McGUIREWOODS
Relationships That Drive Results

Presentation to ACC Charlotte

# Data Security & Privacy

Presented by:

**William J. Cook**

**C. Andrew Konia**

**Mark J. Maier**

November 2, 2011

# Agenda

- Identifying the Issues/Concerns
- Current State/Impact of Breaches
- Susceptible Targets
- Key Terms and Standards
- Questions You Should Ask
- The Laws and Enforcement
- Case Studies – PCI/HIPAA/Industrial Espionage
- Consequences
- The 12-Step Program – Mitigating Risk
- Q&A

# What's the Problem?

- Russia & Bulgaria – Organized Crime
- China – Advanced Persistent Threat
- Unaffiliated Internet Gangs US / Europe
- Corporate Inattention
  - Employees
  - Not aware of threat magnitude
  - Not aware of noncompliance sanctions

# In the News

- Unprecedented rise in the number of hacker attacks and data breaches
- Wide range of companies and organizations have been attacked
  - Sony
  - Citigroup
  - ADP
  - Google
  - EMC Corp
  - Epsilon
  - Lockheed Martin
  - International Monetary Fund
  - Senate website
- Industry survey showed cost to breached companies averaged $7.2 million (Ponemon Institute survey)

# October 2011

- Hannaford Data Breach Lawsuit (October 20, 2011)
  - Class upheld
  - Foreseeable that data loss will cause individual damages
  - A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract."
- Widely Used Web Encryption Algorithm is Vulnerable
  - XML encryption, used to secure communications between Web services, can be exploited.
  - Allows remote break in without physical access.
- DOD $4.98B Data Breach Lawsuit
  - Proposed class action suit involves TRICARE, seeks $1,000 per victim.
  - Physical loss of unencrypted data
  - Healthcare, banks, telecom, governments (fed/state/local) at risk
- JavaScript Hacking Tool Can Intercept PayPal & Other “Secure” Sessions (9/2011)
  - Bank transactions may not be secure.
- Yale Warns 43,000 about 10-month Long Data Breach (8/2011)
  - Prompt and ongoing monitoring

# The Million Dollar Subway Ride

- An employee of General Hospital Corporation and Massachusetts General Physicians Organization Inc. ("Mass General") left documents on a subway that included a patient schedule containing PHI of 192 patients, and billing forms with PHI for 66 of those patients. This included PHI of patients with HIV/AIDS.
- The records were bound only by a rubber band!
- Mass General paid $1 Million to settle the matter

# Current Targets of Hostile Technology

*Individual company loss $1 million to $52 million per incident*

- Payment Processor Breaches: 130 million customer records
- Account Transfers Fraud: $85 million to $255 million keyloggers
- Securities and Marketing Trading Exploitation
- Bank ID and DDOS - $399,000 from account
- ATM Skimming / POS Schemes – one net $600,000
- Mobile Banking Exploits
- Insider Access – Vendors- Industrial Espionage
- Malvertising
- Supply Chain Infiltration
- Teleco and Network Disruption – DDOS

*Source: September 2011 FBI report and Bill Cook*

# Know Your Geek Quiz

*You Should Know Each of These*

- AES 128 bit
- SSL
- RBAC
- 2 Factor Authentication
- 8 Characters with Symbol and #
- Social Engineering
- Law Enforcement Notification Delay
- Business Associate
- PCI DSS
- Breach Notification
- Cloud Security contracting
- DDOS attack
- Social Engineering
- Ping attack

# Corporate Managers are Forced to Ask

- How safe are our systems?
- What can be done in advance to prepare for an attack?
- How should we respond if attacked?
- What will our liability exposure be in the event of an attack?
- What can be done to protect customers, consumers and trade secrets?
- What can be done to reduce losses, minimize potential damages, and protect shareholder value?

# Enforcement

- Retail environment
  - Actual damages from intrusion
  - Noncompliance with PCI DSS
- HIPAA
  - OCR- 150 audits by KPMG before 12/31/12
- SEC 10K disclosures under discussion
- States
  - Breach notification requirements (all but 4 states)
  - Security standards based on PCI standards
  - Some encryption requirements
  - AG lawsuits
- The FTC and online/mobile marketers
- EU vs. US data storage issues

# PCI Case Handling

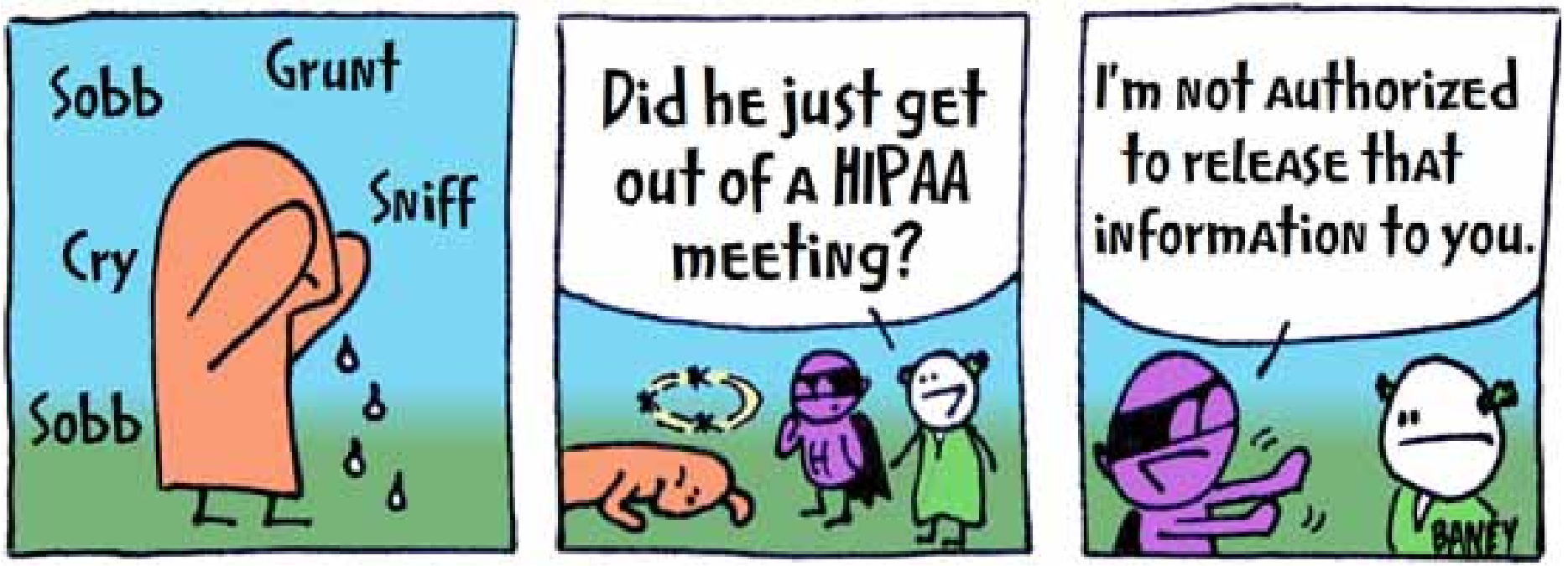
- Define the damage
  - Preserve data environment
  - Determine point of intrusion
  - How long has vulnerability existed
  - How long has it been exploited
  - Vendor involvement with vulnerability
  - Contact law enforcement
- Communicate with your bank
- Determine, with bank, need for forensic audit
- Respond to all credit card company inquiries
- Prepare presentation with assistance of outside counsel
- Negotiate settlements

# HIPAA Breach Case Study

- Laptop stolen from key vendor
- Investigation disclosed all company PHI, PII and salary details lost
- Audit clause of contract triggered at vendors expense
  - Vendor didn't know data location – most overseas and insecure
  - Contrary to contract vendor didn't have uniform security practices
  - Contrary to contract vendor didn't notify company of breach
- Contract modification worked out to preserve contract

# ePHI Security: HIPAA vs. NIST

| Standard | HIPAA | NIST |
|---|---|---|
| Role-Based Access Controls | Addressable | Based on assigned duties; employee satisfies personal security criteria |
| Unique User ID | Required | Ensures that system activity can be traced to a specific user |
| Two-Factor Authentication | N/A | Provides "high level" of confidence in validity of identity |
| Automatic Session Termination | Addressable | Achieved by locking session or disconnecting network |
| Password Requirements (e.g. character length) | N/A | 8-character minimum |
| Encryption Technology | Addressable | 128-bit AES |
| Encrypted Communication Transmission Channels | Addressable | Utilizes secure email connections and message-level standards |
| Risk Assessment/Management | Required | Recommended |


Sobb
Grunt
Sniff
Cry
Sobb
Did he just get out of a HIPAA meeting?
I'm not authorized to release that information to you.
BARNEY

# Industrial Espionage Case Study

- Immediate Emergency Response Team meeting
- Investigate to determine sensitivity level
- Bring in outside counsel to supervise and develop plan
- Consider outside forensic examination
- Interview potential targets
- Seize personal computers and personal computing devices
- Obtain civil search warrant for subject's home
- Keep written record of each step taken and why
- Enforcement options: TRO, law enforcement, meet other side

# Consequences

- Noncompliance (DSSs, Laws, etc.)
  - Fines/Penalties from card associations
    - On acquiring bank as well (passed through)
  - Possible sanctions from federal agencies
  - Curtailment/termination of card processing
  - Probation
  - Actual damages are irrelevant
- Data Security Breach
- Reputational Damage
  - Even without breach or noncompliance
  - Whistleblowing
  - Exponential effect of social media
- Director/Officer Liability/Fiduciary Duties

# The 12-Step Program

1. Be proactive!
2. Establish intracorporate, interdisciplinary Emergency Response Team with authority, mission statement and plan
   - Pre and post; internal and external
3. Create risk-based internal information security regime (policies, technology and HR)
   - Ensure appropriate and consistent application and updating (patches)
   - Employee education (keep a record)
   - Discipline and Termination
4. Protect Personal Information
   - Collection, storage and destruction; Encryption; Non-Disclosure
5. Notification Regime

# The 12-Step Program (cont.)

6. Cooperate with and use law enforcement and its resources (pre/post)
7. Consider intrusion insurance
8. Protect website, marketing & advertising
9. Media Management (pre/post)
10. Routine audits (QSA)
    - Requires regular monitoring and testing (per PCI DSS)
11. Vendor/contract management (pre/post)
    - All vendors are not created equal
    - Give contract drafting due consideration; ensure responsibilities are specific and feasible; Follow-up

# The 12-Step Program (cont.)

12. Know the law and standards that apply to you, and consult with outside counsel when warranted
    - Focus on PCI DSS, SEC requirements and federal and state laws applicable to your business
    - Understand the rapidly changing nature of the laws, regulations and standards
    - Work with experienced and tech-focused outside counsel to establish…
        - The Emergency Response Team and its functions and policies
        - Due diligence track record (pre/post)
        - Compliance programs that meet laws, regulations and standards

# Questions or Comments?

## 900 Lawyers | 19 Offices

**www.mcguirewoods.com**



34436978.1