

**HORNE**  
BANKERS' FORUM **2010**

## A Practical Approach to Assessing and Managing IT Risks

Tony Brooks, CISA  
HORNE LLP Principal  
1020 Highland Colony Parkway  
Suite 400  
Ridgeland, MS 39157  
tony.brooks@home-llp.com  
601.326.1281

©HORNE LLP 2010



### AGENDA

- **What is Risk Management?**
- **Performing a Risk Assessment**
- **Focus on IT Security Risks**
- **Building a Successful IT Security Risk Management Program**

**HORNE**  
BANKERS' FORUM **2010**



## WHAT IS RISK MANAGEMENT?

**HORNE**  
BANKERS' FORUM 2010

**HORNE**  
CPAs & Business Advisors

## WHAT IS RISK MANAGEMENT?

### **Risk Management**

The identification, assessment, and prioritization of risks followed by a coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events



**HORNE**  
BANKERS' FORUM 2010

**HORNE**  
CPAs & Business Advisors

## WHAT IS RISK MANAGEMENT?

### **Risk Management Mandates in Banking**

- GLBA – Sec. 501(b), Protection of Nonpublic Information
- FFIEC – IT Examination Handbook
- FFIEC – Risk Management of Remote Deposit Capture
- FFIEC – Authentication in an Internet Banking Environment
- FFIEC – Guidance on Protecting Against Pharming Attacks
- FFIEC – Guidance on the Security Risks of VoIP
- FFIEC – Guidance on Mitigating Risks From Spyware
- FACT Act – Red Flag Rules
- NACHA 2010, Amendments Regarding ACH Risk Assessment
- PCI-DSS – Payment Card Industry Data Security Standards
- Security Breach Notification Laws now in 46 States

## WHAT IS RISK MANAGEMENT?

### **Goals of IT Risk Management**

- Ensure confidentiality, integrity, and availability of confidential and critical information
- Protect against any reasonably anticipated threats or hazards
- Protect against unauthorized uses, modifications, deletions or disclosures
- Ensure compliance with applicable laws, regulations, and contractual terms
- All this while meeting business needs and goals

PERFORMING A RISK ASSESSMENT

**HORNE**  
BANKERS' FORUM 2010

**HORNE**  
CPAs & Business Advisors

PERFORMING A RISK ASSESSMENT

**Risk Assessment Steps**

▪ Inventory assets	▪ What do you want to protect?
▪ Identify potential threats to those assets	▪ What can cause harm?
▪ Identify vulnerabilities that may allow the identified threats to occur	▪ What puts you at risk for harm?
▪ Identify the likelihood that those threats may occur	▪ How likely is harm to occur?
▪ Identify the potential impact of identified threats should they occur	▪ What harm will result?
▪ Identify existing controls that are designed to mitigate threats	▪ What protects you now?
▪ Recommend new controls that can further reduce the impact of threats	▪ What else do you need to do to reduce your risks?

**HORNE**  
BANKERS' FORUM 2010

**HORNE**  
CPAs & Business Advisors

## PERFORMING A RISK ASSESSMENT

### What is a Threat?

- A threat is the potential for a person, event, circumstance, or condition to trigger or exploit a particular vulnerability and cause harm
- Four main categories of IT threats:
  - Natural
  - Environmental
  - Human
  - Technical

## PERFORMING A RISK ASSESSMENT

### Natural Threats

- Naturally-occurring events:
  - Sun, wind, rain
  - Severe storms, lightning, hail, high winds, flash floods
  - Hurricanes, tornadoes, dust storms
  - Floods, earthquakes, avalanches, landslides
  - Wild fires, snow, ice
  - Termites, ants and other insects
  - Bird flu, anthrax, mold and other biological hazards
  - Tsunami
  - Sun spots and solar winds

## PERFORMING A RISK ASSESSMENT

### Environmental Threats

- Environmental factors that interfere with access to or proper operation of IT systems:
  - Temperature and humidity extremes
  - Power fluctuations and disruptions
  - Communication fluctuations and disruptions
  - Structural integrity failures
  - Chemical spills
  - Water leak
  - Fire
  - Excessive dust and dirt
  - Electromagnetic interference
  - Radio frequency interference

## PERFORMING A RISK ASSESSMENT

### Human Threats

- Events that are either enabled by or caused by human beings
  - Unintentional acts: data entry errors or accidentally deleted data
  - Intentional acts: network based attacks, malicious software, unauthorized access to confidential information
- Common threat sources:
  - Hackers, spies, competitors, thieves, vandals, and employees
- Common threats:
  - Viruses, worms, trojans, spyware, adware
  - Port hacks, password cracks, denial of service attacks
  - Spoofing, phishing, social engineering
  - Tampering, theft, arson, and vandalism
  - Transportation mishaps and physical access interruptions
  - Vendor failures

## PERFORMING A RISK ASSESSMENT

### Technical Threats

- Events that cause hardware and software not to function properly:
  - Operation malfunctions and failures
  - Faulty implementation
  - Failure to implement vendor upgrades and repairs
  - Incorrect configuration
  - Inadequate maintenance

## PERFORMING A RISK ASSESSMENT

### Vulnerability

- Weakness that makes it possible for a threat to create a negative outcome:
  - Flaws or inadequacies in physical and environmental controls
  - Flaws or inadequacies in the specification, design, implementation, configuration, maintenance, and protection of information system components
  - Failures or inadequacies related to the detection of threats
  - Lack of awareness regarding information security policy and practice
  - Deliberate avoidance or circumventing of existing policy and practice
  - Insufficient training and readiness to address information security vulnerabilities
  - Misplaced or inappropriate trust

## PERFORMING A RISK ASSESSMENT

		LIKELIHOOD THAT SOMETHING WILL GO WRONG				
SEVERITY OF IMPACT	CATEGORY	FREQUENT Expected to occur frequently	LIKELY Expected to occur	OCCASIONAL May occur	SELDOM Not likely to occur but possible	UNLIKELY Unlikely to occur
	<b>CATASTROPHIC</b> Total Destruction of Property, Cessation of Operations, Bankruptcy, Loss of Life, Irreparable Damage to Public Image	<b>E</b>	<b>E</b>	<b>H</b>	<b>H</b>	<b>M</b>
	<b>CRITICAL</b> Major Property Damage, Significant Disruption of Operations, Significant Financial Loss, Severe Bodily Injury, Significant Damage to Public Image	<b>E</b>	<b>H</b>	<b>H</b>	<b>M</b>	<b>L</b>
	<b>MODERATE</b> Minor Property Damage, Minor Disruption of Operations, Minor Financial Loss, Minor Bodily Injury, Significant Damage to Public Image	<b>H</b>	<b>M</b>	<b>M</b>	<b>L</b>	<b>L</b>
	<b>NEGLIGIBLE</b> Minimal Property Damage, Temporary Disruption of Operations, Limited Financial Loss, Bodily Injury Not Requiring Medical Injury, No Damage to Public Image	<b>M</b>	<b>L</b>	<b>L</b>	<b>L</b>	<b>L</b>

## PERFORMING A RISK ASSESSMENT

### Example: Remote Deposit Capture Service

- Poor computer security at customer site (computers & network)
- Poor physical security at customer site (computers & items)
- Faulty equipment (misreads, endorsement/franking errors)
- Falsified items (altered information harder to detect)
- Duplicate items (presentment, re-deposit)
- Identity theft by customer's employees
- Poor business continuity preparedness (customer and bank)
- Settlement failures (funds availability, returned items)
- Money laundering and other suspicious activity

## PERFORMING A RISK ASSESSMENT

### Example: ACH Service

- Credit Risks
  - Credit rating
  - Industry type
  - Transaction type
- Fraud Risks
  - Authentication
  - Authorization
- Operational Risks
  - Hardware and software failures
  - Environmental control failures
  - Natural disasters

## PERFORMING A RISK ASSESSMENT

### CALCULATING RISK FOR A PARTICULAR THREAT

**Vulnerability x Likelihood x Impact = Level of Risk**

PERFORMING A RISK ASSESSMENT

**CALCULATING RISK FOR A PARTICULAR THREAT**

**Vulnerability x Likelihood x Impact = Level of Risk**

**TORNADO EXAMPLE**

**Extreme = 4, High = 3, Medium = 2, Low = 1**

$$V \times L \times I = R$$

$$2 \times 2 \times 3 = 12$$

FOCUS ON  
IT SECURITY RISKS

FOCUS ON IT SECURITY RISKS

**New Technology, New Risks**

- Flash Drives, Memory Cards, and other Removable Media
- I-Pods, MP3 players, Digital Cameras
- Cell phones, PDAs, Blackberries, I-Phones
- Instant Messaging, Text Messaging, Media Messaging
- Remote Access: employees, vendors, clients
- Wireless Networks: work and home
- Voice over Internet Protocol (VoIP), Unified Messaging
- Storage Area Networks
- Electronic Data Vaulting
- Software as a Service (SaaS)
- PC Virtualization, Server Virtualization,
- Cloud Computing



FOCUS ON IT SECURITY RISKS

**New Technology, New Risks**

- Flash Drives, Memory Cards, and other Removable Media
- I-Pods, MP3 players, Digital Cameras
- Cell phones, PDAs, Blackberries, I-Phones
- Instant Messaging, Text Messaging, Media Messaging
- Remote Access: employees, vendors, clients
- Wireless Networks: work and home
- Voice over Internet Protocol (VoIP), Unified Messaging
- Storage Area Networks
- Electronic Data Vaulting
- Software as a Service (SaaS)
- PC Virtualization, Server Virtualization,
- Cloud Computing

*Where is your data?  
Who has access?  
Are you considering  
all the threats?*



## FOCUS ON IT SECURITY RISKS

### Data Breach Statistics

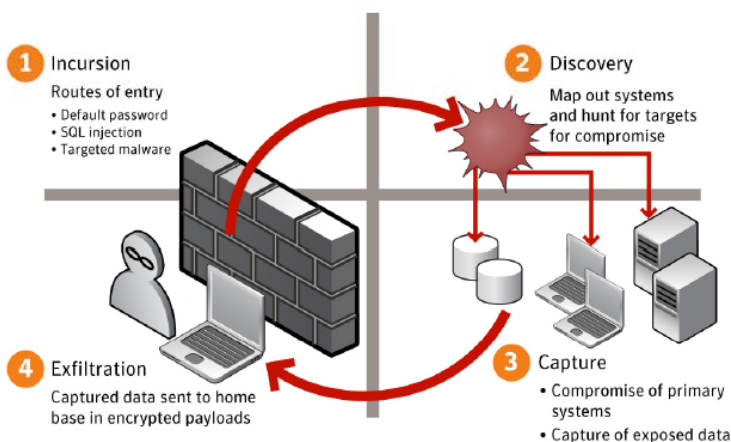
- More than 90% of records breached involved organized crime
- It can happen to any organization
  - Heartland Payment Systems – 100 million credit cards
  - TJ Max – 45 million credit cards
  - Network Solutions – 573,000 credit and debt cards
  - Lincoln National Financial Securities – 1.2 million account records
  - CITI – SSNs printed on outside envelope for 600,000 tax documents
  - Aetna – 65,000 SSNs
  - Suffolk County National Bank – log on credentials for 8,300 customers
  - Rocky Mountain Bank – 1,325 customer records
  - Downeast Energy & Building Supply – \$200,000 transferred
  - Dwelling House S&L – lost \$3 million and was sold off
  - Americaquest Mortgage – employee stole info on 100 accounts

## FOCUS ON IT SECURITY RISKS

### Automated Attacks

- Often use malicious code that penetrates defenses and exports data to hackers
- Example:
  - “Zeus” banking Trojan horse code
  - Infected over 1.6 million computers
  - Targeted 1,000 banks and their customers.
  - Captured online banking and treasury management data
  - FDIC issued a special alert regarding EFT fraud as a result
  - In 2009, Symantec observed 90,000 variants of Zeus
- In 2009, Symantec created 2,895,802 new malicious code signatures, a 71 percent increase over 2008; the 2009 figure represents 51 percent of all malicious code signatures ever created by Symantec.
- In 2009, 75% of companies surveyed experienced a cyber attack
- In 2009, 74% of phishing attacks targeted banks

## FOCUS ON IT SECURITY RISKS



Four phases of targeted attacks: incursion, discovery, capture, exfiltration

Source: Anatomy of a Data Breach, Symantec Whitepaper

**HORNE**  
BANKERS' FORUM 2010

**HORNE**  
CPAs & Business Advisors

## FOCUS ON IT SECURITY RISKS

### Corporate Account Takeover

- Company's online banking/treasury management credentials stolen
- Over \$100 million in attempted losses due to ACH/wire fraud in 2009
- Malicious software
  - Attached to email or embedded link to infected website
  - Infected CD or USB flash drive
  - Infected photo, video or document on social networking site
- Criminal then can do everything client can do, including ACH & wires
  - Log keystrokes, looking for logins for bank accounts
  - Use information to create their own login and transfer funds
- ACH transfers are initiated, typically multiple to unwitting "mules" that have been recruited through work-at-home schemes
- Businesses often did not utilize appropriate safeguards and banks did not deploy sufficient risk detection procedures

**HORNE**  
BANKERS' FORUM 2010

**HORNE**  
CPAs & Business Advisors

## FOCUS ON IT SECURITY RISKS

### Corporate Account Takeover

- High profile examples: Church (\$600,000), Construction Co. (\$532,000)
- Construction Co. sued bank saying...
  - UCC says banks must offer "commercially reasonable" security to protect online customers from fraud
  - FFIEC recommends banks use multi-factor authentication methods to check a customer's credentials
  - Bank did not offer any form of token-based authentication; its multi-factor approach only asked for the user to enter a second password
  - \$1,000 threshold that triggered challenge questions meant questions were so frequent they provided little additional security
  - Even though bank says it monitors customer online accounts for signs of unauthorized access, all of the fraudulent transfers were initiated from IP addresses that had never been used before

## FOCUS ON IT SECURITY RISKS

### Corporate Account Takeover

- Best practices for businesses
  - Up-to-date anti-virus software
  - Properly configured firewall
  - Intrusion detection and prevention software
  - Educate employees about risks of unknown emails, web sites, and storage devices
  - Utilize dual control for ACH and wire transactions
  - Restrict functions for PC used for ACH and wire initiation
    - Strict physical security
    - No removable media, no email, no other internet use
  - Perform daily reconciliation of bank account(s)
  - Provide prompt notification to bank about suspicious activity

## FOCUS ON IT SECURITY RISKS

### Corporate Account Takeover

- Best practices for banks
  - ACH /treasury management agreements that stipulate business's responsibilities; security tips sheet
  - Multifactor authentication using something you know and something you have
  - Utilize out-of-band alerts and out-of-band authentication
  - Offer optional services
    - ACH debit block (pay no ACH debits)
    - ACH debit filter (pay only pre-authorized ACH debits)
    - ACH transaction review (review and pay authorized debits)
  - Utilize FedACH Risk Origination Monitoring Service
  - Monitor for duplicate, unusual and high volume transactions



**HORNE**  
BANKERS' FORUM 2010

**HORNE**  
CPAs & Business Advisors

## FOCUS ON IT SECURITY RISKS

### Corporate Account Takeover

#### *IronKey Trusted Access*



IRONKEY THE KEY TO PORTABLE SECURITY SOLUTIONS | PRODUCTS | TESTIMONIALS

PROTECT COMMERCIAL BANKING CLIENTS

**IronKey Trusted Access for Banking**

Criminals today are targeting commercial online banking users to steal millions of dollars. IronKey Trusted Access for Banking allows commercial banks to protect their users and transactions. Trusted Access for Banking allows clients to use their existing online accounts and money transfer systems within the confines of a locked-down, portable virtual environment.

With Trusted Access for Banking, users simply connect their IronKey portable USB security device to automatically launch a protected, virtualized environment. The Trusted Access Browser opens all the bank's authorized online pages and users can only navigate to bank authorized sites.

To protect users from ever-changing malware, Trusted Access for Banking does not rely on potentially compromised and vulnerable applications on the user's host computer. A secure, encrypted connection to online banking is made through the IronKey Trusted Network to lock out man-in-the-middle and DNS attacks. Advanced encrypted keyboard input protects users from keyloggers while entering authentication credentials and other sensitive data.

Institutions manage policies and devices using the IronKey Enterprise Management Service. Banks can quickly deploy Trusted Access for Banking without the need for server hardware, software, or time spent updating banking applications. For customer service and fraud management teams, the Enterprise Management Service allows banks to track and audit device activation, usage, and policy updates.

**Benefits**

- Protect commercial online banking
- Meet NACHA and FBI safe banking guidelines
- Deliver rapid time to market
- Manage policy and updates remotely
- Reduce demands on customer service and fraud teams

[REQUEST EVALUATION](#)  
[DATASHEET](#)

**HORNE**  
BANKERS' FORUM 2010

**HORNE**  
CPAs & Business Advisors

## FOCUS ON IT SECURITY RISKS

### Malicious Insiders and Corporate Espionage

- A former New York state tax department worker
  - Gathered credit card, brokerage account and Social Security numbers
  - Opened more than 90 credit card accounts and lines of credit.
  - Investigators searched the employee's home and found
    - 700 state tax forms containing taxpayer information
    - 300 birth certificates
    - 1,000 Social Security cards, credit card statements and applications
    - Handwritten notes such as "good prospect," "had money" and "go with this one"

## FOCUS ON IT SECURITY RISKS

### Well-Meaning Insiders

- 67% of breaches were aided by significant errors of insiders (Verizon report)
- Of 43 organizations suffering data breaches, 88% involved negligence (Ponemon study)
- Common occurrences
  - Confidential data stored, sent, copied unencrypted
  - Lost or stolen laptops and PDAs
  - Email, web mail, IM
  - Portable storage (tapes, CDs, DVDs, memory sticks)
  - Third-party vendor data loss
  - Out-of-date business practices

## FOCUS ON IT SECURITY RISKS

### **Terminated and Departing Employees**

- Employee often notified prior to network and application access rights being terminated, or employee plans to quit
- 2009 Ponemon study on employee terminations revealed that 59% of ex-employees took company data, including customer lists and employee records
- Employees store company data on home PCs to build up a library of work for future career opportunities

## BUILDING A SUCCESSFUL IT SECURITY RISK MANAGEMENT PROGRAM

## IT SECURITY RISK MANAGEMENT PROGRAM

### A comprehensive written program

- Ensures the confidentiality, availability and integrity of confidential and critical information
- Includes administrative, technical, and physical safeguards
- Appropriate to the size and complexity of the organization
- Appropriate to the nature and scope of its activities

## IT SECURITY RISK MANAGEMENT PROGRAM

### Assess Risk

- Inventory information that must be protected
- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of confidential and critical information
- Assess the sufficiency of policies, procedures, information systems, and other arrangements in place to control risks

## IT SECURITY RISK MANAGEMENT PROGRAM

**Manage and Control Risk**

- Control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the organization's activities
- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing information to unauthorized individuals
- Access restrictions at physical locations containing confidential and critical information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals

## IT SECURITY RISK MANAGEMENT PROGRAM

**Manage and Control Risk**

- Encryption of electronic information, including while in transit or in storage on networks or systems
  - Portable storage media (CDs, DVDs, tapes, thumb drives)
  - Portable devices (laptops, minis, PDAs, I-Phones, I-Pods, cameras)
  - Desktop PCs, servers, NAS, SAN, midranges, mainframes
  - Communication (email, SMS, MMS, IM, VOIP)
  - Techniques
    - Full disk encryption
    - Virtual disk and volume encryption
    - File and folder encryption
    - Message encryption
    - Network encryption
  - NIST Special Publication 800-111 (rest), FIPS 140-2 (motion)

## IT SECURITY RISK MANAGEMENT PROGRAM

**Manage and Control Risk**

- Procedures designed to ensure that system modifications maintain security controls
- Dual control procedures, segregation of duties, and background checks for employees with responsibilities for, or access to, customer information
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems (IPS, IDS, DLP, logging)
  - Example vendors: Cisco, Checkpoint, Trend Micro, Symantec, McAfee, Tripwire, Vericept, Code Green, Proofpoint, LogRhythm, CornerBowl, GFI, Qualys, SecurityMetrics, SecureWorks, Trustwave

## IT SECURITY RISK MANAGEMENT PROGRAM

**Manage and Control Risk**

- Implement measures to protect against destruction, loss, or damage of information due to potential environmental hazards
- Service provider oversight (required by GLBA)
  - Exercise appropriate due diligence in selection process
  - Require service providers by contract to implement appropriate security measures
  - Monitor service providers to confirm that they have satisfied their obligations as required
  - Review audits, summaries of test results, or other equivalent evaluations of its service providers

## IT SECURITY RISK MANAGEMENT PROGRAM

**Manage and Control Risk**

- Implement response programs that specify actions to be taken when an employee suspects or detects that unauthorized individuals have gained access to customer information systems
  - Determine what happened (no breach, no response)
  - Contain and control the situation (close the barn door)
  - Protect the evidence (use forensic methods)
  - Determine which customers are affected
  - Determine how customers may be affected
  - Notify regulatory and law enforcement agencies
  - Provide customer notice and assistance
  - Delay notice for law enforcement investigation

## IT SECURITY RISK MANAGEMENT PROGRAM

**Manage and Control Risk**

- Regularly test/audit the key controls, systems, and procedures with the frequency/nature of tests/audits determined by risk assessment and conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs

## IT SECURITY RISK MANAGEMENT PROGRAM

### Report to Management

- Describe the overall status of the IT security risk management program and the financial institution's compliance with the program
- Discuss material matters such as:
  - risk assessment
  - risk management and control decisions
  - service provider arrangements
  - results of testing
  - security breaches or violations and management's responses
  - recommendations for changes

## IT SECURITY RISK MANAGEMENT PROGRAM

### Adjust the Program

- Monitor, evaluate, and adjust, as appropriate, the information security risk management program in light of:
  - Relevant changes in technology
  - The sensitivity of customer information
  - Internal or external threats to information
  - Changing business arrangements
    - Mergers and acquisitions
    - Alliances and joint ventures
    - Outsourcing arrangements
    - Changes to customer information systems

QUESTIONS?


**HORNE**  
BANKERS' FORUM 2010

 **HORNE**  
CPAs & Business Advisors

**HORNE**  
BANKERS' FORUM 2010

**A Practical Approach to  
Assessing and Managing  
IT Risks**

Tony Brooks, CISA  
HORNE LLP Principal  
1020 Highland Colony Parkway  
Suite 400  
Ridgeland, MS 39157  
tony.brooks@home-llp.com  
601.326.1281

 **HORNE**  
CPAs & Business Advisors

Contact Information

**Tony Brooks, CISA**  
**HORNE LLP Principal**  
**1020 Highland Colony Parkway**  
**Suite 400**  
**Ridgeland, MS 39157**  
**tony.brooks@horne-llp.com**  
**601.326.1281**

HORNE LLP is one of the top 50 accounting and business advisory firms in the country, as reported by the Public Accounting Report (PAR), and one of the top 10 accounting and business advisory firms in the Southeast. With 13 offices in Mississippi, Tennessee, Alabama, Louisiana, Texas and Arizona, the firm serves clients across the nation. For more information on HORNE, visit [www.horne-llp.com](http://www.horne-llp.com).

©HORNE LLP 2010

