THE POOL
Tennessee's Leader in Risk Management Services

Cyber Risks & Internal Controls

"Preparing Your Organization for Current and Emerging Risks"

Cyber Risks & Financial Internal Controls

- Key Points:
  - Traditionally, little-to-no IT and Financial Risk management efforts
    - Areas often were deemed too "Technical" and off limits (we leave it to the experts approach)
  - Required: Enterprise Risk Management (ERM) approach: looks at all risks
  - Don't need to be an operational specialist to understand risk!
  - IT and Finance should be reviewed like any other operational department!

Cyber Risks & Financial Internal Controls

Cyber Risks, discuss:

- Some legal exposures related to compromised stored sensitive information and lax computer security safeguards
- Some of the commonly identified threats (**which are already outdated**)
- A cyber threat identification and mitigation framework to minimize loss exposures

Financial Controls, discuss:

- Issues leading to the current (core) recommendations
- Common exposures related to lax (or no) internal controls
- Core internal controls

THE POOL
Tennessee's Leader in Risk Management Services

Cyber Risks

Case Study

- ***Finance officer receives email from Better Business Bureau with an attachment.***
- ***Finance officer clicks on the attachment, computer flickers, and nothing happens***
- ***Finance officer has some on-line banking to complete and proceeds to do her work***
- ***Later, the finance officer checks the entity's bank account and notices 3 unauthorized withdrawals in the amount of $60,000.***

Case Study

- ***Finance officer calls the bank, and the bank freezes the account.***
- ***The bank traces these withdrawals, 2 of which were transferred to other accounts in another state before moving to an overseas account.***
- ***The third withdrawal, was reported by a bank in New York, and that money was recovered before going overseas.***

Case Study

- ***FBI investigates and determines:***
  - *BBB email was bogus*
  - *The attachment contained key logger malware*
  - *Once clicked, the key logger malware was downloaded to the finance officers computer*
  - *All keystrokes were recorded and sent to author of the malware*
  - *Malware place of origin was traced to the Russian Mafia in Eastern Europe*

Why Be Concerned?

Objections Heard:

- A full time computer department;
- A computer security suite on all computers;
- A small organization, and nobody wants anything you have…

Not So Fast!

What Do Cyber Criminals & Hackers Want?

- **Digitally store sensitive information**
  - •Medical Records (State of Virginia Theft)
  - •Credit Card Numbers (Theft & Fraud)
  - •On-line banking log in and password info (Theft & Fraud)
  - •Societal Disruptions chaos (electrical grid, financial institutions, etc.)
  - •Computer Political Activism (Hactivism)
  - •Etc.

THE POOL

Top Targets:
Local Government & Small Businesses

Verizon Security Research:

- Cyber criminals are risk managers
  - Mass producing attack techniques geared towards local governments and small businesses.
  - Why?
    - Big business has invested in cyber security and many have partnered with Federal Law Enforcement – More work and more risk!
    - Local government and Small business have not invested, some have not accepted their vulnerabilities – less work and risk – *path of least resistance!*

THE POOL

Some still may ask:

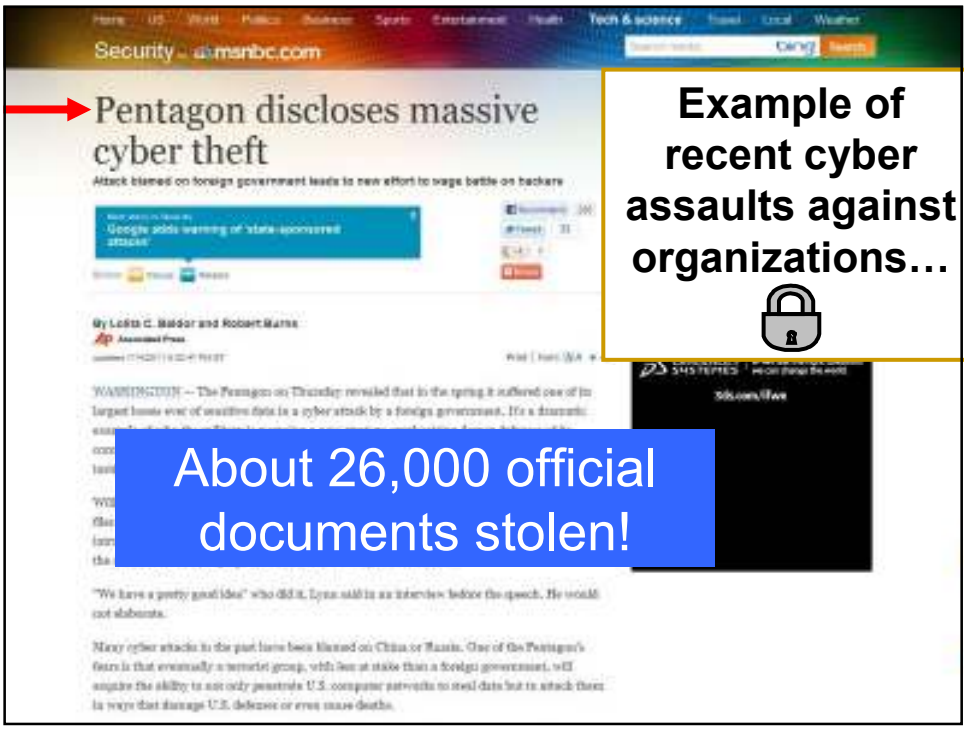
Why be concerned?

Isn't this just another Y2K Scare?

THE POOL


InformationWeek Government
Cyber Attacks Becoming Top Terror Threat, FBI Says
Get InformationWeek Daily
FEATURED WEBCASTS
More Government Insights
Webcasts
Slideshow: Inside DHS' Classified Cyber-Coordination Headquarters
THIS WEEK'S ISSUE


TECHNOLOG
msnbc.com TECH
Example of recent cyber assaults against organizations…
LinkedIn works with FBI on password theft
CHECK OUT THIS WEEK'S HOTTEST DEALS



Malware (malicious software)

Attack Method Examples (generic definitions):

- *Virus* – most common and prevalent – replicates itself within a computer system;
- *Trojan Horse* – a program that looks like its useful, but then turns malicious; (Warning your computer has been infected!)
- *Logic Bombs* – often installed and lies dormant until released by a certain trigger, such as a specific date;
- *Worms* – a self contained program(s) that can spread copies of itself or smaller segments along a network
- *Adware & Spyware* – marketing and tracking
- *Rootkits* – a backdoor program via a trusted app that allows remote access
- *Etc…*

THE POOL

Cyber Security and Sensitive Information

T.C.A. 47-18-2107 & 47-18-2901

Among other things, these two laws:

- Place certain notification requirements on organization where sensitive data has been compromised; and
- Require security of all laptops and portable storage devices that contain sensitive information.

Cyber Security and Sensitive Information

Internal Control and Compliance Manual for Tennessee Municipalities states:

1. *Municipal officials should ensure that controls are in place to ensure that only authorized people have access to electronic data and municipal computers (this would include passwords, access limitations, procedures to revoke authorization when employment is terminated, etc.).*
2. *Regular backups are made of data;*
3. *Disaster recovery plans are in place*

Cyber Security and Sensitive Information

Health Insurance Portability and Privacy Act (HIPPA) of 1996 provides federal privacy protections for personal health information held by covered entities, regardless of its format (print or digital);

Fair and Accurate Credit Transactions Act (FACTA) of 2003, which contains provisions designed to help reduce identity theft.

Family Educational Rights and Privacy Act (FERPA), which requires schools receiving funds from the U.S. Department of Education to protect certain private records of students.

THE POOL

Cyber Security and Sensitive Information

- **Definition**. A policy should be established defining sensitive information that is subject to protective measures.
- **Location**. Once a definition is established, each entity should then identify the sensitive information it collects, how it is collected (print or digital), and its location (department) within the entity.
- **Protection**. Once this stored sensitive information has been located, each public entity should implement administrative, physical, and digital safeguards to protect this information.
- **Disposal**. If the stored sensitive information is no longer needed, and eligible for disposal as outlined in your documents retention policy, then appropriate disposal methods should be employed.
- **Preparation**. Each entity should have a written response plan to address lost, stolen, or otherwise compromised sensitive information stored by the entity.

THE POOL

Computer Security

Most exposure are from:

1) Negligent Entities
   - Failure to recognize & plan
2) Negligent Employees
   - IT shortsightedness
   - Little or no training
3) Rogue Employees
   - Selection
   - Supervision

THE POOL

Computer Security

Most exposure are from:

4) Malware
   - Training
   - Computer safeguards
5) No Comprehensive Computer Security Plan

Computer Security Plan

Most organizations make the mistake of thinking that just having an IT department and a security suite is all you need. The three most important elements are:

1. Management/Administrative Controls -Policy
2. Operational Controls - Practices
3. Technical Controls – Hardware/software/security updates & safeguards

Each must have a place in your overall plan!
"Don't focus on Technical Controls alone"

Computer Security Risk Management Plan

- Identify Computer Exposures
- Develop Policy
- Train Employees
- Supervise & monitor
- ***Have a response plan***

The written checklist contains general recommendations that every organization with exposures should review and consider as a part of a larger comprehensive plan.

Computer Security Plan

Key planning areas:

1. Cross-department assessment & planning team
   - What's at risk and what is our prevention plan?
2. Employee Training
   - Hazard Recognition
   - Cyber Threat Updates
3. Encryption of Sensitive Information
4. Banking Institution Consultation
   - Token System
5. Public WI – FI & Unsecured Networks
   - Hacking Tools - Wireshark, Cain & Able, ARP, YouTube
6. Hardware/Software Firewall & Security Suite

POOL

Firewall Examples

Hardware Firewall →

Software Firewall →

POOL

Computer Security Plan

Key planning areas:

6. Portable Storage Devices*
7. Non – Disclosure Agreements
8. Backup and Recovery
   - Backup of Sensitive Data
   - Secondary Off-site Storage
9. Incident Response Plan
10. Insurance Coverage

Coverage Issues?

At a minimum:

- **Privacy Liability and Network Liability**
  - Covers liability arising from the failure to properly handle, manage, store, destroy, or otherwise control information, an unintentional violation of your privacy policy that results in the violation of any privacy regulation, or a failure of network security.
- **Data Breach Coverage**
  - Covers expenses that result from an information breach including computer forensics service, notification of affected parties, credit monitoring services, and expenses associated with coming into compliance with privacy regulations.
- **Property & Crime**
  - Cyber theft of funds

Computer Security Plan Bonus Content

Additional Technical Areas:

- Switches
- Load Balancers
- Proxy Severs
- Web Security Gateways
- URL Filtering
- Intrusion Detection Systems
- Mobile Device Security
- Etc…

Many of these items depend on the size of your organization and the assets at risk.

THE POOL

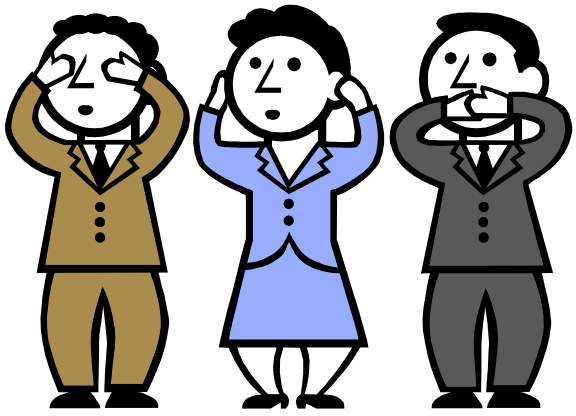
THE POOL
Tennessee's Leader in Risk Management Services

Financial Internal Controls

Financial Controls & State Laws

- Local Government Instances of Fraud Reporting Act of 2007
- The Municipal Finance Officer Certification and Education Act of 2007

How Did We Get Here?



A little closer to home….

Examples of losses:

- $5,702 – **Human resources agency clerk**: misappropriated funds, lax internal controls, criminal charges filed
- $11,920 – **City court clerk**: misappropriated funds, lax internal controls, criminal charges filed
- $28,998 – **Police chief**: misappropriated funds, stolen weapons and other city property, lax internal controls, criminal charges filed
- $70,000 – **City Recorder**: Misappropriated funds, fraudulent use of city credit card, lax internal controls, criminal charges filed
- $73,000 – **Police Chief & Court Clerk**: public funds lost, but were later located (no criminal activity) - lax controls, no criminal charges filed

Internal Controls

In an effort to prevent the loss of cash or other assets:

The Tennessee State Comptroller recommends that cities complete a

Risk Assessment

of their financial internal control structure.

(Title 3, Chapter 1 of the Internal Control and Compliance Manual for Tennessee Municipalities)

The Comptroller recommends numerous internal controls to prevent or minimize losses.

Common Exposure Areas

- No written policies and procedures for internal controls
- No or lax training on policies and procedures related to internal controls
- No segregation of duties
- No or lax verification of receivables (paper-trail)
- No or lax verification when cash changes hands
- Other departments handling public funds are often excluded – **BIG EXPOSURE!**

Common Steps to Minimize Financial Risk

1. Written internal control policies and procedures
2. Integration of internal checks and balances
   - Appropriate documentation
   - Verification – invoices, expenditures, etc.
   - Segregation of duties
3. Documented training on these policies
4. Periodic supervisory audit and appropriate oversight
5. Small cities – Elected Officials must play a role in the process

Internal Controls

- *Collections deposited intact & in < 3 days*
- *Safety measures for routine bank deposits*
- *Adequate checks & balances for petty cash*
- *Check writer differs from a person who balances checking account*
- *Counter signature on all checks*

Internal Controls

- *Incoming checks stamped "for deposit only"*
- *Person opens mail and stamps checks different from the person who posts to ledger & makes deposits*
- *Person who verifies & submits timesheets differs from person who prepares payroll*
- *CC/DC authorized users & approved purchases outlined in policy*
- *All collections receipted in duplicate* ***(P&R concessions, Community Centers & Pools, Police, Clerks)***

Internal Controls

- *Written policies/procedures and training on internal controls*
- *CMFO/ CMFO equivalent*
- *Annual Inventory of Capital Assets and other equipment by physical count. ICCM – 5:24(1 & 2)*
- *Accepted Independent Audit conducted annually*

THE POOL

Tennessee's Leader in Risk Management Services

Questions?

For copies of our Cyber risk and information Security Guidelines:

gdalton@thepool-tn.org

THE POOL