

Introduction to Compliance: Protecting Customer Information

Presented by
Joshua Schafer & Rachel Fisher

Introductions

- **Joshua Schafer** has over 10 years experience in information technology and is currently Director of Security Services at Langan Enterprises, Inc. During his 5+ years at LEI he has specialized in network and security consulting, vulnerability assessments, penetration testing and information technology audits. His certifications include: A+ Core Hardware, A+ OS Technologies, Microsoft Certified Professional, Microsoft Certified Systems Administrator, and Microsoft Certified Systems Engineer.
- **Rachel Fisher** is currently a partner at Nearman, Maynard, Vallez, CPAs & Consultants, P.A. Rachel received her Bachelor of Business Administration degree, magna cum laude, from Clayton College and State University in Morrow, Georgia. Rachel has earned the Certified Information Systems Auditor (CISA) designation issued by the Information Systems Audit and Control Association (ISACA) and the Certified Compliance Officer (NCCO) designation issued by the National Association of Federal Credit Unions. She assists clients with information technology audits as well as compliance and internal audit services. In addition to ISACA, Rachel is a member of the Institute of Internal Auditors (IIA) and the American Institute of Certified Public Accountants (AICPA).

How We Got Here

TJMaxx – Wireless Network Hacked

- Lost 45.7 million consumer credit and debit card numbers due to an intrusion is believed to be linked to weaknesses in its wireless network.
- Expenses estimated at \$500 million to \$1 billion – Settlement with VISA USA- \$40.9 million to fund an alternative recovery payments program
- At least 19 lawsuits have been filed, investigations underway by the FTC and 37 state Attorneys General.

**Important because this began the pushback of costs to the organization that caused the breach

Bank of America – Backup Tape Lost

- Shipping vendor lost computer data tapes containing personal information on up to 1.2 million federal employees, including some members of the U.S. Senate.

**Important because we began to think of where we have the data, not just internally but externally as well.

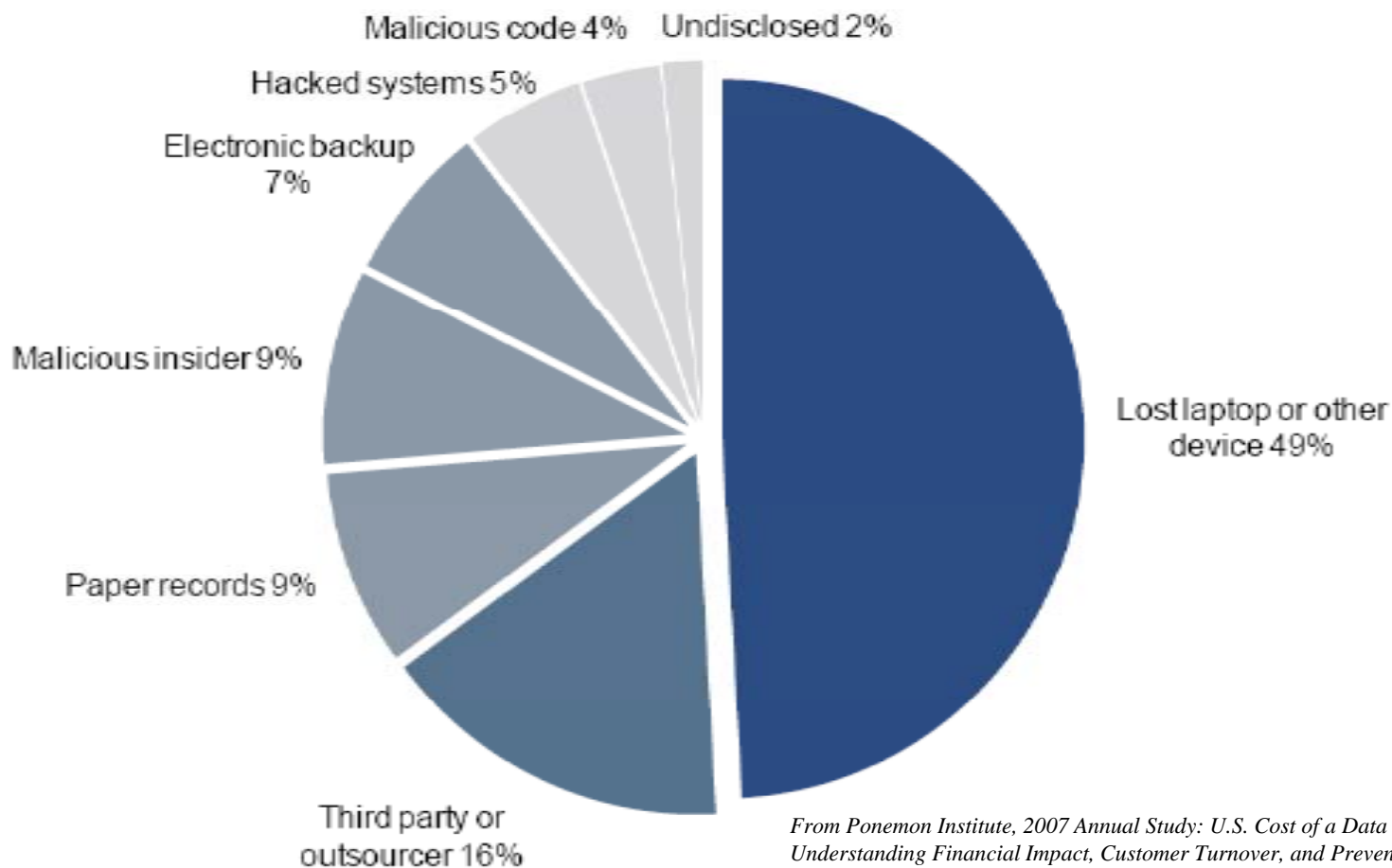
Veterans Administration – Laptop Stolen

- A laptop containing sensitive data was stolen from a VA employee's home.

**Important as mobile devices are increasingly the target of data compromises.

Full Chronology of Data Breaches
<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Causes of a Breach



*From Ponemon Institute, 2007 Annual Study: U.S. Cost of a Data Breach
Understanding Financial Impact, Customer Turnover, and Preventative Solutions*

Laws for Customer Notification

- Highest profile regulations/laws in privacy environment. Ex. Gramm-Leach Bliley Act (GLB) and Health Insurance Portability and Accountability Act (HIPAA).
- Significant reputational risk impact, potential financial and legal implications
- Over 40 State Laws – all differ as to the liability, the instances in which notification is required, and the types of data considered nonpublic.
- Federal regulations/laws only setting minimum standards, if state laws are more stringent then they take precedence.
- FACT Act – requires notification in the event of breach for regulated Financial Institutions, FTC regulated companies and SEC regulated companies
- Four pending Federal Bills
- ID Theft Red Flags are a FACT Act requirement to monitor customers behaviors to assist in quickly identifying future breaches.

Federal Trade Commission

- 2 Main Driving Forces:
 - Privacy of Consumer Information
 - Prevention of Identity Theft

Federal Trade Commission

- Federal Trade Commission (FTC) Act
- Gramm Leach Bliley (GLB) Act
- Fair Credit Reporting Act (FCRA)

FTC Act

- Prevents unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce
- Guards against unfairness and deception by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information

FTC Act (cont.)

- Applies to persons, partnerships, or corporations except banks, savings and loans associations, federal credit unions, and common carriers (exceptions who are subject to other regulations)

Section 5 Cases

- March 2008 – TJX – discount retailer
- March 2008 – Reed Elsevier and Seisint – data broker
- March 2008 – ValueClick – online advertiser
- January 2008 – Life is Good Retail, Inc. – online apparel retailer

Federal Trade Commission

- Under the Gramm-Leach-Bliley Act, the Commission has implemented rules concerning financial privacy notices and the administrative, technical and physical safeguarding of personal information.

Gramm-Leach-Bliley

- The GLBA Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information.

Gramm-Leach-Bliley Act (cont).

- The GLBA Data Protection and Safeguards Rule are mandated to:
 - Insure the security and confidentiality of customer data.
 - Protect against any reasonably anticipated threats or hazards to the security or integrity of such data.
 - Protect against unauthorized access to or use of such data that would result in substantial harm or inconvenience to any customer.

Gramm-Leach Bliley Act (cont.)

- To comply with GLBA, all organizations within the financial services industry must implement a comprehensive written **information security program*** specifying how their customer information is protected. The following institutions fall within the scope of the act:

Banks

Credit Unions

Mortgage Brokers

Insurance Companies

Mortgage Lenders

Credit Card Companies

Real Estate Agents

Financial Planners

Appraisers

Thrifts

Securities Firms

* Information Security Program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

The Road to GLB Compliance

- No single total solution for comprehensive information security.
- Depends on complexity, sensitivity, and risk profile of each organization.
- Layered approach that includes policies, procedures, practices, solutions and technologies.

The Road to GLB Compliance (Cont).

The regulation stipulates that you:

- **Involve the board of directors**
- **Assess risk that may threaten customer information**
- **Manage and control risk**

The Road to GLB Compliance (cont.)

- **Train employees**
- **Test your program**
- **Oversee service providers**
- **Adjust the program**
- **Report to the board**

Fair Credit Reporting Act

- The Fair Credit Reporting Act (FCRA), enforced by the Federal Trade Commission, promotes accuracy in consumer reports and is meant to ensure the privacy of the information in them. The FCRA was recently amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA).

FCRA (cont.)

- Purpose of the FACTA is to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes.

FCRA (cont.)

- FCRA and FACTA apply to any organization who provides consumer reports, who furnishes information to consumer reports, or who uses consumer reports

FCRA (cont.)

- FCRA defines the term consumer report to include information obtained from a consumer reporting company that is used – or expected to be used – in establishing a consumer’s eligibility for credit, employment, or insurance, among other purposes.

FCRA Highlights

- Disposal of consumer information
- Identity theft prevention program
- Sharing of information

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996.

- Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.
- Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.
 - The Administrative Simplification provisions also address the security and privacy of health data.

HIPAA

- HIPAA regulates the use and disclosure of "protected health information" ("PHI"). For purposes of HIPAA, PHI includes information relating to an individual's physical or mental health and the provision of, or payment for, an individual's health care, if the information is individually identifiable – meaning it contains information such as the person's name, address, date of birth, social security number, or other information that could be used to identify a specific person.

Who Must Comply With HIPAA?

- HIPAA applies to "covered entities" and "business associates" of covered entities. Covered entities generally include health-care providers, health plans, and health-care clearinghouses.
- Business associates of covered entities are those persons or entities that have access to PHI as a result of a contractual relationship with a covered entity to perform services that involve the use or disclosure of PHI.

HIPAA - The Security Rule

- The Final Rule on Security Standards was issued on February 20, 2003. It took effect on April 21, 2003 with a compliance date of April 21, 2005 for most covered entities. The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance:
 - ***Administrative Safeguards*** - policies and procedures designed to clearly show how the entity will comply with the act
 - ***Physical Safeguards*** - controlling physical access to protect against inappropriate access to protected data
 - ***Technical Safeguards*** - controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.

PCI Compliance

Payment Card Industry (PCI) compliance
(a.k.a. the PCI Data Security Standard)

- The PCI Security Standards Council was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.
- PCI DSS is all about preventing the electronic and paper theft of cardholder data.
- The heart of the PCI DSS is about mitigating the risk of a direct attack on the cardholder data.

PCI Compliance (cont.)

- The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
- The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data.
- Payment channels include retail (brick and mortar), mail/telephone order, and e-commerce organizations.

PCI Compliance (cont.)

- Each payment brand develops and maintains its own PCI DSS compliance programs in accordance with its own security risk management policies
 - AMEX – Data Security Operating Policies (DSOP)
 - Discover – Discover Information Security and Compliance (DISC)
 - JCB – Data Security Program
 - MasterCard – Site Data Protection (SDP)
 - Visa USA – Cardholder Information Security Program (CISP)
 - Other Visa Regions Account Information Security (AIS) Program



Teaching Individuals to Achieve...
Helping Companies Succeed

Why do we need PCI DSS?

	Small (< 50 Staff)	Large (> 250 Staff)	Very Large (> 500 Staff)
Organizations that had a security incident in the last year	45%	72%	96%
Average Number of Incidents	6	15	> 400
Average Cost of worst incident in year	\$20k to \$40k	\$180k to \$340k	\$2m to \$4m

Source: Information Security Breaches Survey 2008, conducted by Price Waterhouse Coopers

Why bother with PCI DSS?

- Principally because you have to if your organization:
 - Processes Primary Account Number (or Credit Card Numbers)
 - Stores PAN
 - Transmits PAN
- Not law (Contract) – although some US states are legislating. Ex. Minnesota
- The law does not mention PCI, but is strongly based on it. You will note that this law now enables the cardholder to seek direct damages against a company that improperly discloses their credit card data.
- Enforceable through financial penalties or sanctions (revocation of credit card facilities)

When is PCI applicable to my organization?

- PCI is applicable and therefore a contractual requirement (mandated) to any organization processing, storing, transmitting cardholder data, this applies to:

“Any network component, server, or application that is connected to the cardholder data environment”

- Dependent upon whether your organization credit card transactions are outsourced
- Dependent upon if you are a Service Provider or Merchant (see next slide)



Teaching Individuals to Achieve...
Helping Companies Succeed

PCI – Merchant Levels

Merchant Level	Selection Criteria	Validation Actions	Validated By
1	Any merchant - regardless of acceptance channel - processing more than 6,000,000 transactions per year Any merchant that has suffered a hack or an attack that resulted in an account data compromise	Annual On-Site Security Audit and Quarterly Network Scan	Independent Security Assessor or Internal Audit if signed by an Officer of the company Qualified Independent Scan Vendor <i>Level 1 Merchants should have validated compliance by September 30, 2004</i>
2	Any merchant processing between 150,000 to 6 million transactions per year	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	Merchant Qualified Independent Scan Vendor <i>Validation is required no later than June 30, 2005</i>
3	Any merchant processing between 20,000 to 150,000 transactions per year	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	Merchant Qualified Independent Scan Vendor <i>Validation is required no later than June 30, 2005</i>
4	Less than 20,000 transactions per year	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan	Merchant Qualified Independent Scan Vendor <i>Note: While compliance is mandatory for Level 4 Merchants, validation is optional but strongly recommended</i>

Validation Requirements for Merchants

- All merchants must comply with PCI DSS (all brands)
- Validation of merchant compliance varies by payment brand
- AMEX, MasterCard & Visa have defined merchant levels based on transaction volume
- Discover and JCB do not have defined merchant levels
 - Discover - compliance validation requirements are outlined in the Discover Network Merchant Operating Regulations
 - JCB - compliance validation requirements will be addressed in forthcoming JCB rules and regulations

PCI-DSS requirements

Build and maintain a secure network

Requirement 1 Install and maintain a firewall configuration to protect cardholder data

Requirement 2 Do not use vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data

Requirement 3 Protect stored data and do not store card and transaction data unnecessarily

Requirement 4 Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a vulnerability management program

Requirement 5 Use and regularly update antivirus software

Requirement 6 Develop and maintain secure systems and applications

Implement strong access control measures

Requirement 7 Restrict access to data by business need-to-know

Requirement 8 Assign a unique ID to each person with computer access

Requirement 9 Restrict physical access to cardholder data

Regularly monitor and test networks

Requirement 10 Track and monitor all access to network resources and cardholder data

Requirement 11 Regularly test security systems and processes

Maintain and information security policy

Requirement 12 Establish and maintain high level security principles and procedures (documented policies and procedures)

Resources

- PCI Security Standards Council
(<https://www.pcisecuritystandards.org/>)
- PCI Compliance Guide
(<http://www.pcicomplianceguide.org/>)
- Federal Trade Commission
(<http://www.ftc.gov/privacy>)

Contact Information



Joshua Schafer, MCSE, MCPS, MCNPS
<http://langanenterprises.com/>

Nearman ♦ Maynard ♦ Vallez
CPAs & Consultants, P.A.

Rachel Fisher, CISA, NCCO, CTGA
<http://nearman.com/>

Summary

Remember that compliance is a ‘bare minimum’ while security is however much at or above that line you define it to be.