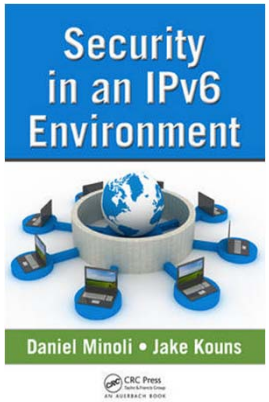
Cyber Liability Insurance Who Pays When Your Data Goes Missing?

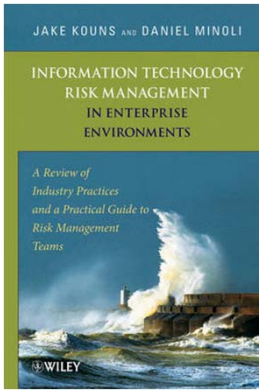
JAKE KOUNS
Markel Corporation

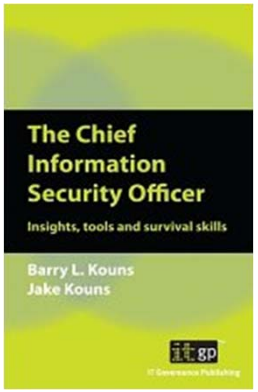
Session ID: GRC-201
Session Classification: Lightning Round

Why Should You Listen?

- Director, Cyber Security and Technology Risks Underwriting at Markel
- Founder / CEO at Open Security Foundation

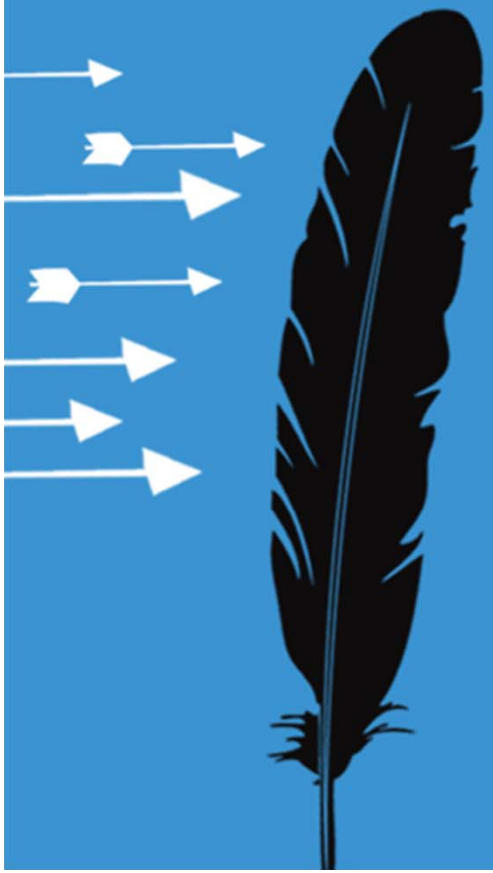






DATALOSS db
open security foundation

April 2010 Issue of SCMagazine



Insurance Drivers and Coverage

Insurance Drivers

- Insurance is purchased for numerous reasons:
  - Reducing liability
  - Loss recovery
  - Legal requirements
  - Securing loans and/or investments
  - Improving business image and stability
  - Peace of mind
- Typically purchased for most valuable assets

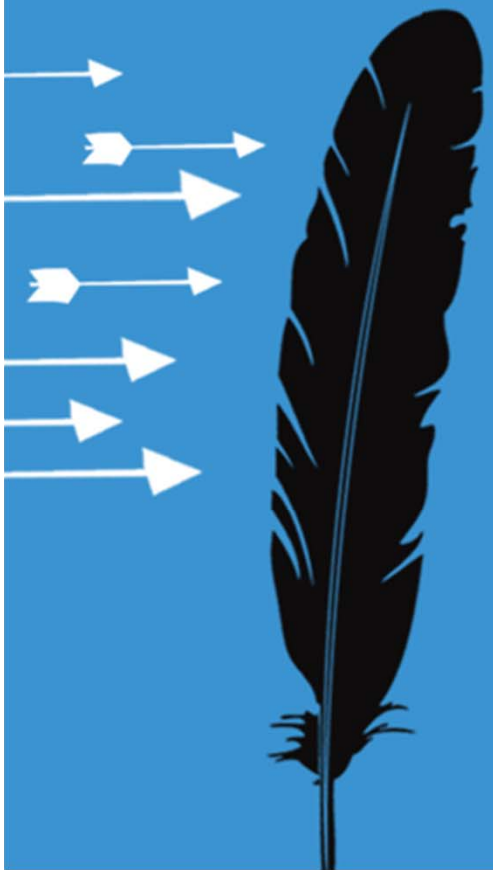
Insurance Coverage

- Do you or have you ever purchased:
  - Car or home insurance?
  - Electronics insurance plan (phone, TV, etc)?
  - Rental car insurance?
  - Trip or event insurance?
  - Umbrella coverage, just in case something happens?

Cyber Liability Insurance

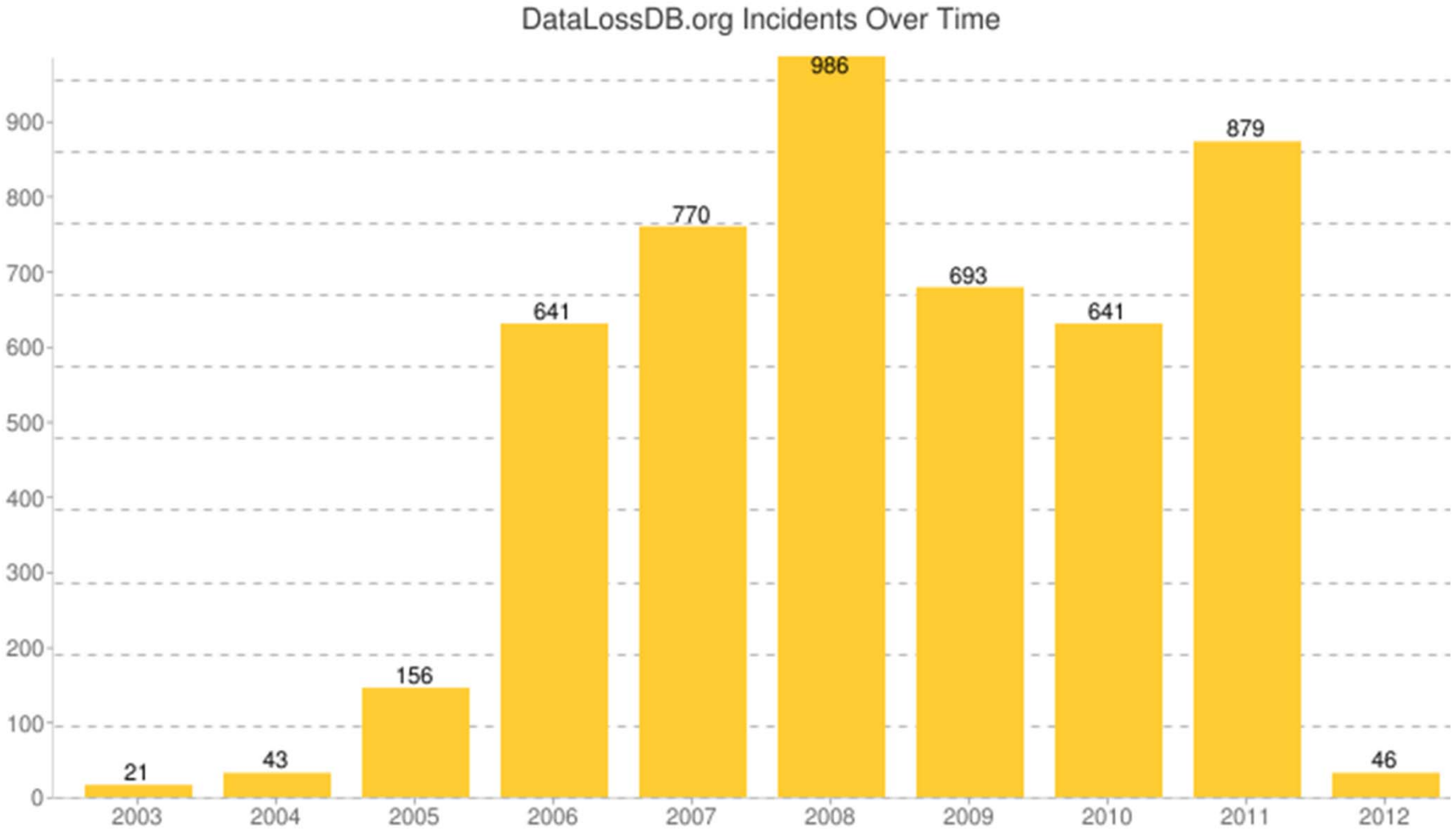
Cyber Liability Insurance

- Why haven't more organizations bought Cyber Liability?:
  - They have "unbreakable" security controls?
  - They are not aware of the market?
  - They think the coverage won't last or respond?
  - They don't believe its a good spend of budget?
  - They believe security risks are decreasing?
  - Something else?
  - Perhaps, organizations don't truly understand it?



Risks and Exposures

Data Breach Statistics



Major Data Breaches

Date	Organization	Breach
2007-01-17	TJ Maxx	94,000,000 Credit cards
2009-01-20	Heartland Payment Systems	130,000,000 Credit cards
2010-11-28	WikiLeaks	US Diplomatic Cables released
2011-04-01	Epsilon	Over 100 companies marketing lists hacked including names and email addresses
2011-04-26	Sony PlayStation Network	77 million names, addresses, email addresses, birthdates, passwords and logins, purchase history and possibly credit cards obtained.

RUNNING A BUSINESS | JULY 21, 2011

Hackers Shift Attacks to Small Firms

Article | Video | Stock Quotes | Comments (39)

Email | Print | Save | +1 1 | Tweet 817 | A A

By GEOFFREY A. FOWLER And BEN WORTHEN

Recent hacking attacks on Sony Corp. and Lockheed Martin Corp. grabbed headlines. What happened at City Newsstand Inc. last year did not.

Unbeknownst to owner Joe Angelastri, cyber thieves planted a software program on the cash registers at his two Chicago-area magazine shops that sent customer credit-card numbers to Russia. MasterCard Inc. demanded an investigation, at Mr. Angelastri's expense, and the whole ordeal left him out about $22,000.

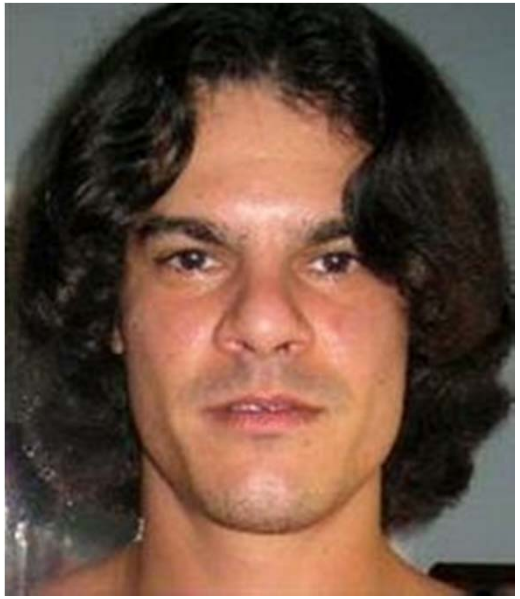
Clayton Hauck for The Wall Street Journal

Joe Angelastri, owner of City Newsstand in the Chicago area, is out $22,000 because cyber hackers attacked his stores' payment system.

His experience highlights a growing threat to small businesses. Hackers are expanding their sights beyond multinationals to include any business that stores data in electronic form. Small companies, which are making the leap to computerized systems and digital records, have now become hackers' main target.

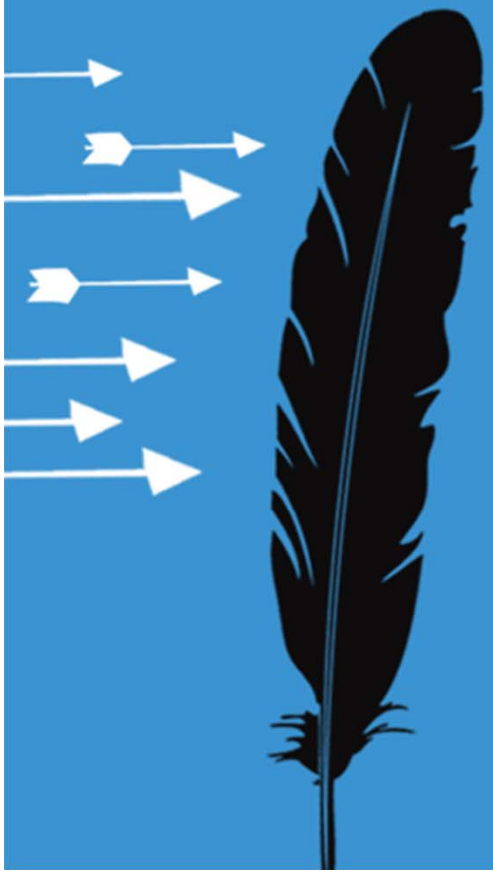
"Who would want to break into us?" asked Mr. Angelastri, who says the breach cut his annual profit in half. "We're not running a bank."

Targeted Attacks



Real Exposures

- No need to use FUD
- Breaches are happening:
  - All types of industries
  - All sizes of organizations
- Costs to recover from a breach are real
- Regulations are increasing



Data Breach Costs

Data Breach Costs

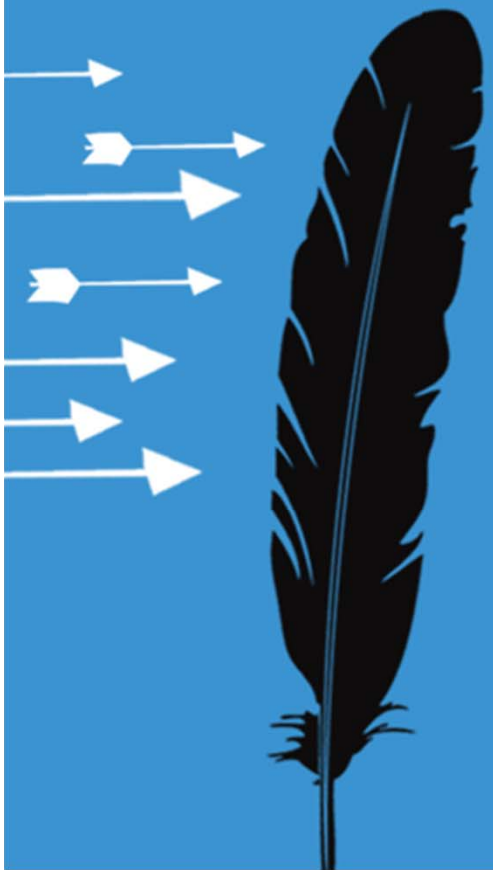
- In 2010, average post-breach cost per record of $214 (up from $204 in 2009)
- Do you agree with this research from Ponemon?
  - $141 indirect costs
  - $73 direct costs
- What should the number be then?

Data Breach Costs – Real Examples

- **Hotel customers' credit card data stolen from hacked server.**
  - Number of Records–700
  - Estimated Costs at $73 per record–$51,100
- **Laptop with employee information stolen out of a parked car.**
  - Number of Records–4300
  - Estimated Costs at $73 per record–$313,900
- **Missing hospital computer tapes containing Social Security numbers of patients.**
  - Number of Records–52,000
  - Estimated Costs at $73 per record–$3,796,000

Data Breach Costs

- Sony costs estimated to be at least $171 million and had to warn investors of the impact.
- Recent federal appeals court decision allows class-action lawsuit to proceed against Hannaford after 2007 data breach.
- California's Sutter Health Faces Two Lawsuits Over Data Breach Affecting 4.2M Patients
- Symantec and the National Cyber Security Alliance estimate average annual cost of cyber attacks was $188,242 for small and medium-sized businesses



Cyber Liability Insurance

Cyber Liability Market

- Annual premium volume information about the U.S. Cyber Risk market is hard to come by
- Annual gross written premium is growing at a rapid pace
- $450-500 million in 2008
- $600 million range in 2009
- $800 million range in 2010
- 29+ Carriers have some kind of a Cyber Liability Product
- Information from Betterley Report June 2011

Many Names, Little Commonality

- Cyber Liability
- Privacy Injury Liability
- Network Security Liability
- Data Privacy
- Theft of Digital Identification
- Cyber Extortion
- Internet Liability

Cyber Liability Exposures

- **3rd Party Liability**
  - Use of your network to harm other 3rd parties
  - Cost to reissue credit & debit cards
  - Lawsuits including fines and penalties
- **1st Party Exposures**
  - Notify affected individuals & credit monitoring
  - Restoration of the system & extra expense to remain functional
  - Security consultants, legal notices
  - Extortion demands, lost monies, lost business
- **Website and Social Media Liability**

Risk Management Services

- Typically included with a Cyber Liability Policy:
  - Security consulting
  - Legal assistance
  - Notification assistance
  - IT forensics / response
  - Portals that include free documents / consulting
  - Hotlines for questions
- Small to medium sized companies find this is extremely valuable

Trigger – Unauthorized Access

- Access gained as the result of fraud or deception
- Authorized user for unauthorized purposes
- Introduction of fraudulent or destructive code
- The threat to initiate malware for the purpose of extorting money or other valuable consideration
- Loss of a laptop or other digital storage device
- Whether or not for profit or gain

Cyber Liability Insurance

But companies have other coverage such as GL or professional liability insurance, so aren't they covered for all this stuff?

Cyber Liability Insurance

SC Magazine > News > Zurich seeking immunity from covering Sony over breach

Zurich seeking immunity from covering Sony over breach

Dan Kaplan July 22, 2011

PRINT EMAIL REPRINT PERMISSIONS TEXT: A | A | A Tweet 22

Sony's insurer is contesting any obligation to cover the electronics giant for costs related to lawsuits filed over its massive PlayStation Network breach earlier this year.

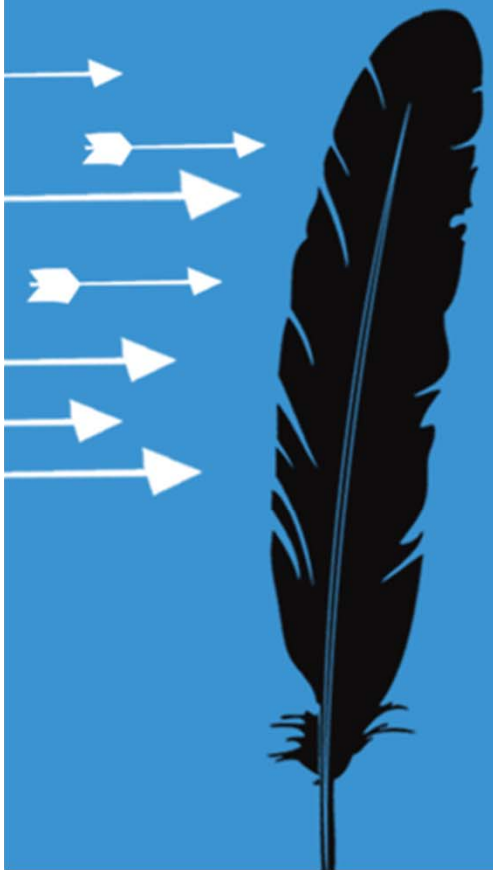
In a complaint filed with the state Supreme Court in New York, Zurich American Insurance Co. is seeking "declaratory relief" from having to defend and possibly compensate Sony over class-action lawsuits or state attorneys general actions filed in response to the breach.

RELATED ARTICLE

- Sony faces new PSN hack
- Sony expects to $171 million ov
- Sony PlayStatio online after intru
- Anonymous spo

Exclusions

- Failure to maintain “reasonable security”
- Wireless
- Failure to comply with PCI standards
- Widespread virus
- Failure to encrypt data
- Paper records
- Fine and penalties (regulatory and PCI)
- Third parties / contractors / service providers / cloud
- Voluntary notification



Integrating Cyber Liability Insurance

Integrating Cyber Liability

- Lets estimate costs for a security program for a small business (Approximately $2-5M revenue)
  - Security Staff
  - Security Software / Hardware
    - Antivirus, Encryption, Firewall, IDS, DLP, Compliance, Scanners, etc.
  - Security Consulting
    - External Vuln Scans, Pen Tests, PCI compliance, Legal, Awareness, etc.

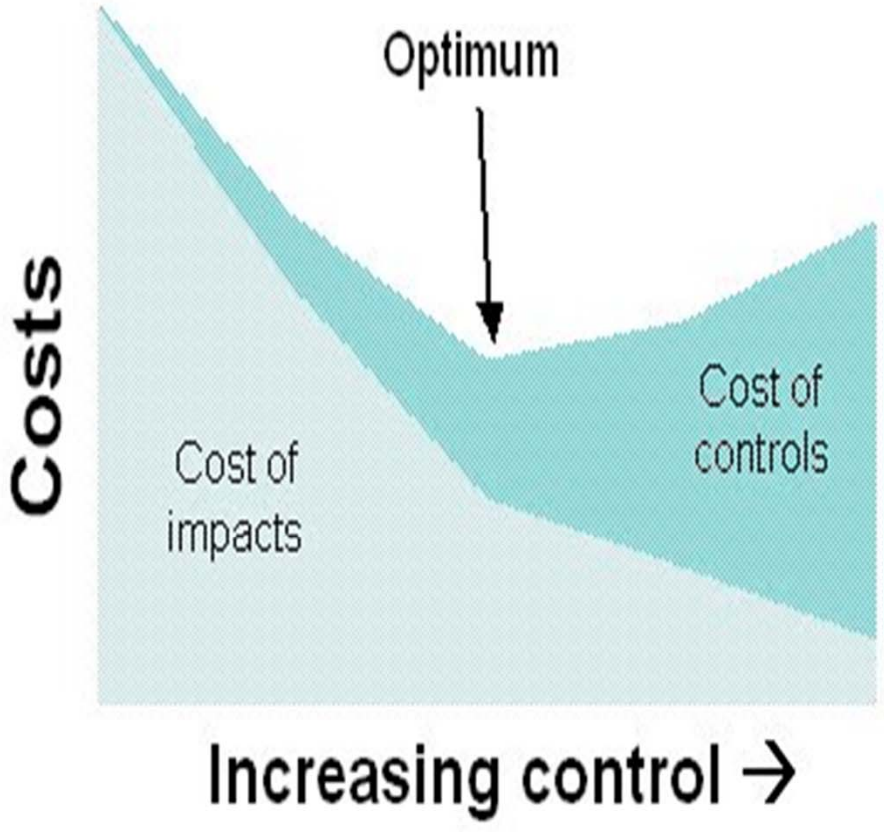
Integrating Cyber Liability

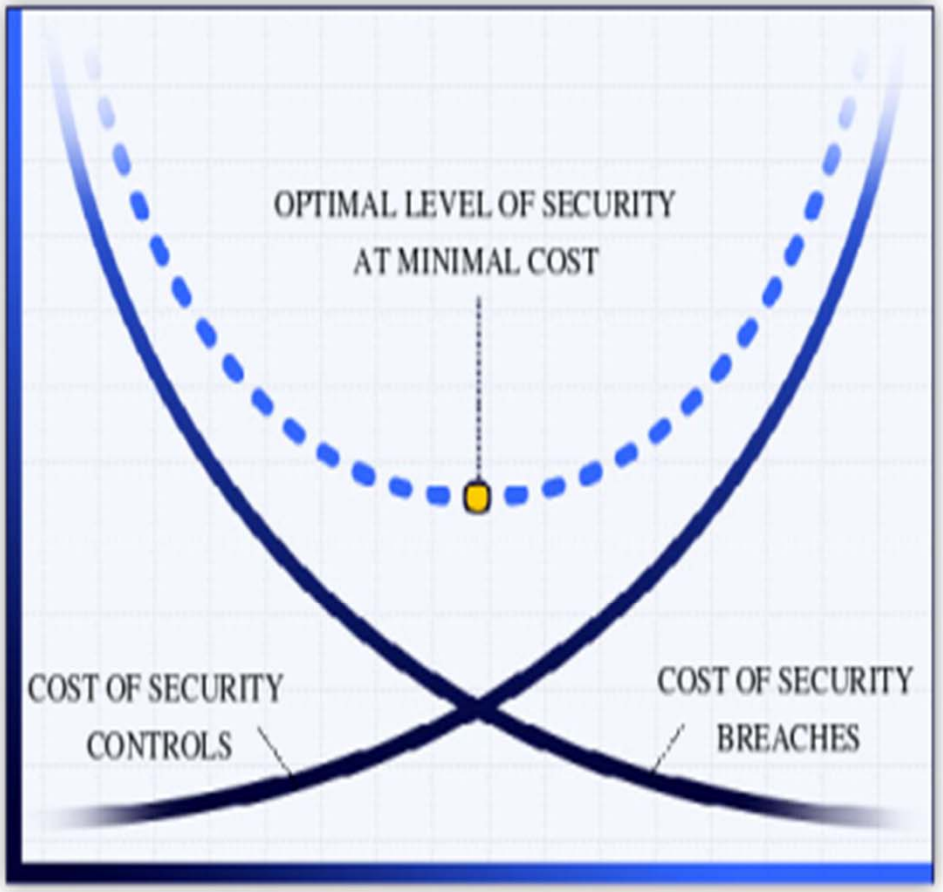
- For sake of argument……..
- Lets say it costs a business with $2-5M in revenues spends approximately $100,000/per year on security
- Not including initial investment costs
- This estimate is extremely low if they are to implement proper security
- Should they be spending more?
- Does this ensure that they won't have a breach?

Integrating Cyber Liability

- Typical costs for Cyber Insurance are currently extremely reasonable
- Minimum premiums can be $1,500 for $1M in coverage
- Includes many Risk Management Services
- Pricing can change based on industry and controls
- Many smaller companies confused by security and are not yet doing anything

Perfect Security





Integrating Cyber Liability

- Larger organizations can also get Cyber Insurance for a reasonable cost
- Large hospital with $2B in revenues premium estimates:
  - $100,000 for $1M in coverage
  - $200,000 for $5M in coverage
- Limits are available up to $50M
- Pricing can change based on industry & controls
- Larger organizations have not shown much interest thus far in actually using Risk Management Services, but like them available

Cyber Liability Underwriting

- Underwriting is far from a science
- Most underwriters are not security experts
- Typically written applications
- Model encourages less information not more
- Minimal security controls that are….. LOW
- Typically no scans or audits performed
- Carriers do have prohibited classes/industries
- Most the market rates on revenues (rather then real exposure of records)

Cyber Liability Insurance

- Effective security programs cost $$$
- Yet, can still be compromised
- Cyber Liability cheaper than most controls and provides serious financial coverage including security services
- If you are a CISO and you have a breach. What do you want to say?
  - Whoops? Sorry.
  - We are covered. Lets file a claim.

Apply Cyber Liability

- In the first three months following this presentation you should:
  - Continue to invest in the appropriate security controls
  - Understand your exposure & number of records
  - Obtain a Cyber Liability quote
- Within six months you should:
  - Define an action plan in case of a data breach
  - Discuss transferring a portion of risk in the form of Cyber Liability insurance with management
  - Define a plan to integrate Cyber Liability into your risk management plan

Data Protection Challenge: Managing Your Legal Responsibilities

Jill Feagans
Network Design Associates, Inc

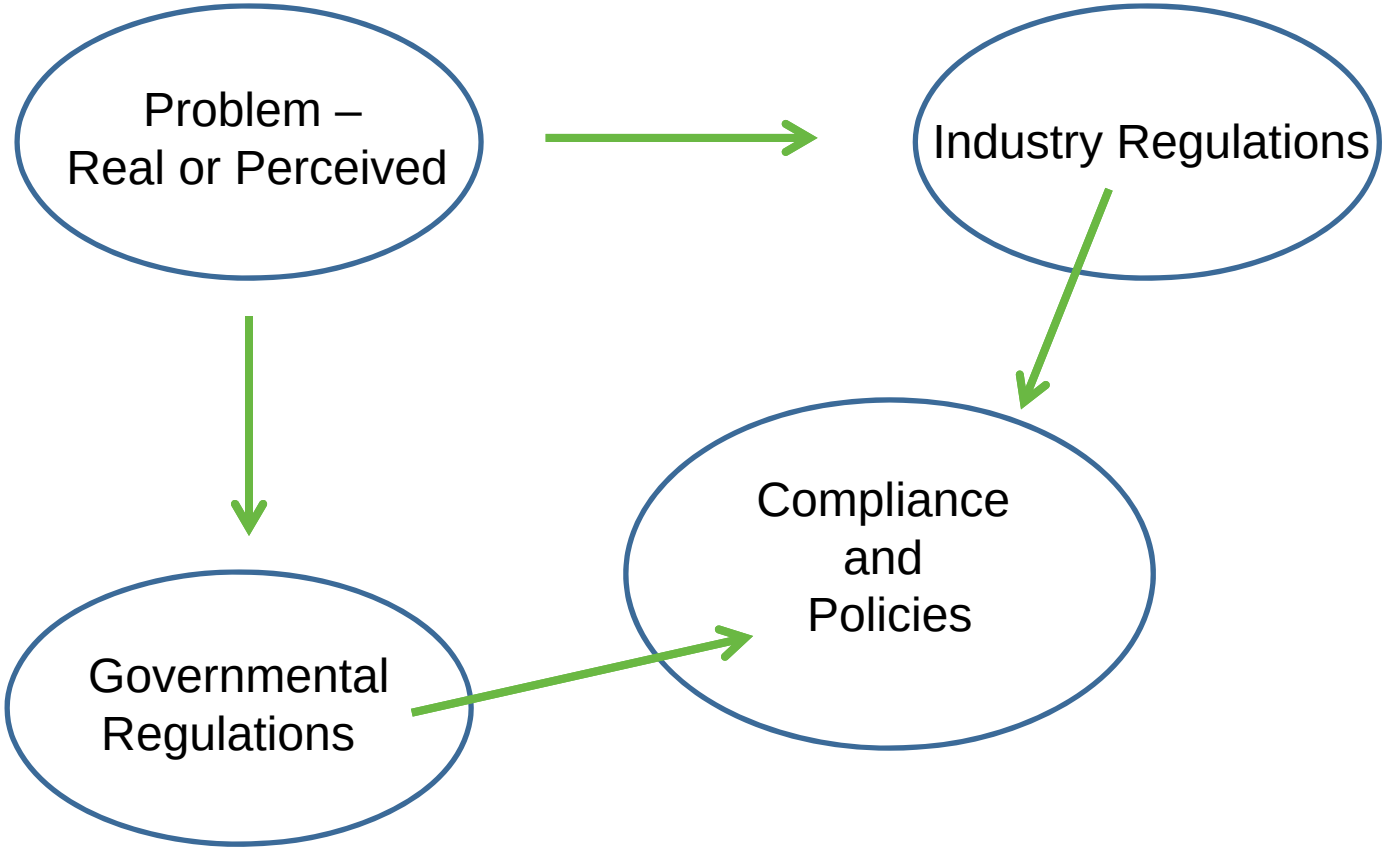
Session ID: GRC-201
Session Classification: Lightning Round

What If…..The Unexpected Occurs?

- Are you ready?
- Regulation and Compliance
- Policy Challenges
- Legal Issues
  - Data Ownership v. Data Stewardship
  - eDiscovery
- Keeping track
- What Can You Do Today?

Regulation and Compliance

Why Regulation and What It Means



Regulation and Compliance

- Increasing regulation which affects information technology
- Implications of regulations
  - Average of 32 regulations affecting every company – not just public sector[1]
  - Large companies can be affected by more than 45 regulations
  - Standards
    - Sarbanes-Oxley
    - HIPAA
    - PCI

[1] ISSA Webcast Changing Face of Security Ethics - 2010

Regulation and Compliance

- Growing areas of regulation and law
  - Electronic Discovery Acts
  - Telecommunications Acts
  - Privacy Acts
  - Stored Communications Acts
  - Rules of Civil Procedure
  - Red Flag Rules
  - Sunshine Laws
- Evolving policy issues
- Evolving legal precedents

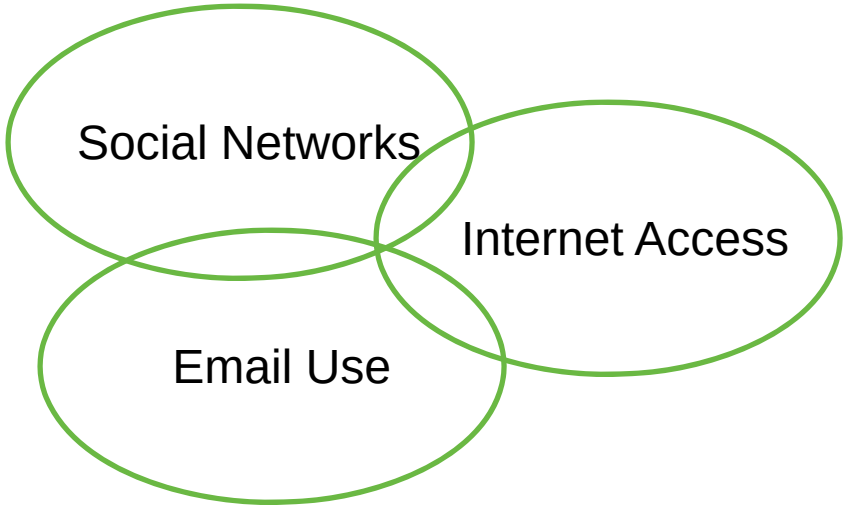
Compliance Framework

- Cross-functional committee develops strategy to achieve compliance
- Security and information technology team are often not part of the strategy process
- ISO 27001
- NIST SP 800-53
- Continuous compliance must be attained

Policy Challenges

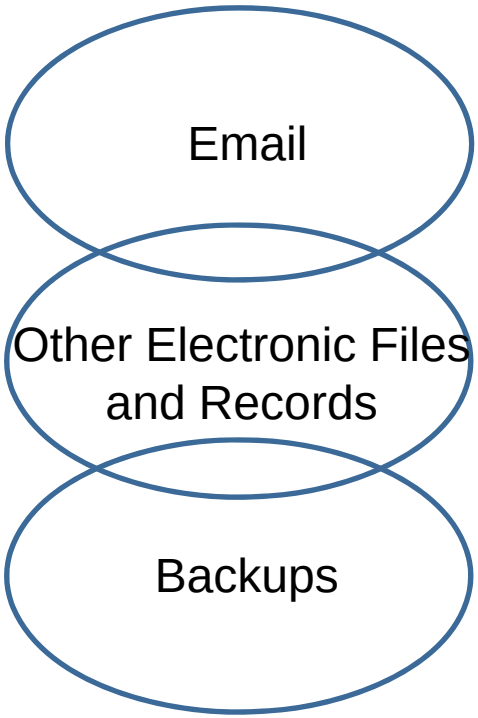
Policies – More Than Just Acceptable Use

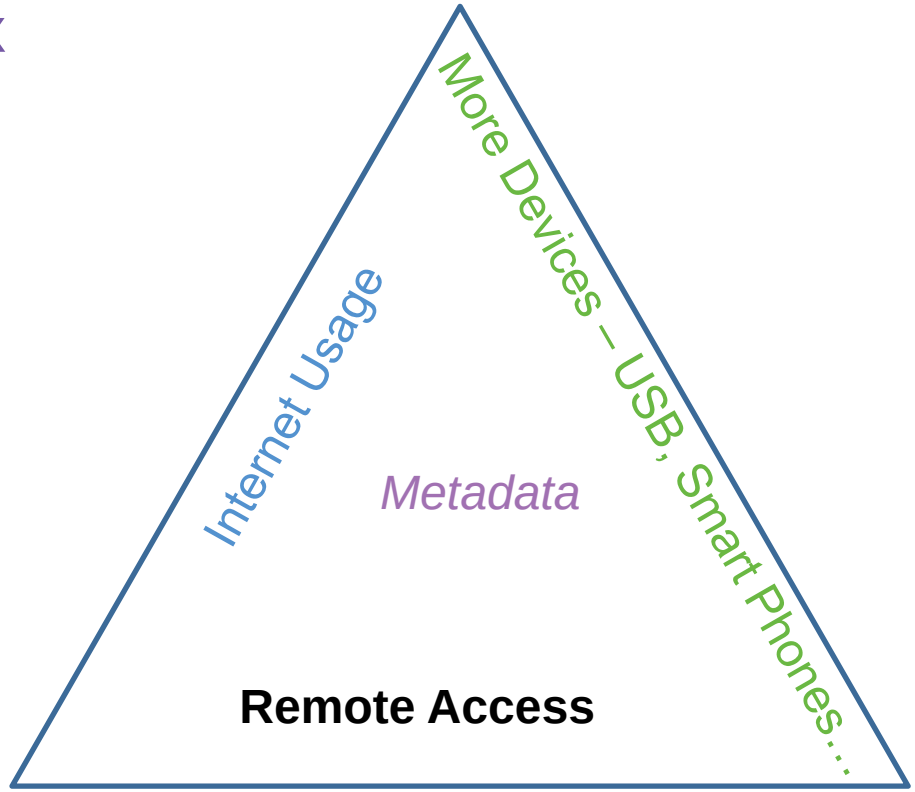
- Acceptable Use
- Privacy
- Security
- Intellectual Property



Policies – More Than Just Acceptable Use

- Retention – Often Most Overlooked!
  - Can be most complex





Challenges

Policies – More Than Just Acceptable Use

- Must be part of daily routine
- Auditing is a useful tool
- Defensible policies do not need to mandate complete retention of all information and documents

Legal Issues

Data Ownership v. Data Stewardship

- Data Owner
  - Ultimately responsible for information
- Date Steward/Data Custodian
  - Responsible for safe handling of data
  - According to ISC^2 must preserve and protect Confidentiality, Integrity and Authenticity
- Example: Healthcare

eDiscovery

- Process to locate and secure any form of electronic data
- Discovery uses
  - PRA's
  - Litigation/Legal proceedings
- What is discoverable?
  - Email
  - Records
  - Calendars
  - Blogs
  - Usage

eDiscovery

- Everyone is at risk!
  - Does not just affect public sector
- Request does not require subpoena
  - Subpoena mandates compliance
- Remember This!
  - It is your job to discover the information
  - Legal staff determines what information is applicable to the request

Litigation/eDiscovery Process

- Part of compliance strategy
  - Determine who should discover – legal or IT
    - Third party?
    - *Garcia v. Berkshire Life Insurance Company*
    - *Vaughn v. City of Puyallup*
  - Same process should be used
    - Retention policy
    - Procedure for discovery
- CANNOT be a reactive process
  - Obstruction

Litigation/eDiscovery Process

- Predictive
  - *Wigington v. CB Richard Ellis*
    - Duty to preserve if could reasonably foresee
  - *Willard v. Caterpillar*
    - Litigation – 10 year difference with record retention
- Usable Form
  - *White v. Graceland College*
  - Printouts of data not acceptable

Litigation/eDiscovery Process

- Metadata
  - AZ first state to require
    - 32 states require in discovery
    - NJ defines limit of discoverability
  - Best Practice: Always provide to legal team – let them make the call
- Device Management
  - *Wilson v. Thorn Energy*
  - Culpable for damages due to fact information on flash drive was not backed up

Keeping Track

Bringing It All Together

- Involve Others
- Reminders on responsibility for all involved
- Get automated tools to maintain in normal course of business operations
  - Retention
  - Policy creation
  - Discovery
  - Compliance
- Always get management and legal involved!

What Can I Do Today?

Where Do I Start?

- Getting Started
  - Identify what regulations apply to your business
  - Determine your risk areas
  - Develop a compliance strategy team
  - Create retention and compliance policies
- Long Term Goals
  - Automate
    - Develop a budget
    - Attain tools
  - Audit

Where Do I Start?

- Issues
  - Regulation and Compliance
  - Policy Challenges
  - eDiscovery
  - Getting it together

- Jill Feagans
  - CISSP,CCSP,CCNP,CCDP,CCVP,MCITP,FCNSP,CCA,MCNI,MCNE
  - jfeagans@ndasacramento.com or jill@graviet.com