HR Confidential:

The Expanding Role of HR in Protecting Confidential Information

Susan R. Fiorentino, JD, MA

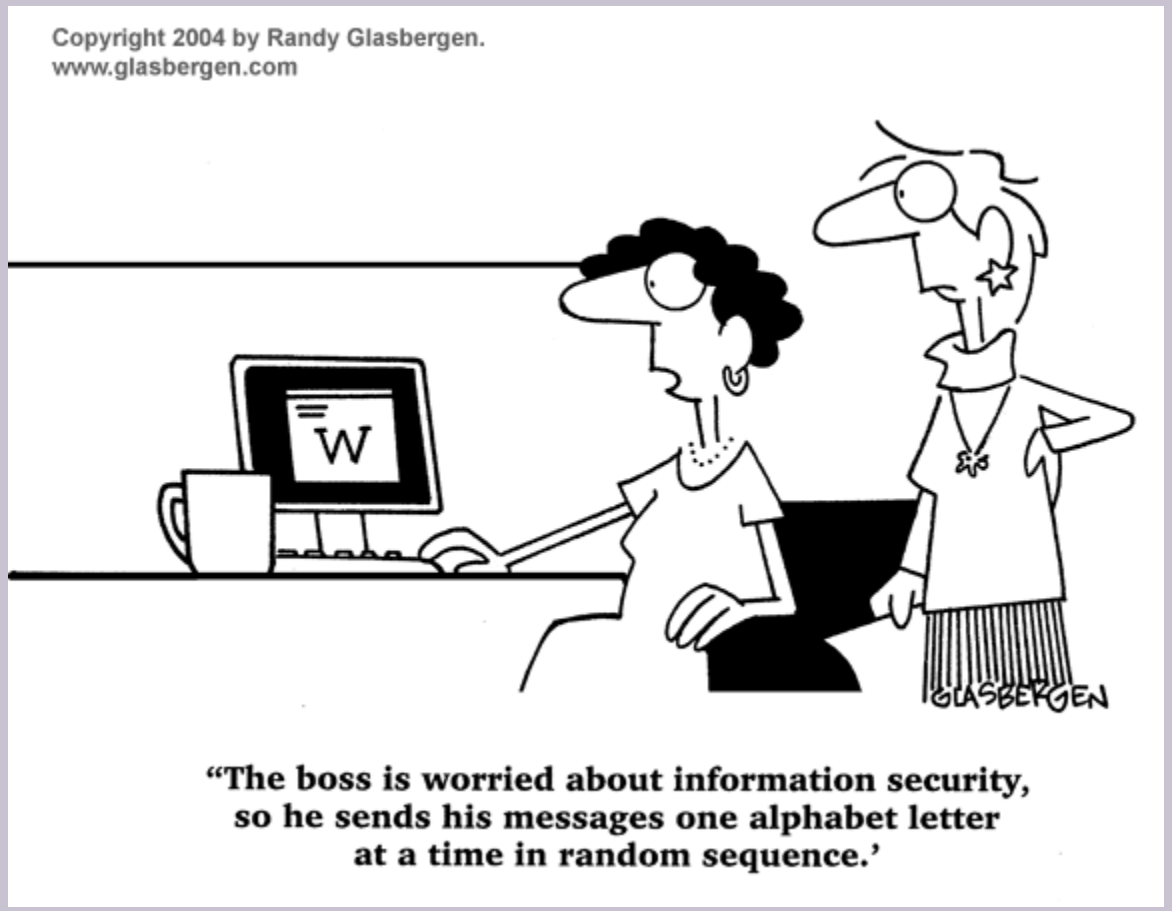
Assistant Professor, Public Policy and Administration

Information Security in the Spotlight

Anthem®

SONY

But first, some comic relief…



Who's Out There?

- Healthcare?
- Financial?
- Educational?
- Other?

Some Ice-Breakers!

- How worried are you?
- Have you already suffered an information breach?
  - Would you know if you had been breached?
- How much effort has your organization put into developing an information security plan?
  - Effective?

Workshop Objectives

1. WHAT is the scope of the problem?

2. WHAT does the law require for protecting and/or reporting confidential information?

3. WHAT confidential information does your organization collect, process, store or transmit?

4. WHAT are some best practices?

Objective #1: SCOPE
2015 Information Security Breaches

- Identity Theft Resource Center Data Breach Report: http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2015.pdf
  - Number of Records Breached as of 10/6/15:
    - 155,825,455
    - 591 breaches

If It Can Happen To Them…

- Vulnerability of Smaller Organizations
  - Lack of understanding about information security
  - Uncertain about how/where to start
    - Lack of resources to engage IT expertise
    - Lack of resources to provide training

It Can Happen to YOU!

- Internal Threats
  - Lost mobile device or USB drive with sensitive data
  - Disgruntled employee takes customer data
  - Carelessly leaving confidential documents out in the open
- External
  - Employee clicks on an emailed phishing link
  - Malware infection that steals and then leaks data

What's the Big Deal?

- Identifiable harms:
  - Identity theft
  - Potential legal penalties
  - Reputational harm
  - Financial harm

Some Basics…

- What IS “information security?”

- What IS confidential information?
  - Personally identifying information
  - Medical information
  - Educational information
  - Financial information
  - Internal or proprietary information

Objective #2:
Laws, Laws Everywhere…

- No SINGLE federal law
- Piecemeal approach to information security law
  - Federal government
  - Industry-specific
  - State level

Federal Government

- Privacy Act of 1974, 5 U.S.C. § 552(a)
- Federal Information Security Management Act(FISMA) 2002, 44 U.S.C. §§ 3541 et seq.
- Veterans Affairs Information Security Act of 2006, 38 U.S.C.§§5722 et seq.
- OMB Guidance, 2007

Private Sector/Industry-Specific

- HIPAA (healthcare)
- Gramm-Leach-Bliley Act (financial)
- FERPA (education)

Health Insurance Portability and Accountability Act of 1996

- PURPOSE of Part C of HIPAA:
  - Establishment of federal standards for the security and confidentiality of protected health information (PHI)
  - Standards are achieved through:
    - "Privacy Rule"
    - "Security Rule"

Do HIPAA Rules Apply to Me? (PROBABLY NOT)

- COVERED ENTITIES:
  - HEALTH PLANS
  - HEALTH CARE PROVIDERS
    - “Business Associates” with whom PHI is shared
  - HEALTH CARE CLEARINGHOUSES
- http://goo.gl/UJusK

Gramm-Leach-Bliley Act of 1999
15 U.S.C. §6801 *et seq.*

- Financial Institutions
- Privacy rule
  - Provides certain notice to customers
- Safeguards rule
  - Financial institution needs to have information security plan with administrative, technical and physical safeguards
- FTC enforces the law and provides training

Some Other Industry-Specific Laws

- **Fair and Accurate Credit Transactions Act** (FACTA)
  - If you use credit screening reports
- **Family Educational Rights and Privacy Act** (FERPA)
  - Personally identifying information in education records
- **Payment Card Industry Data Security Standard**

  (PCI DSS)

State Laws

- State data breach notification laws
  - **WIDESPREAD APPLICABILITY**
  - All states but Alabama, New Mexico and South Dakota
- Requires private or public entities to notify individuals of security breaches of information involving personally identifiable information
  - Credit monitoring sometimes required after breach

A Closer Look: Pennsylvania Law

- "Breach of Personal Information Notification Act of 2006"
  - Broad reach of statute
  - Requires notice of any breach of confidential/personal information
  - Exemptions are important!

OBJECTIVE # 3
WHAT? WHERE? WHO?

- WHAT confidential information does the organization collect, process, store or transmit?
- WHERE can the information be found?
- WHO has access to the information in the organization?

WHAT
Confidential Information

- Recap:
  - Personally identifying information
  - Medical information
  - Financial information
  - Educational information
  - Proprietary information

WHERE IS INFORMATION STORED?

- Network servers
- Desktop and laptop computers
- Personal devices such as phones and tablets
- “The cloud”
- Backup devices like tapes and flash drives
- Email accounts and services
- Paper documents
  - File cabinets
  - Desk access

WHO HAS ACCESS?

- Employees and staff
- Volunteers
- Board members
- External vendors
  - “business associates” under HITECH

Objective #3 Exercise

- WHAT
- WHERE
- WHO

Objective #4
Best Practices=HR+IT

- Comprehensive Plan
  1) WHAT-WHERE-WHO analysis of organization
  2) Development of ISP (Information Security Policies)
  3) Security Awareness Training
  4) IT Best practices

Information Security Policies

- General Policies:
  - Information Security
  - Acceptable Use
  - Clean Desk
  - E-mail/Social Media
  - Mobile Device
- Network Security Policies:
  - Remote Access
- Server Security Policies:
  - Software Installation
- www.sans.org/security-resources/policies

Security Awareness

- Create a “culture of security”
- Appoint a security officer
- Distrust unsolicited links and files
- Distribute policies
- Periodic training
- Disposal awareness
- Physical security awareness
- Develop plan for response to incidents

IT Best Practices*

- Update operating systems and applications
  - Java, Flash, MS Office, PDF readers
- Encryption in transit, in use, and at rest
- Firewalls, anti-virus
- Limit administrative access
- Password strength or multifactor authentication
- Cautious use of emails
- Minimize data access/storage on mobile devices
  - *Special thanks to Prof. Tom Imboden

Case Study: "Credit Counselors R US"

- A nonprofit organization with a staff of 20 employees provides credit counseling for low income individuals:
- WHAT:
  - Financial information from variety of sources, including W-2s, 1040's, bank accounts and credit reports
  - Personally identifying information of clients and staff
- WHERE:
  - Electronic files stored on server
  - File cabinet personnel files
  - Laptops and mobile devices
- WHO:
  - staff

Information Security Plan for Credit Counselors R US

- Start with WHAT-WHERE-WHO analysis of organization
- Adopt Appropriate Info Security Policies
  - Gramm-Leach-Bliley Safeguard and Privacy Rules
  - General and Network/Server Policies
- Security Awareness Training
- Implement IT Security Measures

Susan R. Fiorentino, Esq.

- Susan Fiorentino is Assistant Professor at West Chester University in the Department of Public Policy and Administration. In addition, she counsels clients in employment and labor law matters.
- *The Law Office of Susan Fiorentino, LLC*
  - sfiorentino@sfiorentinolaw.com
  - 610-209-3741