity Law
Indiana University Mauer School of Law by Hanover Research
February 2015

- **Cybersecurity is a growing priority for legal practitioners** - numerous law firms have formed cybersecurity practice groups

- **Cybersecurity has become as much a legal issue** - lawyers must play a role in designing the procedures, training, and risk assessments required to implement managerial, operational, and technical controls needed to protect data.

- **Lawyers are becoming more proactive in addressing cybersecurity concerns** - until very recently, companies primarily involved lawyers in the response to cybersecurity incidents, rather than in the planning against such crises.
The Future of Data Breach Risk Management

The Emergence of Cyber Insurance

Sep 2015 – Insurance 2020 & beyond: Reaping the dividends of cyber resilience

71 percent of insurance CEOs, 79 percent of banking CEOs, and 61 percent of business leaders across all industries see cyber attacks as a threat to growth

- 2008 - $500 million
- 2012 - $805 million
- 2013 - $1 billion
- 2014 - $2 billion
- 2015 - $2.5 billion
- 2020 - $7.5 billion estimate
- 2025 - $25 billion estimate

Cyber insurance is no replacement for robust IT security, but rather creates a second line of defense to mitigate cyber incidents.
The Future of Data Breach Risk Management

International Association of Privacy Professionals
https://iapp.org/certify/programs

CIPP - Certified Information Privacy Professional - The CIPP shows that you understand the laws, regulations and standards of privacy in your jurisdiction or discipline.

CIPM - Certified Information Privacy Manager - The CIPM says that you understand how to use process and technology to manage privacy in an organization—regardless of the industry or jurisdiction.

CIPT- Certified Information Privacy Technologist - The CIPT shows that you know how to manage and build privacy requirements and controls into technology.
The Future of Data Breach Risk Management

InfraGard is a non-profit organization serving as a public-private partnership between U.S. businesses and the Federal Bureau of Investigation.

InfraGard Chapters
https://www.infragard.org/FbTty4cyYBFFAj3Spx5ms%2525252BxhvOgLbrLQDorlo3ju04Y%25252525253D!
The Future of Data Breach Risk Management

Response and Recovery

- Make an initial assessment of cyber/data breach event - including nature and scope; accidental or malicious; type of information and type of damage

- Implement measures to minimize continuing damage - whether cyber intrusion or an accidental release, determine next steps to stop ongoing damage and take steps to prevent it from happening again

- Record and collect information - make a “forensic image” of the affected computers and/or a record of the data-breach event to preserve a record of the incident for later analysis and potentially for use as evidence at trial

- Public relations and communications - create a positive and consistent message for internal and external use
The Future of Data Breach Risk Management

Response and Recovery

- Notify - contact employees within the organization and affected individuals outside the organization
- Notify - law enforcement if criminal activity is suspected
- Notify - know that 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have notification laws in place to notify any individual whose personally identifiable information has been breached
- Notify - know the two Federal laws including the FTC Red Flag Rule and HIPAA HITECH Data Breach Notification Rule
Contact Information

Mark Pribish
VP & ID Theft Practice Leader
602-744-3736
mpribish@merchantsinfo.com

Integrity Matters – since 1912