2009 HOSPITALITY LAW CONFERENCE

Information and Technology Risk

Challenges for a Connected World!

Presenters

- **Joe DePaul – Senior Vice President – Arthur J. Gallagher Co. of New York, Inc.**
- **National Resource for Cyber and Professional Liability for the firm.**
- **Market management and technical support for technology sector clients and brick and mortar companies with technology, media and professional exposures.**
- **15 Years experience with Management and Professional Liability**

- **John Mullen – Partner at Nelson Levine deLuca & Horst "NLdH" and Chairman of the firm's Complex Liability Group.**
- **NLdH is an insurance services law firm with 50 attorneys practicing in 5 offices.**
- **He has practiced nationally for 17 years, and is a frequent speaker and writer in his areas of focus: data/cyber risk, ediscovery, mass/toxic tort and construction law.**
- **John represents companies that experience data theft/losses focused on immediate response to issues including forensics, public relations, litigation holds, notice, class action and other "triage" areas.**

Presenters

- Mark Greisiger leads NetDiligence, a Cybersecurity Risk Management company.
- For the past 8 years NetDiligence has been offering unique cybersecurity e-risk assessment services to businesses.
- Their due diligence services support the unique loss control and compliance needs for many businesses as well as their professional liability insurers in US and UK, which offer network liability coverage (aka “privacy insurance”).
- Mark is also a frequent published contributor for various insurance and risk management publications on similar topics.

- Kristi Janicek is a Vice President in ACE USA’s Professional Risk division in Dallas, Texas, where she is the Southwest Zonal Manager
- She is responsible for managing ACE’s Professional Liability division for the Dallas and Houston regions.
- Mrs. Janicek has more than 17 years’ experience in the insurance arena specializing in underwriting professional liability for Network, Privacy, Technology, Media, Miscellaneous, Public Entity, Architects & Engineers and Contractors product lines.

Cyber Landscape

Loss Data Types

- Account Information
- Personally Identifiable Information (PII)
- Medical
- Trade Secrets/Client Lists

What are the Risks

- That E&O, PL, CGL, D&O don’t apply

- Data

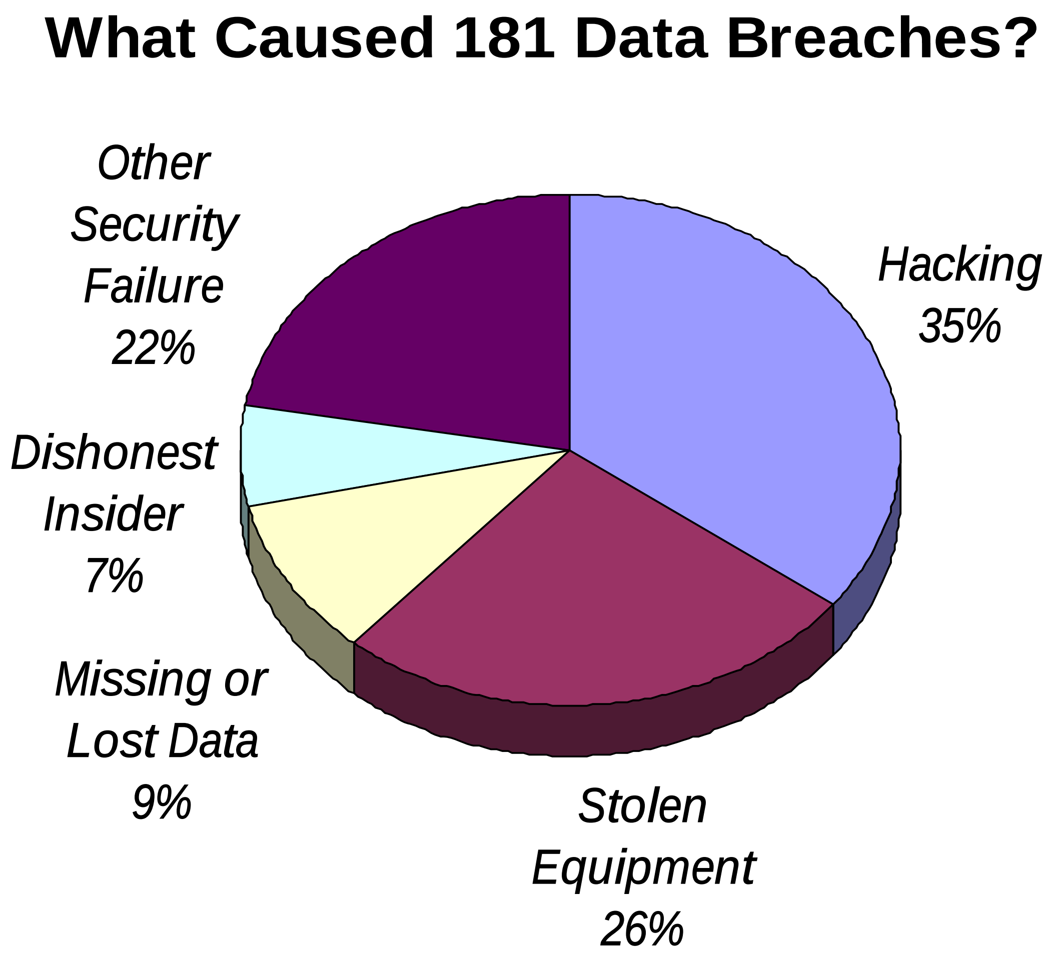
Stolen

Lost

Destroyed

- Account fraud/identity theft/nothing (yet)

PrivacyRights.org



HospitalityLawyer.com

Current Events…sample of incidents

March 2008 – Hannaford Supermarket: A major security breach reported by the supermarket may have compromised more than 4.2 million unique credit and debit card numbers. The company said it is currently aware of about 1,800 cases of reported fraud. A class action lawsuit has been filed in Maine.

March 2008 - Cascade Healthcare. Breach at the hospital may affect more than 11,500 people. The virus penetrated the computer system Dec. 11 07.

March 2008 – MTV: Network breach impacts 5,000 employees, successful social-engineering blamed. The network, owned by Viacom, issued a memo to employees, announcing that an employee's computer was compromised through an internet connection, published reports said. The data included names, Social Security numbers, birth dates and salaries.

Jan 2008 - OmniAmerican Bank: An international gang of cyber criminals hacked into OmniAmerican Bank's records, the bank's president disclosed…They stole scores of account numbers, created new PINs, fabricated debit cards, then withdrew cash from ATMs in Eastern Europe, including Russia and Ukraine, as well as in Britain, Canada and New York.

Jan 2008 - T. Rowe Price Retirement Plan Services alerted 35,000 current and former participants in "several hundred" plans that their names and Social Security numbers were contained in files on computers that were stolen.

Jan 2008 – EDS: About 260,000 participants in Medicaid programs were sent a recent mailing that included the recipients' Social Security numbers above their names on the address labels..

Jan 2008 – Sears: Class Action Suit Alleges Sears Privacy Failures: privacy activists revealed that the company's Web site exposed the details of customer purchases going back more than a decade..

Example Claim Costs

- **Costs to notify consumers:** $1 to $5 per individual (plus costs for a lawyer to help interpret/ comply with multiple state privacy/ notice laws)
- **Investigation:** Legal and technical costs to forensically investigate/stop an attack or confirm the breach and the extent of it.
  - **How far did the bad guy get? Was there a reasonable chance they illegally accessed customer data.**
  - **What type(s) of NPI was touched.**
  - **Who are the victims, what state do they reside?**
- **Credit Monitoring Services**: $10 to $60 per person per year [approx 20% of individuals accept]
- **Defense Costs:** class action defense costs : notification, forensic, litigation hold, P.R., $XXX,XXX+
- **Legal Liability?** Key consideration: Minor damages for large groups = significant potential loss

  $1,000 (damages) X 300,000 (claimants) = $300 million!!!
- **Other**: FTC & VISA Fines, Bank reimbursements

Array of Plaintiffs

- Individuals
- Government
- Effected businesses (banks)
- Class Actions
  - Currently – no “breakthrough” case yet
  - Trend – toward finding liability
  - Federal Courts are not yet agreeing that credit monitoring is enough damages to sustain a class action
  - Plaintiff’s bar – filing and probing

Impacts and Costs

Third party claims arising from a network event:

- Failure to protect customer information/privacy
- Failure to notify/timely notification
- Cost to cancel or reissue payment cards/open new accounts
- Costs of fraudulent purchases
- Consumer Redress – credit monitoring/identity theft insurance
- Regulatory Actions – fines and penalties

Regulations

- **State level ‘breach notice’:** 43 states require notice to customers after unauth access to NPI
  - Calif SB 1386: Requires firms that conduct business in California to notify California-consumers of security breaches of unencrypted computerized personal information. Customers have private right of action for violations
  - Data-at-rest (disc level) encryption often a safe harbor

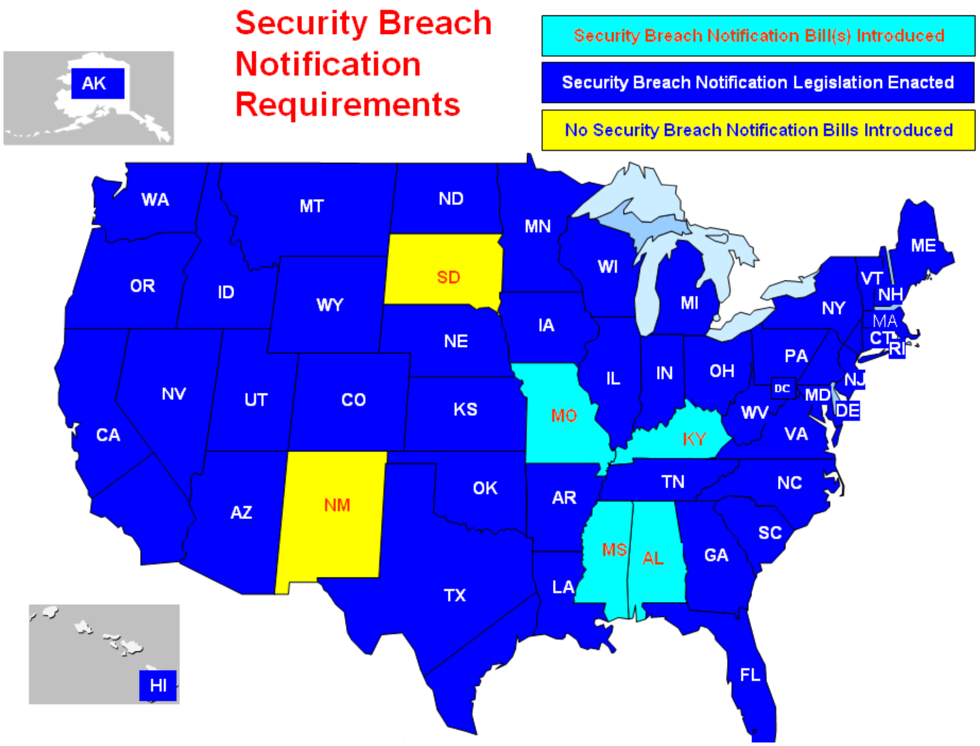
- **Plastic Card Act (Mn):** Issuing banks seeking reimbursement from merchants for costs to reissue credit cards (and other “reasonable costs”) after a security breach.
  - “The 48-hour Rule” – do not retain sensitive authentication data
  - Trigger: “security breach” (acquisition of personal information by an unauthorized person)
  - No encryption safe harbor
  - Other states considering similar law

- **Fair And Accurate Transaction Act of 2003 (FACTA)**
  - **Truncation**
    - Section 15 U.S.C. § 1681c(g) of FACTA limits the information that can be printed on an electronically printed credit card receipt to the last five digits of the credit card number, and specifically prohibits printing a credit card’s expiration date on the receipt.
    - A single violation of FACTA could result in damages ranging from $100 to $1,000
    - Over 100 class actions
  - **Disposal**: proper disposal of consumer report information required. “Consumer information” under FACTA includes
    - records that are consumer reports
    - records that are derived from consumer reports

Costs

- Attorney fees, including:
  - Investigation
  - Notification
  - Guidance
  - Defense/e-discovery
- Indemnity payments
- Notification costs
- Card re-issuance
- Credit monitoring
- Call centers
- I.D. theft insurance

Compliance Trends – Breach Notice



Security Breach Notification Requirements

Security Breach Notification Bill(s) Introduced

Security Breach Notification Legislation Enacted

No Security Breach Notification Bills Introduced

State level 'breach notice'

45 states require notice to customers after unauthorized access to personal data

(NEW) Identity Theft Enforcement and Restitution Act

New law allows identity theft victims to seek restitution in federal court for the loss of time and money spent in restoring their credit.

A Note on ‘Privacy’

You can NOT have privacy without solid info-security!

Privacy Practices are often based on Fair Information Principles

The Fair Information Principles, the basic components of a privacy program, are:

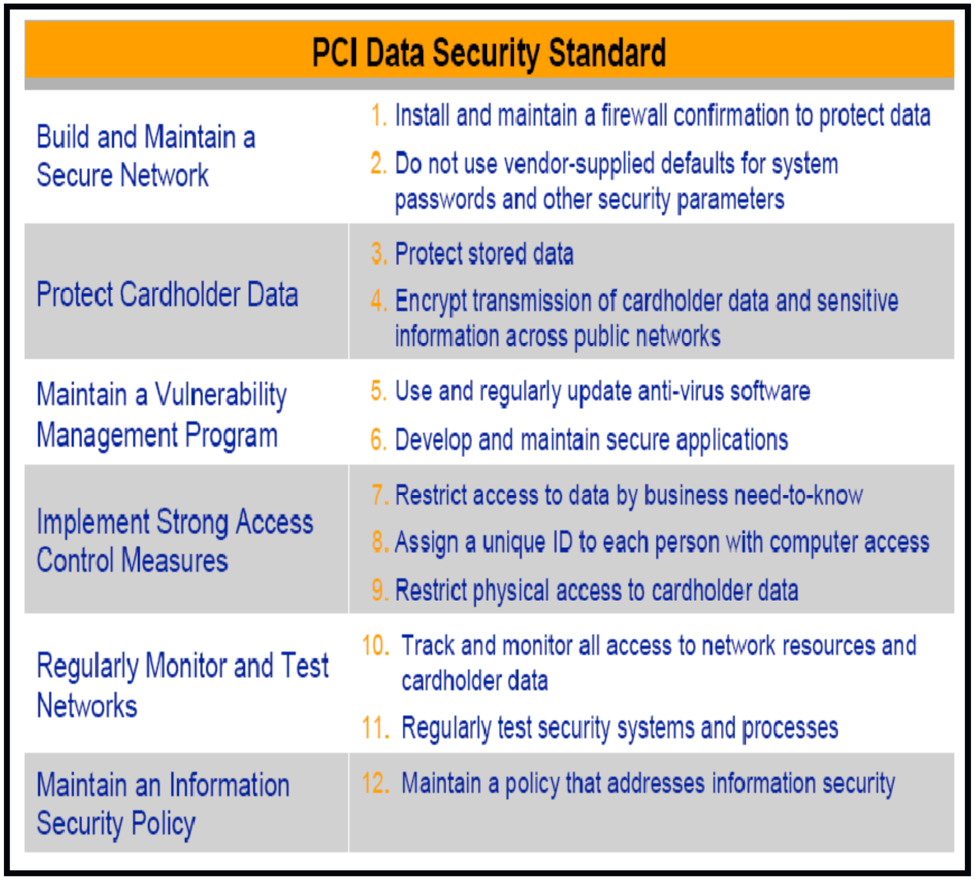
- Provide consumers with ***notice*** regarding data collection
- Give consumers ***choice*** regarding use of their data
- Provide consumer ***access*** to review/comment on ***quality***
- Ensure data accurate/ up-to-date; review and ***correct*** all data
- Set ***collection*** and ***use limits*** (purpose)
- Provide adequate ***security*** against improper use
- Be ***accountable*** for legal conformance

Compliance Trends – PCI DSS

- PCI DSS (“Payment Card Industry Data Security Standard”) includes requirements for critical protective measures:
  - security management
  - policies and procedures
  - network architecture
  - software design

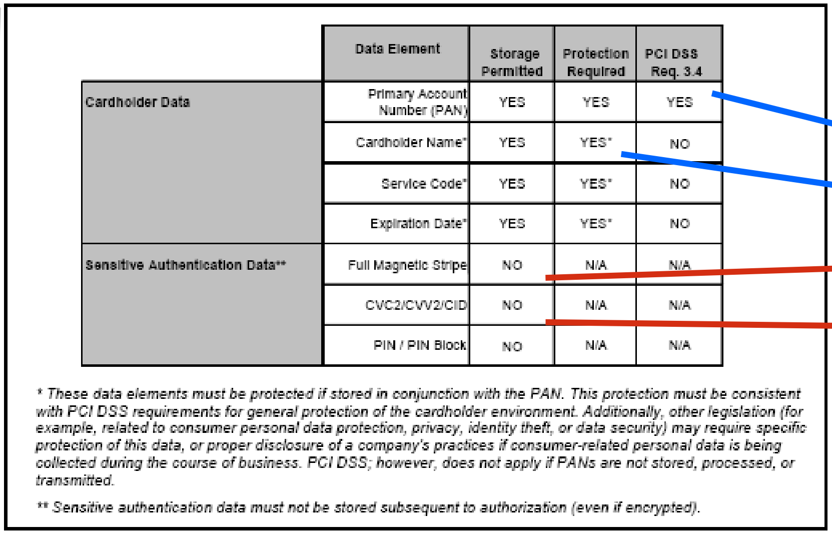
- Goal: to helps organizations proactively <u>protect customer account data</u>

- Developed by - American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International



PCI Data Security Standard	
Build and Maintain a Secure Network	1. Install and maintain a firewall confirmation to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure applications
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

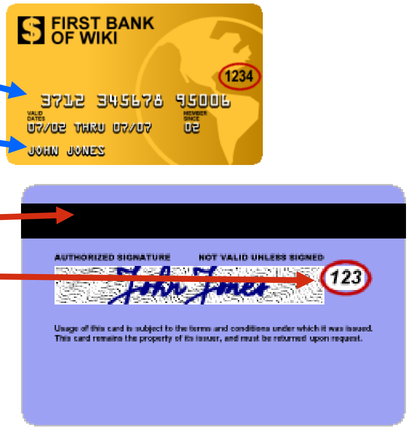
Key to PCI: Watch How & What You Store



	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.

*** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).*


FIRST BANK OF WIKI
1234
3712 345678 95006
VALID DATES
07/02 THRU 07/07
MEMBER SINCE
02
JOHN JONES
AUTHORIZED SIGNATURE
NOT VALID UNLESS SIGNED
John Jones
123
Usage of this card is subject to the terms and conditions under which it was issued.
This card remains the property of its issuer, and must be returned upon request.

- **Customer NPI data should be encrypted in a database**
- **Do not store sensitive authentication data subsequent to authorization (not even if it’s encrypted)**
  - **Do not store the full contents of any track from the magnetic stripe (on the back of the card)**
  - **Do not store the card validation code (3- or 4- digit value printed on the front or back of a payment card)**
  - **Do not store the PIN verification value (PVV)**

- **Acquirers can be fined between $5,000 and $25,000 a month for each their merchants that have not <u>validated</u> PCI compliance**

Why the Problem?

The Internet's open network

- Many companies have a transactional website

- Businesses collect and store customer *private data*
  - More data often collected than needed
  - Data often Stored for too long

- Business servers (websites) are very porous and need constant care (hardening & patching). *4 out of 5 fail scan test*

- IRP is suspect (often find out about an incident after a long period of time)

- Bad buys rely on the prevalence of *human error*
  - Unchanged default settings
  - No applied patches
  - Customer private records (paper) improperly disposed (dumpster)
  - Poor Passwords

What can be done?

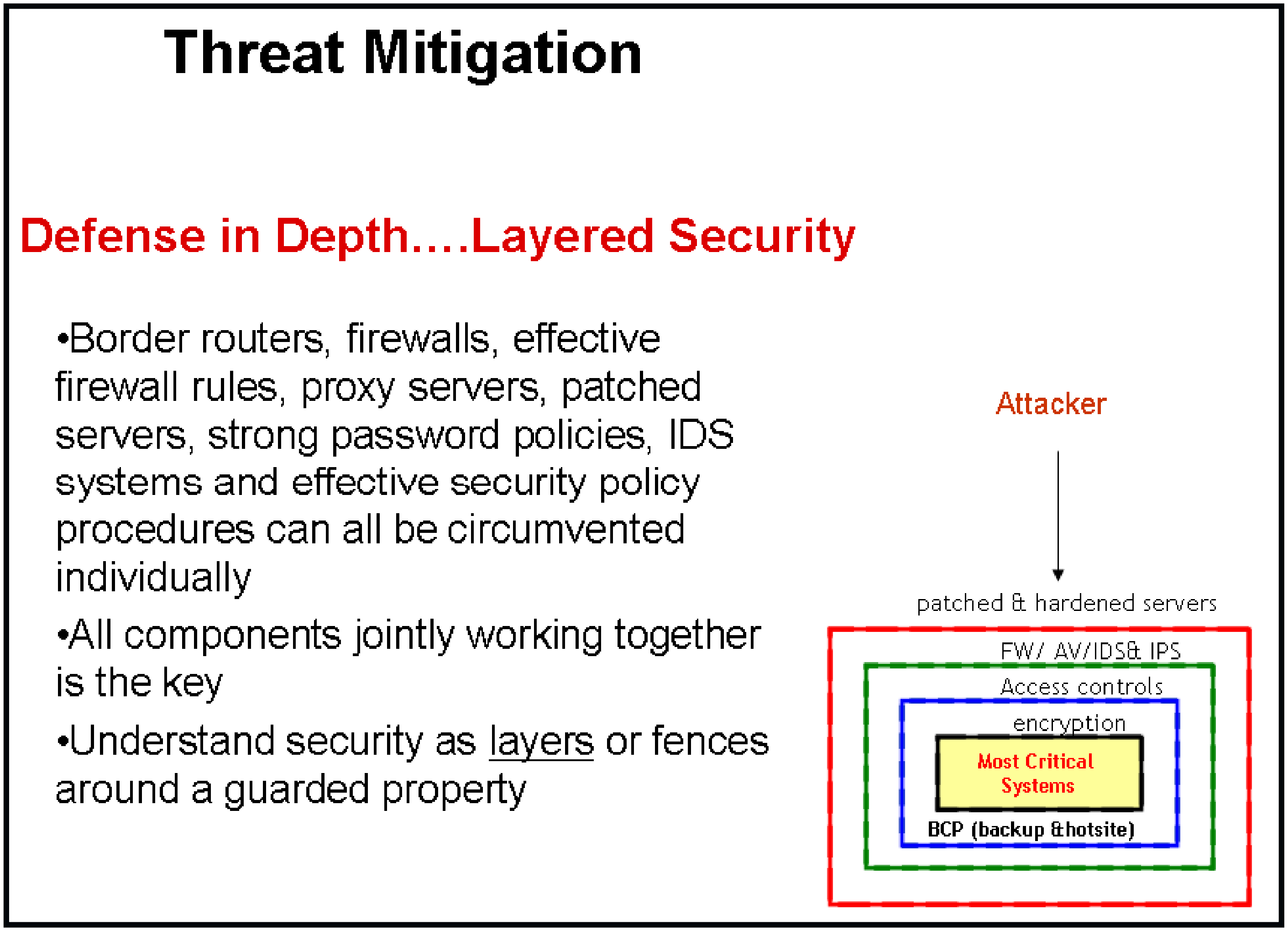
- Increase awareness of risk. Talk to your IT Sec folks, let them know about your insurance and claim notice conditions
- Gain an appreciation of the many challenges they face to manage the risks. ex. what type(s) of customer data is being collected, stored, protected…and where does all this data reside?
- Assess & Test your own staff and operations…. try to understand your orgs strengths & weaknesses. Document due care
- Back to basics: Implement at least ‘baseline’ safeguard controls
- Vigilance: Update & monitor your measures

Loss Prevention Approach

Proactively Assess Controls Surrounding:

- **People:** dedicated info sec personnel; Background checked; Proper security budget and vigilant about their job!
- **Processes:** enterprise ISO17799, GLBA/ FFIEC ready; policies enforced daily; employee education/ training; change management processes, etc.
- **Technology:** managed firewall with IDS/IPS, hardened & patched servers, strong passwords, event logging, anti-virus software, data is encrypted in transmission & storage, port scanning, daily backup, redundancy/ hot-site..

Key Concept – Layered Safeguards



Threat Mitigation

Defense in Depth….Layered Security

- Border routers, firewalls, effective firewall rules, proxy servers, patched servers, strong password policies, IDS systems and effective security policy procedures can all be circumvented individually
- All components jointly working together is the key
- Understand security as layers or fences around a guarded property

Assessment Scope

Example Physical controls

- Prohibit external portable storage devices
- Lock down USG Keys
- Configure PCs and Laptops so they only accept encrypted external hard drives
- Eliminate file sharing programs
- All discarded hard drives must be degaussed and destroyed in chipper
- Color code and label waste bins, office paper must be placed in locked bins
- Shredding must be done on site and supervised including shredding vendors
- Clean desk policy

Example Electronic Controls

- All PCs, laptops, mainframes must be encrypted
- Robust passwords that have 30 day expiration
- Password protection on all portable email devices

Administrative

- No client data on laptops
- No external instant messaging
- Establish strict policy on email usage
- Remote access policy
- No message boards access on Internet
- No downloads permitted
- No personal software
- Only company installed virus protection & FW

Summary – Why Assess?

- Purpose: Showcase Risk Mgmt Strengths
  - Reaffirm & document due care and a prudent information security program
  - Good faith effort towards compliance
  - Lessons learned from past loss/ incidents
- Illuminate Red Flags (weak security controls to improve upon)
  - No firewall
  - Mis-configuration: Key Server in-front of FW
  - No DR Test (many)
  - No DB/Storage Encryption (most)
  - Opening in the Corp Network perimeter (many)
  - IDS really of no help
  - Poor Passwords
  - No background checks
  - No Dedicated Security Personnel/ Role

- Proactive Risk Mitigation Efforts
  - Assess & Test
  - Inventory of Assets; Data, Systems, applications
  - Effective Privacy Policy
  - Employee training
  - Quarterly Pen testing (know the hacker's view)
  - Encrypt & Detect
  - Review of you ASP's & Partners own safeguards

1st Steps

- **Data loss Event**
  - Forensics
  - Public Relations
  - Notifications
  - Litigation Hold
  - Reconcile Event to company policies.

Take Aways

- All data at risk
- Expensive – customers
- Proactive is best
- Expensive – defending a loss
- Now or Later

If Security and Privacy Procedures Fail Cyber Insurance Can Help!

Network and Privacy Insurance Background of ‘Cyber Insurance’

- Exclusion on Traditional Insurance Products (reinsurance implemented virus exclusion in 2001)
- First and Third Party Exposures
- Stand Alone Network Security Policy
- Network and Privacy Endorsements

Network and Privacy Insurance
Gaps in Traditional Insurance Coverages

- General Liability:
  - Impaired access liability
  - Product disparagement
  - Customer injury suits
  - Wrongful or offensive web content
  - Channel attack liability
  - Banner advertising
  - *Copyright* or *trademark* infringement
  - Domain name (trademark) disputes
  - Misuse of *meta tag* language
  - Misuse of *framing* or linking

- Property:
  - No direct physical loss to tangible property
- Misappropriation of a record
  - BI and EE
- Professional Liability:
  - Strict definition of Professional Services
  - Services for a customer and a fee
  - Personal, Advertising and Bodily Injury exclusions

Network and Privacy Insurance
Overview of Insurance Coverages

- Third Party
  - Privacy Liability
  - Network Security Liability
  - Internet Media Liability
- First Party
  - Crisis Management and Notification Expenses
  - Cyber Extortion
  - Digital Asset Loss
  - Business Interruption Loss

Network and Privacy Insurance Privacy Coverage under Network Security

- **Privacy coverage was subject to a network security event**
  - Unauthorized access by a hacker
  - Unauthorized use of a computer system by a rogue employee

- **What about enterprise breaches of privacy?**
  - Stolen/lost laptop
  - Media
  - Administrative errors
  - Human errors

- **Privacy coverage NOW includes failure to properly handle, manage store, destroy or otherwise control**
  - Personal information in any format
  - Third party corporate information in format

Network and Privacy Insurance
Overview of Privacy Liability Coverages

- Identity Theft Response Fund
  - – Notification Expense Fund
    - Covers expenses to notify customers whose sensitive personal information has been breached.
  - – Crisis Management Expense Fund
    - Covers expenses to obtain legal, public relations or crisis management services to restore the company’s reputation.

Network and Privacy Insurance
Overview of Network Liability Coverages

- Network Security Liability
  - Covers any liability of the organization arising out of the failure of network security, including unauthorized access or unauthorized use of corporate systems, a denial of service attack, or transmission of malicious code.

Network and Privacy Insurance
Privacy and Network Liability Market

- Limits of up to $20 million available - single carrier
- Excess capacity available
- Premiums vary according to:
  - Company revenues
  - Industry group
  - Limits, sub-limits, retentions, terms & conditions
  - Information management practices in place
  - Standalone or packaged coverage (1st & 3rd)

Q & A

Contact Information

Gallagher Cyber Risk Services *Joe_Depaul@Ajg.Com* *(212) 994-7054*	**John F. Mullen** *Partner, Nelson Levine* *de Luca & Horst, LLC* *Jmullen@nldhlaw.com* *(215) 358-5154*
Mark Greisiger *President, NetDiligence* *Mark.Greisiger@netdiligence.com* *(610) 525-6383*	*Kristi Janicek*