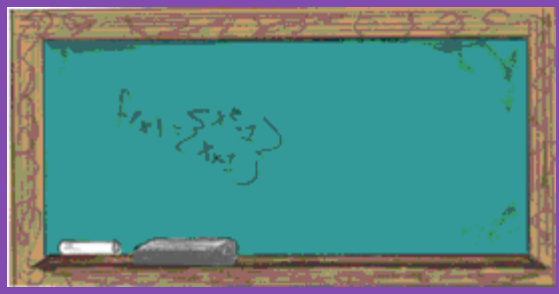
Grant Thornton

# Is your privacy secure?

## HIPAA Compliance Workshop
September 2008

Presented by:
**Andrés Castañeda**, Senior Manager
**Steve Nouss**, Partner

# Agenda



- Have you secured your key operational, competitive and financial information?
- IT control options to secure your key information
- IT control options to prevent fraud
- Case study: How HIPAA helped the healthcare industry protect their confidential information
- Case study: How to protect key information in different areas of your business


UM ETHICS PROGRAMS © 2002

# Have you secured your key operational, competitive and financial information?

## In the news…

Education Department working to fix software after student loan data breach
StarTribune.com

Sentry Insurance Customer Data Sold by Thief
Duluth News Tribune

Hacker swipes PortTix data
Portland Press Herald

CPA group says hard drive with data on 330,000 members missing (AICPA)
computerworld.com

Insurance firm posts private data breach to customers (Blue Cross Blue Shield of NC)
Infowatch.com

IRS Laptop Lost With Data on 291 People
www.washingtonpost.com

Veterans Affairs warns of massive privacy breach
SecurityFocus.com

Bank security breach may be biggest yet: Account info at Bank of America, Wachovia sold by employees; more arrests expected, N.J. police say.
CNN Money

Breach exposes H&R Block customers' tax records
News.com

# Have you secured your key operational, competitive and financial information? (cont.)

**Gartner Group analysis**:

- By the end of 2007, 75% of enterprises were infected with undetected, financially motivated, targeted malware that evaded their traditional perimeter and host defenses.
- The threat environment is changing - financially motivated, targeted attacks are increasing. Automated malware generation kits allow quick, simple creation of thousands of variants, but our security processes and technologies haven't kept up.

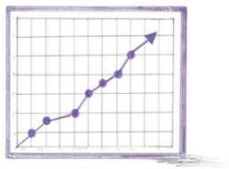
# Have you secured your key operational, competitive and financial information? (cont.)

**What information is important to your organization?**

Payroll Information

Proprietary Information

Acquisition Targets

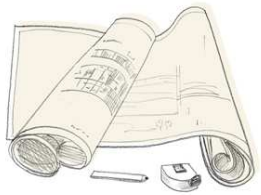


Financial Information

Cost Structure

Supplier Information

Client Listing



R&D Information

# Have you secured your key operational, competitive and financial information? (cont.)

- Securing your organization's information involves:
  - Preventing unauthorized access
  - Preventing unauthorized transmission
  - Preventing accidental or intentional destruction
  - Preventing unauthorized modifications

# Have you secured your key operational, competitive and financial information? (cont.)

**What are the threats?**

- Threats to data security can be grouped into three categories:
  - **Physical threats** – e.g. hurricane, fire, theft, flood, and power outages
  - **Human error** – e.g. careless disposal of information, sharing access information, social engineering techniques and transmitting data using non-secure channels
  - **Malicious activities** – e.g. malicious damage, corporate espionage, viruses and fraud

# Have you secured your key operational, competitive and financial information? (cont.)

## What are some of the weak points?

Trash

Segregation of Duties

Physical Security

Smartphones

Authentication

Media

Internet

Reports

Laptops

Outdated Technology

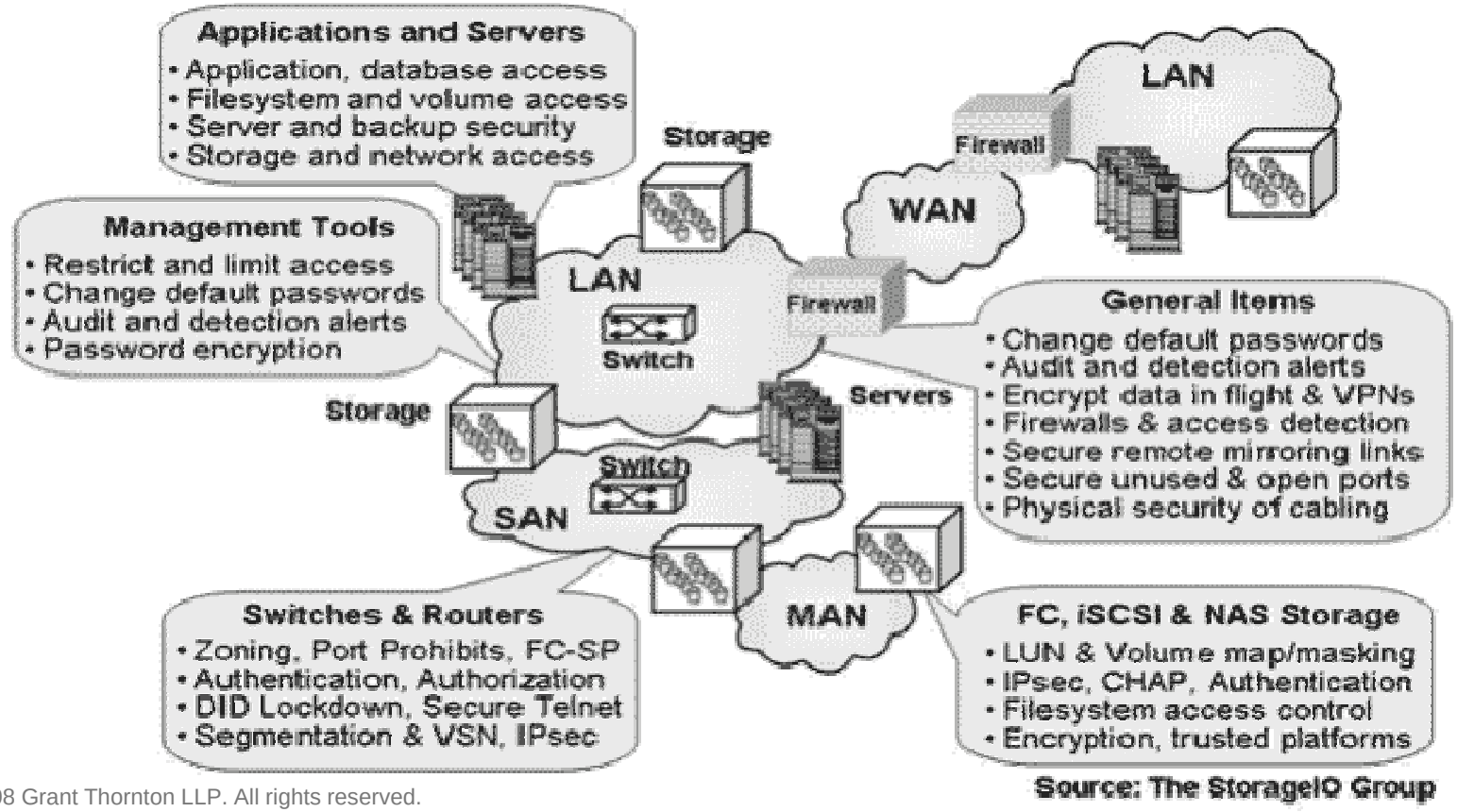
Portable Storage

Social Engineering

Inadequate Network Architecture

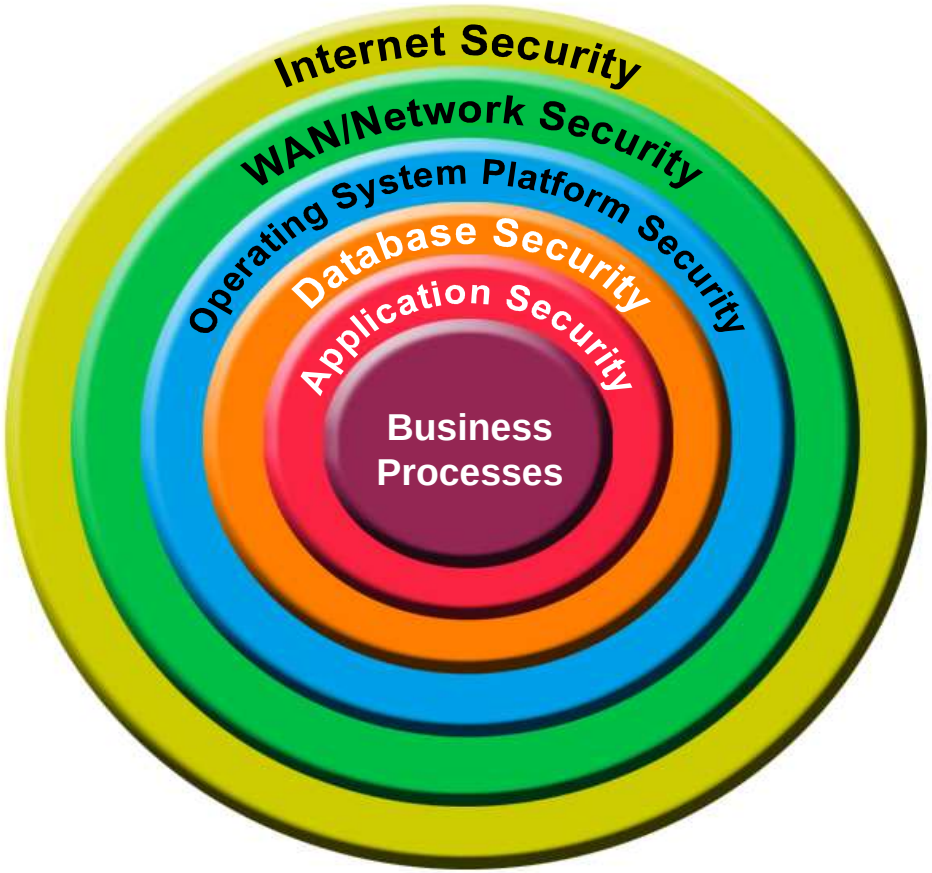
# Have you secured your key operational, competitive and financial information? (cont.)

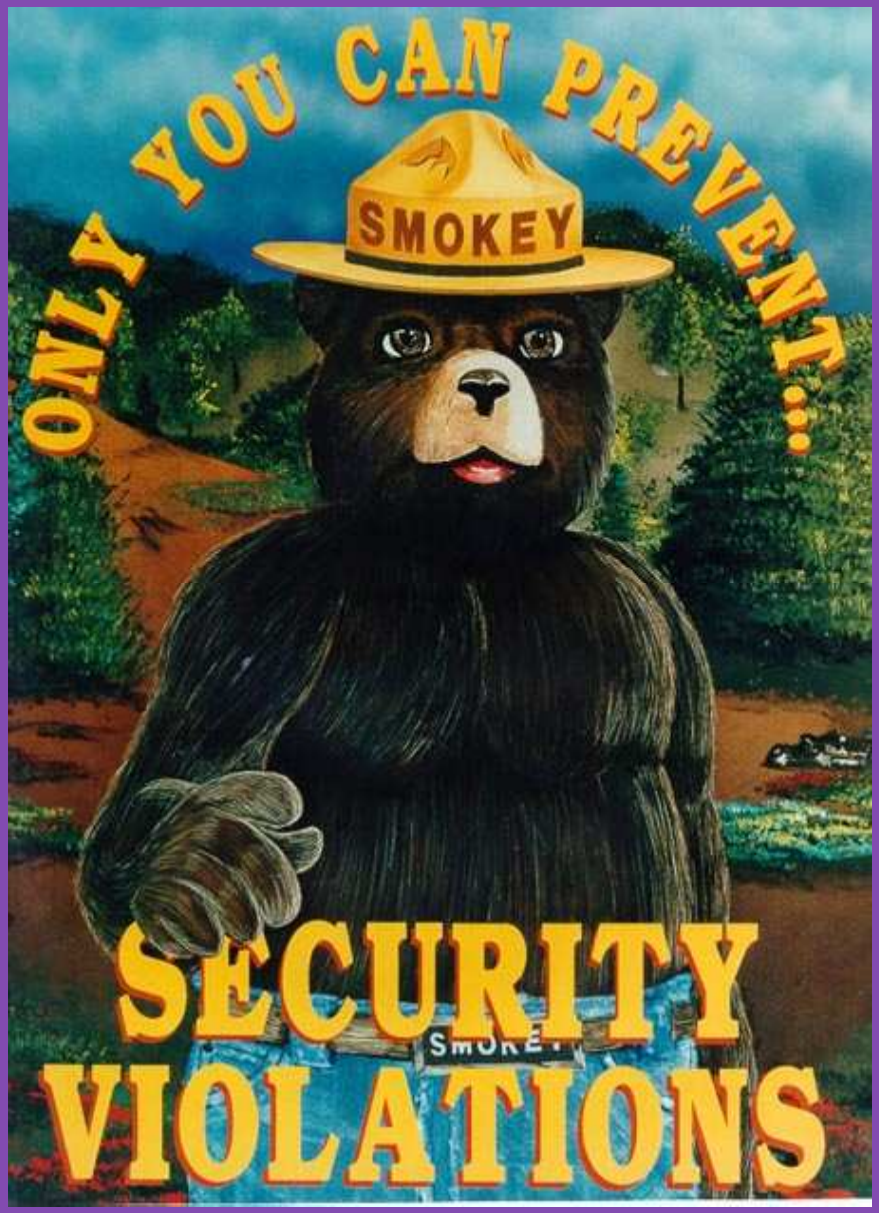
## Common risk areas for the information



# Have you secured your key operational, competitive and financial information? (cont.)

**At what levels should security be implemented?**






UM ETHICS PROGRAMS © 2002

# IT control options to secure your key information: **How can you secure your data?**

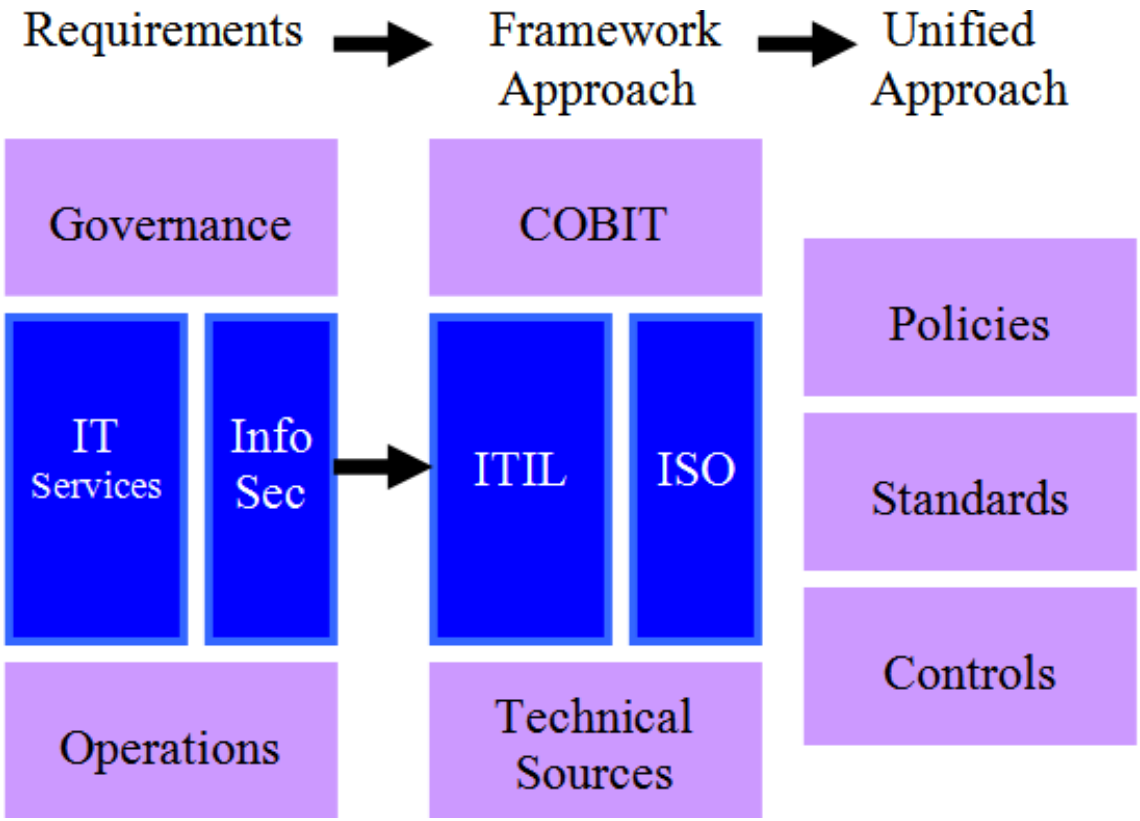
- **Logical security** – e.g. passwords, segregation of functions, encryption, firewalls, antivirus software
- **Physical security** – e.g. restricted access to the data room, networking cabinets, tokens and workstations
- **Network infrastructure** – multi-tiered data protection schema with multiple levels of protection to ensure that data is protected if a layer is compromised

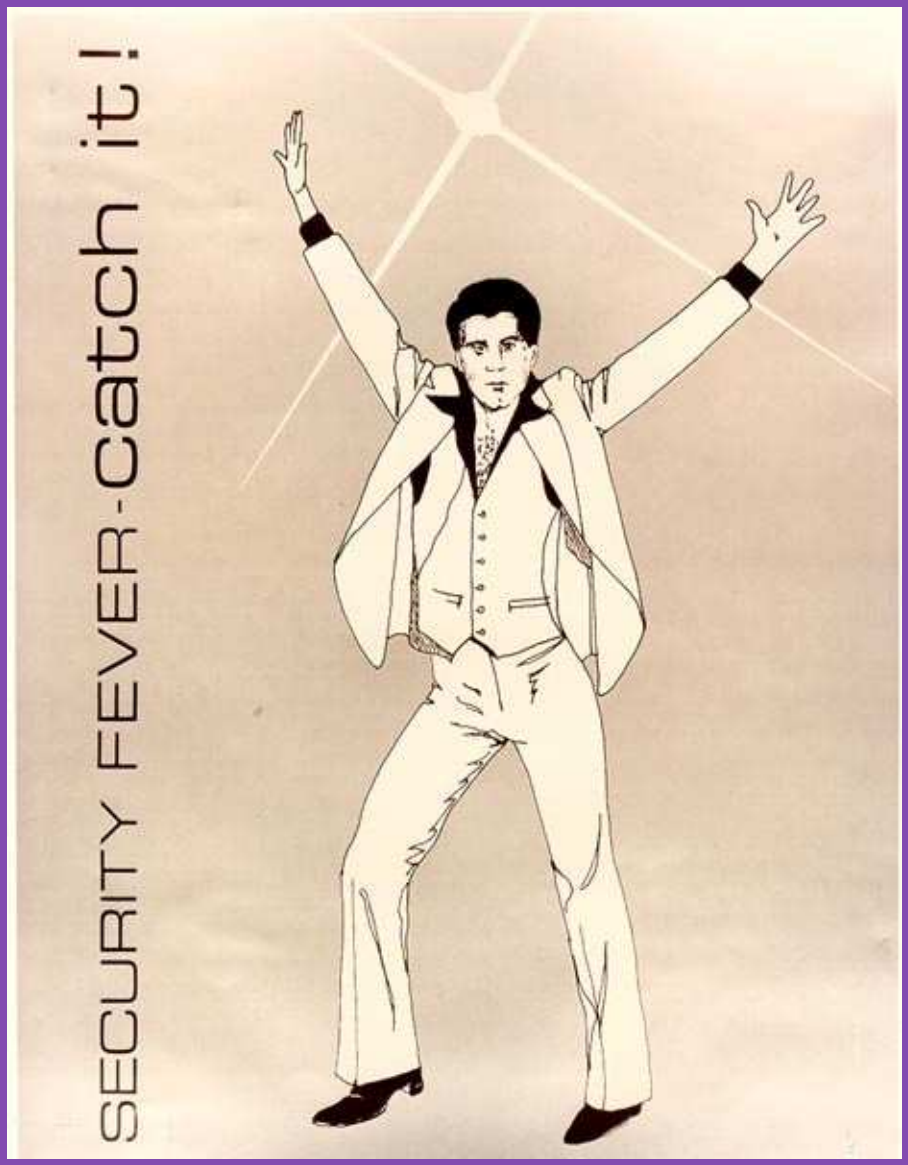
# IT control options to secure your key information
## **How can you secure your data?** (cont.)

- **Backups** – e.g. backup strategy, offsite storage and recovery strategy
- **Data Loss Prevention** (DLP) – Implementing a DLP that ensures protection of the sensitive data during storage and transmission by allowing for:
  - content inspection
  - automatic protection of sensitive data
  - incident response workflow

# IT control options to secure your key information
## **How can you secure your data?** (cont.)

### Implementing an IT control framework:



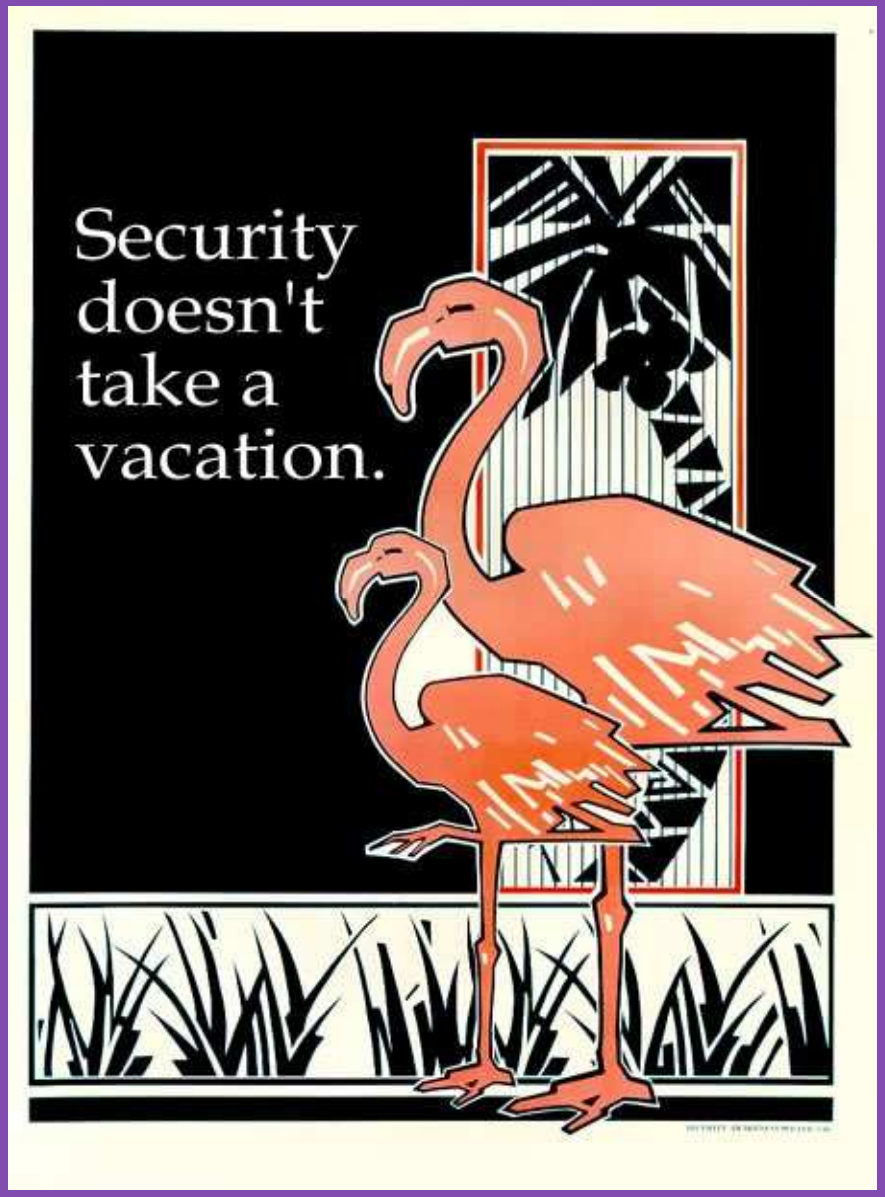



UM ETHICS PROGRAMS © 2002

# IT control options to prevent fraud

**How can IT help prevent fraud?**

- Enforce segregation of duties
- Log sensitive transactions
- Generate automated exception reports
- Allow ongoing monitoring of the IT environment
- Safeguard sensitive data
- Restrict user access to all layers of the IT stack

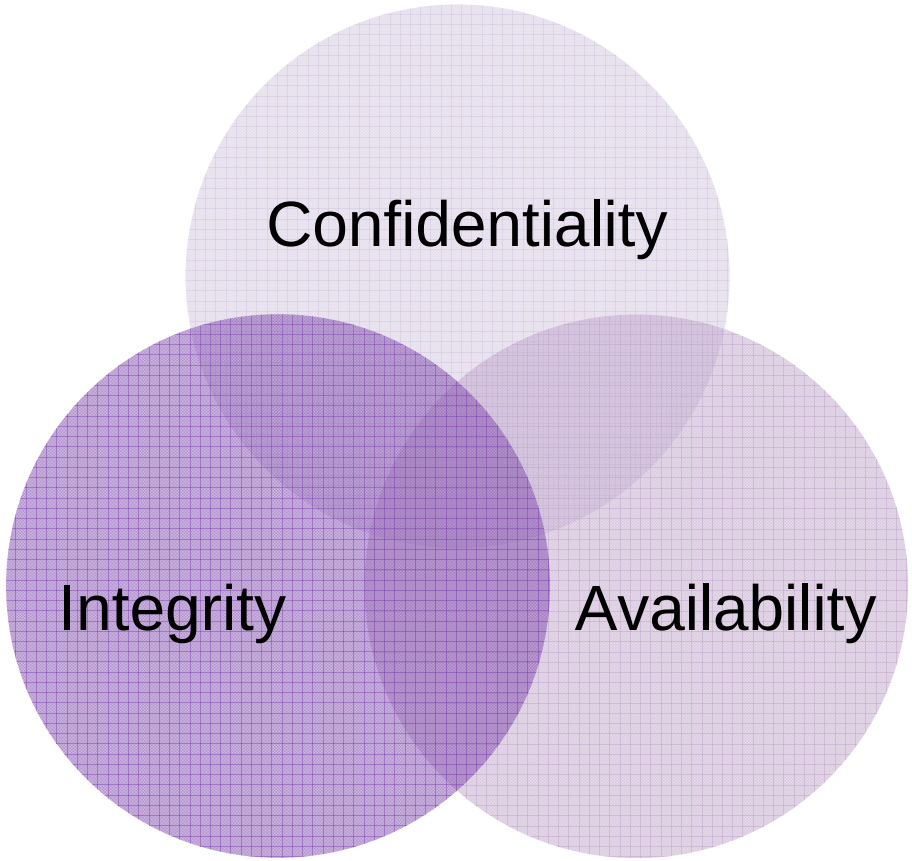



UM ETHICS PROGRAMS © 2002

# Case study:
# **How HIPAA helped the healthcare industry protect their confidential information**

HIPAA forever impacted the internal and external operations of the healthcare industry by protecting both employees and patients under Federal law. While HIPAA regulations are not entirely IT related, information security plays a vital role in complying with HIPPA. In fact, two of the four main objectives of HIPAA are directly related to information security, including the reduction of fraud and abuse, and the safeguarding of Protected Health Information.

# Case study:
# **How HIPAA helped the healthcare industry protect their confidential information** (cont.)



# Case study:
# **How HIPAA helped the healthcare industry protect their confidential information** (cont.)

**Confidentiality:**

- "The property that data or information is not made available or disclosed to unauthorized persons or processes."
- Providers must protect against unauthorized
  - Access
  - Users
  - Disclosures

# Case study:
# **How HIPAA helped the healthcare industry protect their confidential information** (cont.)

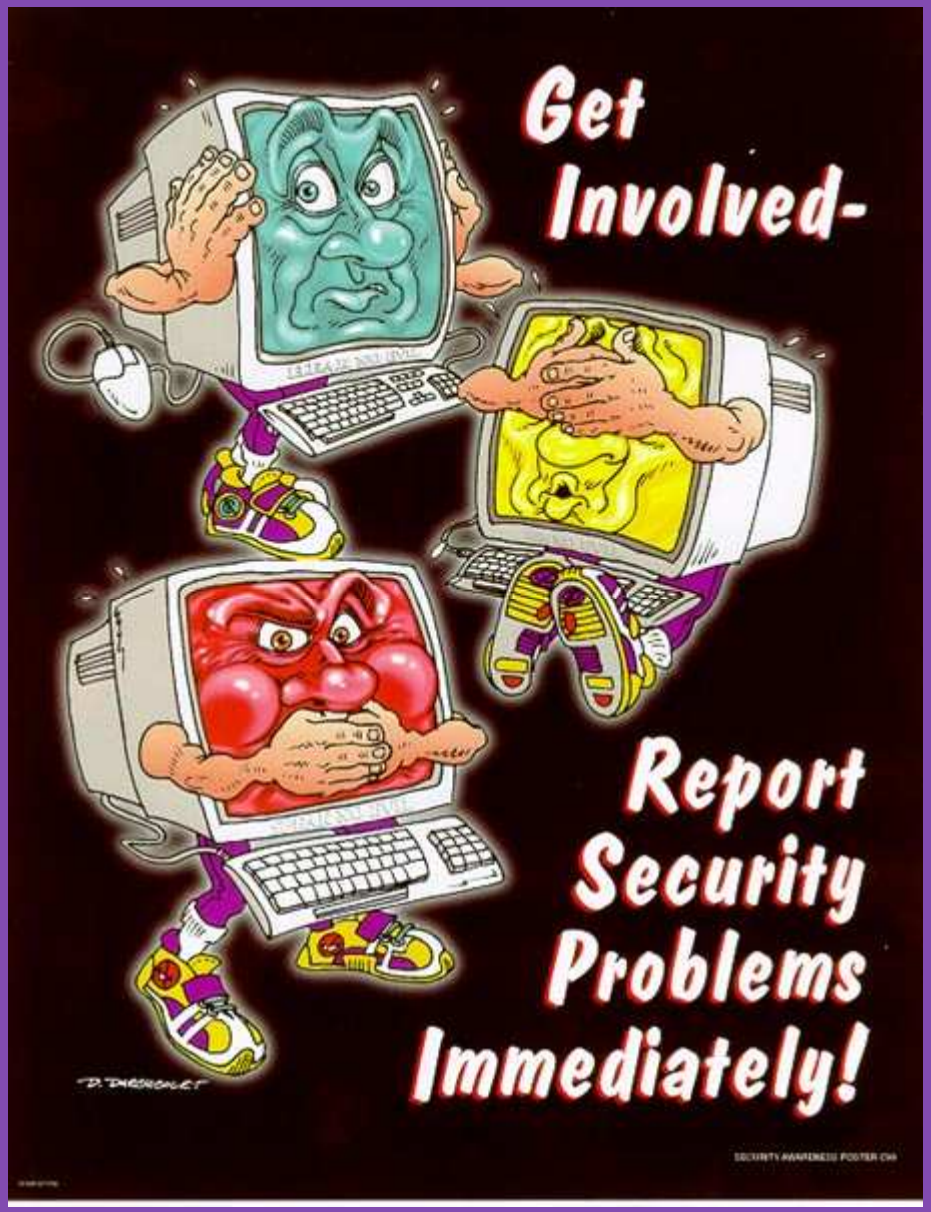
**Integrity**: "The property that data or information has not been altered or destroyed in an unauthorized manner."

- Providers must protect against improper destruction or alteration of data
- They must also provide appropriate backup in the event of a threat, hazard, or natural disaster

# Case study:
# **How HIPAA helped the healthcare industry protect their confidential information** (cont.)

**Availability**: "The property that data or information is accessible and usable upon demand by an authorized person."

- Must guard against threats and hazards that may deny access to data or render the data unavailable when needed
- Must provide appropriate backup in the event of a threat, hazard, or natural disaster
- Must provide appropriate disaster recovery and business continuity plans for departmental operations involving electronic protected health information (ePHI).




UM ETHICS PROGRAMS © 2002

# Case study:
# **How to protect key information in different areas of your business**

Accounts Payable

Inventory

Accounts Receivable

Online Banking

Payroll

# Case study:
# **How to protect key information in different areas of your business** (cont.)

**Accounts Payable**

- Segregation of the ability to receive and buy goods
- Access controls to the receiving function
- Access controls to the purchasing function
- Monitoring of unusual transactions

# Case study:
# **How to protect key information in different areas of your business** (cont.)


- Segregation of the ability of creating and approving payments using the online banking application
- Security tokens to access the online banking application
- Digital certificates to access the online banking application
- Encryption of information

# Case study:
# **How to protect key information in different areas of your business** (cont.)

**Inventory**

- Segregation of the ability to maintain the inventory levels and participation in the inventory control processes
- Restriction to adjust the inventory levels
- Ongoing monitoring of inventory levels
- Automated inventory control processes

# Case study:
# **How to protect key information in different areas of your business** (cont.)

**Payroll**

- Restriction to modify the payroll information
- Encryption of the payroll information
- Segregation of duties to ensure that the person who approves time reports does not prepare, disburse, or reconcile payroll
- Reporting of changes to the payroll data

# Case study:
# **How to protect key information in different areas of your business** (cont.)

**Accounts Receivable**

- Segregation of the ability to receive and buy goods
- Access controls to the receiving function
- Access controls to the purchasing function
- Monitoring of unusual transactions

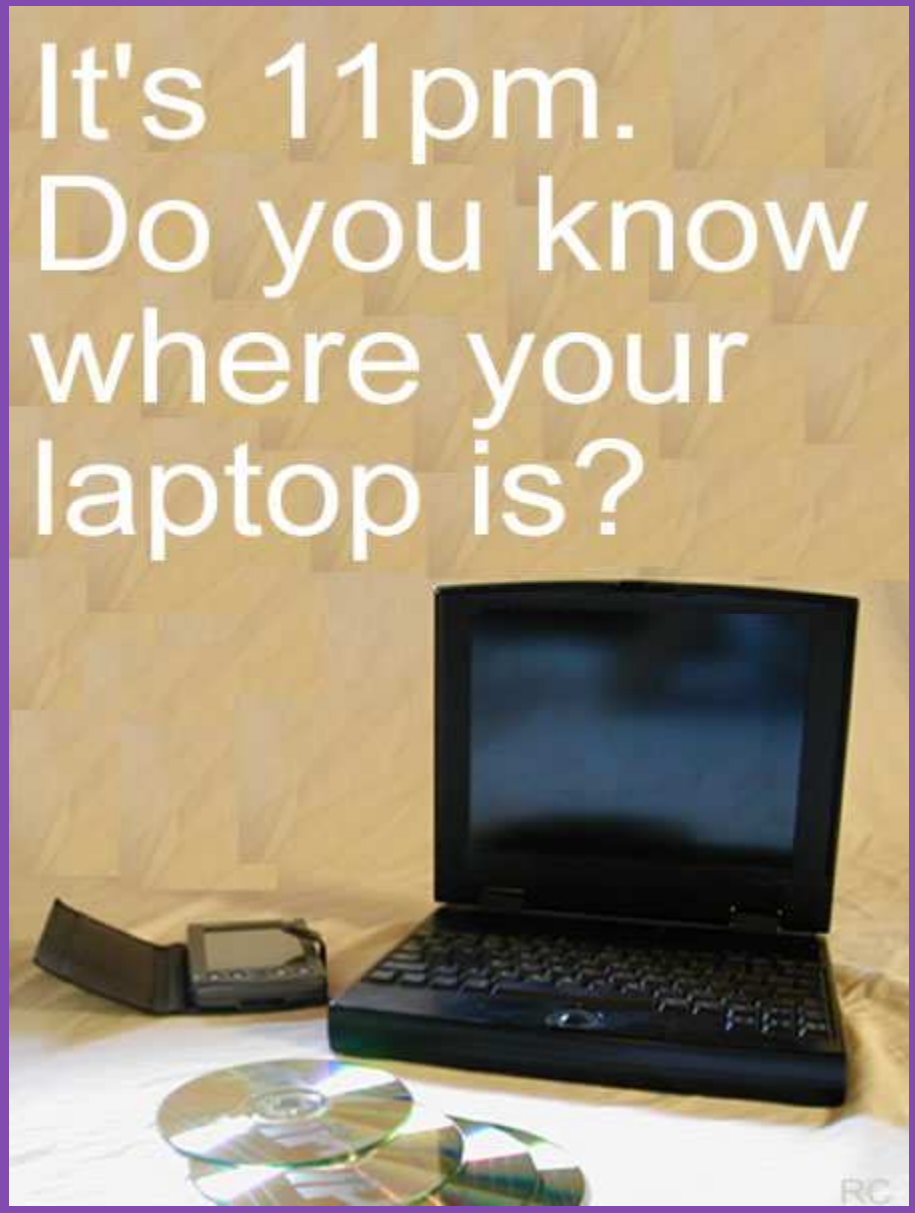
# Q&A

Grant Thornton

**For additional information, contact:**

**Andres Castañeda,** Senior Manager, Advisory Services
**T** 786.206.2311
**C** 954.817.0663
**E** Andres.Castaneda@gt.com

**Steve Nouss,** Partner, Advisory Services
**T** 954.727.5610
**C** 954.254.0222
**E** Steve.Nouss@gt.com




UM ETHICS PROGRAMS © 2002