

# THE FACTS ON FRAUD AND EMBEZZLEMENT

Philanthropy New York  
A Regional Association of Grantmakers  
with Global Impact

October 1, 2015

Presented by

Kevin P. Foley, CPA

Matthew P. O'Dell, CPA

Scott Perry

**CONDON  
O'MEARA  
MCGINTY &  
DONNELLY LLP**

Certified Public Accountants

# Impact of Fraud on an Organization

- Embarrassing to Board, Staff (auditors)
- Short and long-term effects on reputation
- Morale
- Cost of investigation and litigation
- Damaging to fund raising efforts
- Could affect relationship with other funding sources



# Try Your Luck

■ How much is lost to fraud world wide?

- A) \$10,000,000
- B) \$1 Billion
- C) \$450 Billion
- D) \$ 3.7 Trillion



# Try Your Luck

**D)\$3.7 Trillion Dollars!**

**\*5% of Gross World Product is lost to fraud**

**\*Source of all statistics referred to in this seminar are from the Association of Certified Fraud Examiners report.**

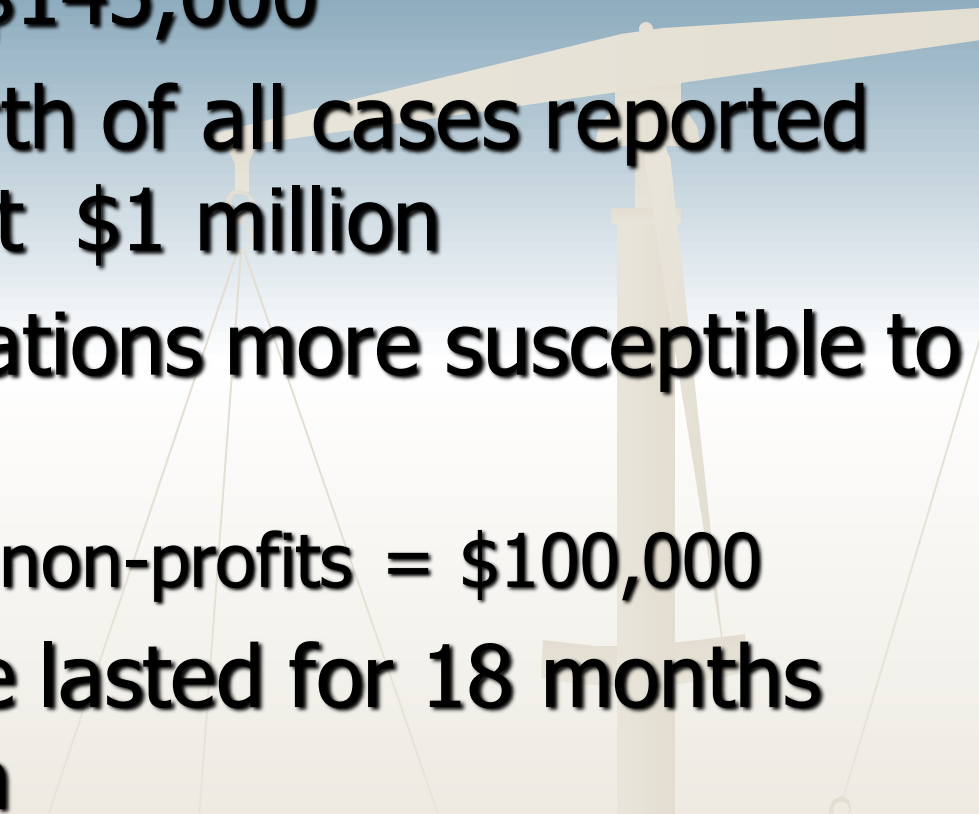


**BEWARE**

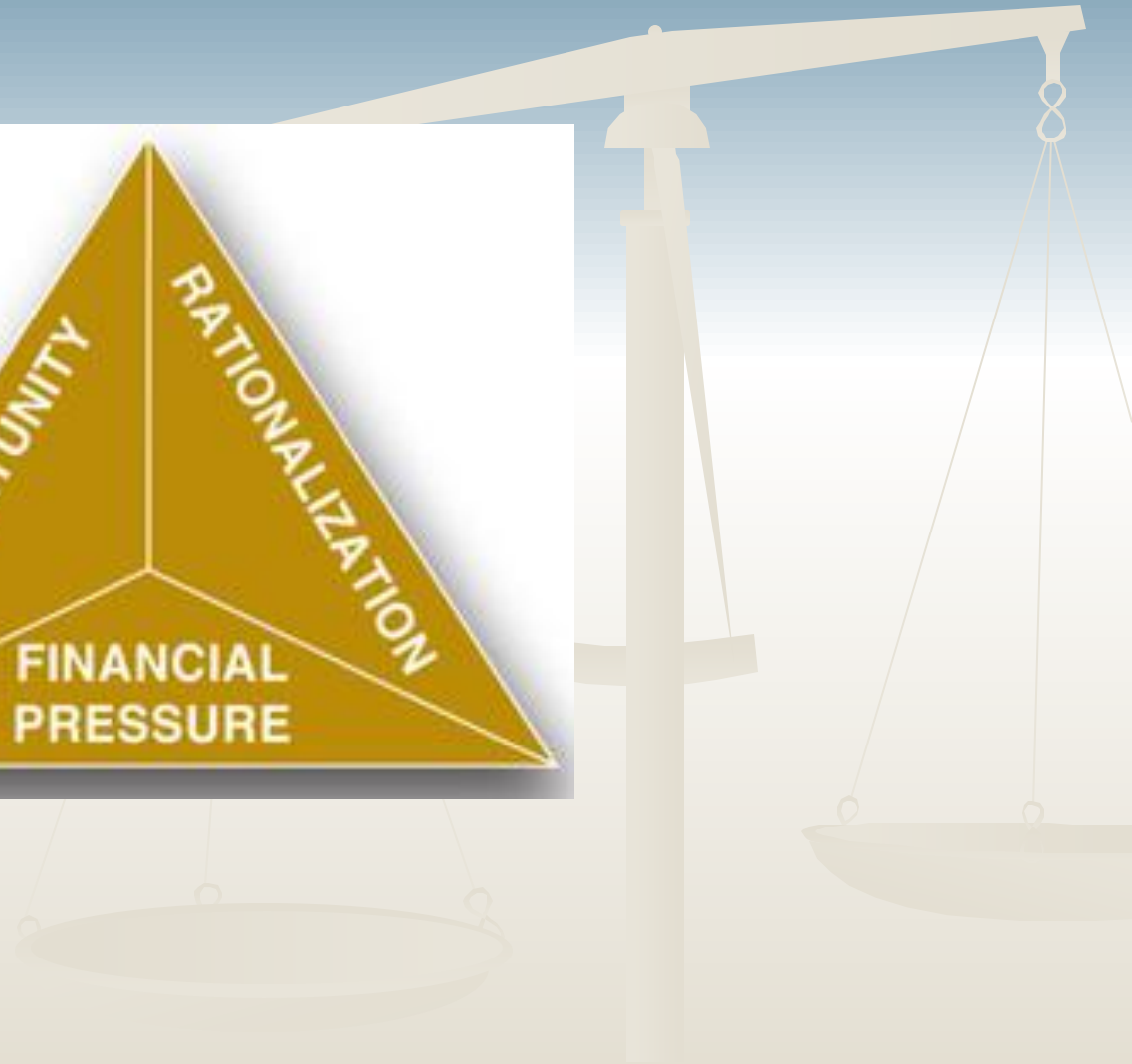
**OF THE CUTE DUCKLING SCAM**



# Fraud Facts

- Median Loss = \$145,000
  - Almost one-fourth of all cases reported losses of at least \$1 million
  - Smaller organizations more susceptible to fraud
    - Median loss for non-profits = \$100,000
  - Average scheme lasted for 18 months before detection
- 

# FRAUD TRIANGLE





# WHO STEALS?

- 67% are male
- More than half are between the ages of 31-45
- Trusted longtime employees
  - 52.5% of employees with greater than 5 yrs with organization
- Living beyond their means
- Financial problems
- Control freaks!
- Frequently defensive
- Refuses to take vacation
- Substance abuse or family problems







# WARNING SIGNS



- **Sloppy records**
  - Small but unusual problems start to occur
- **Work not timely or at all**
  - Reconciliations
  - Financial statements
  - Audit preparation
- **Missing or Incomplete bank statements**
- **Unauthorized debits on bank statements**
- **Numerous journal entries**



# Initial Detection of Frauds



- 42% of fraud found through tips
- 49% of tips are from employees
  - IRS asks about whistleblower policies
  - Auditing standards adapted to include interviews with employees
  - Organizations with whistleblower hotlines 18% more likely to receive a tip

# Initial Detection of Frauds



## ■ Other methods

- Reconciliations
- Financial statement variances
  - Budget versus actual and historical comparisons
- Management review of transactions
- Internal audits (be creative)
  - Not only for large organizations
  - Periodic/Surprise
  - Get board or committees involved





# Sensitive Areas for Fraud & EMBEZZLEMENT

- **Cash, cash & cash**
- Petty cash
- Check signing
- Wire/bank transfers
- Write-offs and adjustments to accounts receivable accounts
- Journal entries



# Sensitive Areas for Fraud & EMBEZZLEMENT

- Payroll
  - Fictitious employees
  - Credits
- Fictitious vendors
- Reward programs (Kickbacks)
- Personal expenses
  - Credit cards
  - Expense reimbursements
- Theft of inventory and/or equipment



# Governance Policies to Detect & Protect From Fraud

- Tone at the Top/Zero Tolerance
- Establish an audit committee or equivalent
  - Formalized charter outlining responsibilities regarding fraud
- Establish and Document Accounting & Internal Control Procedures
- Formalize Code of Ethics Statement
- Establish Policies
  - Whistleblower Protection Policy
  - Records retention
  - Conflict of interest





# Case Studies



■ **Reason for Defalcation**

**Opportunity**

■ **Amount**

**\$900,000**

■ **Means/Method of Fraud**

**Credit Cards & Wire Transfers**

■ **How was fraud determined**

**Email from Bank**

■ **Criminal Sentence**

**2.5 – 6 years**

■ **Employee Dishonesty**

**\$1,000,000**

# Case Studies



- **Reason for Defalcation**

**Other Debt**

- **Amount**

**\$2,500,000**

- **Means/Method of Fraud**

**Wire Transfers**

- **How was fraud determined**

**Bank Statement Review**

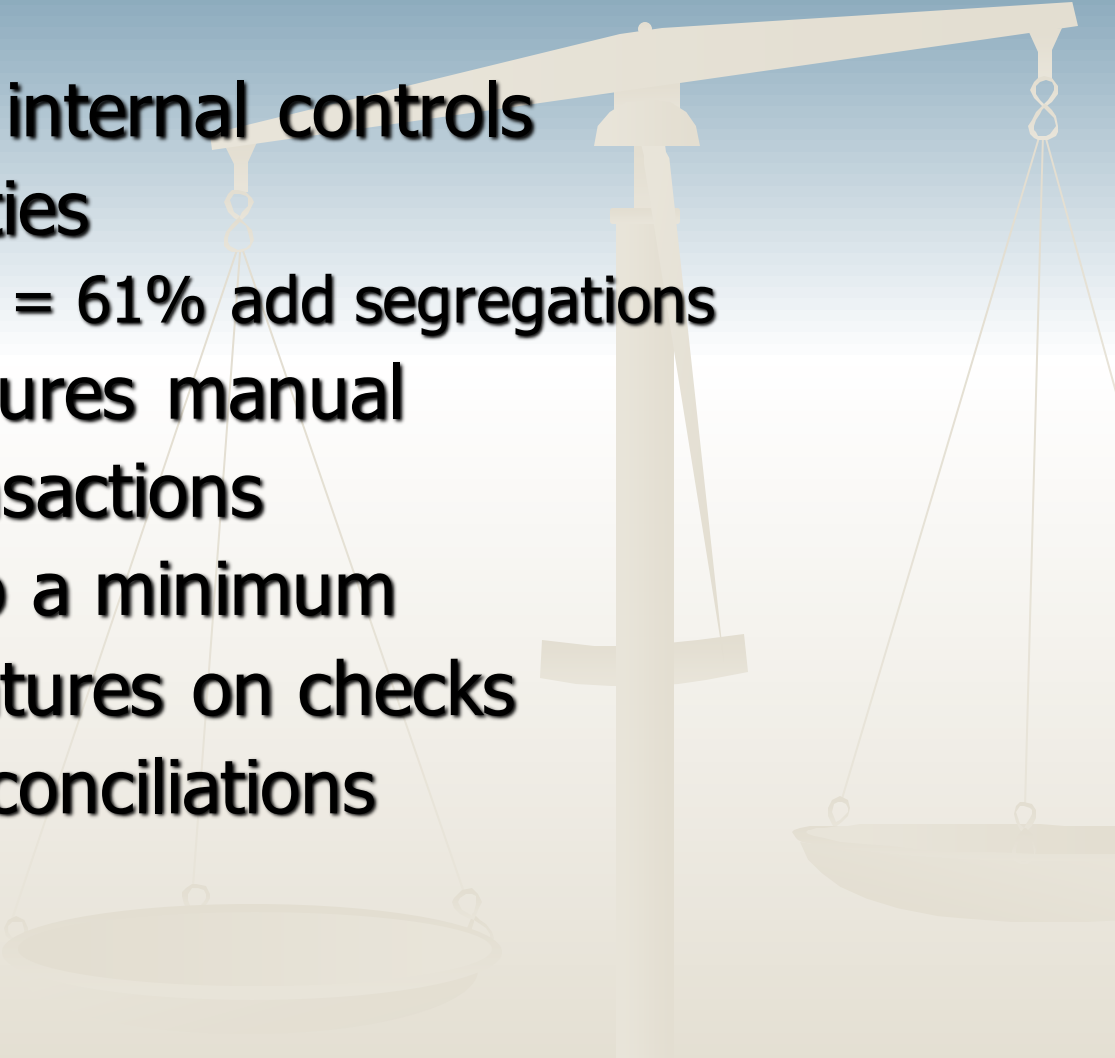
- **Criminal Sentence**

**3.5 – 9 years**

- **Employee Dishonesty**

**\$25,000**

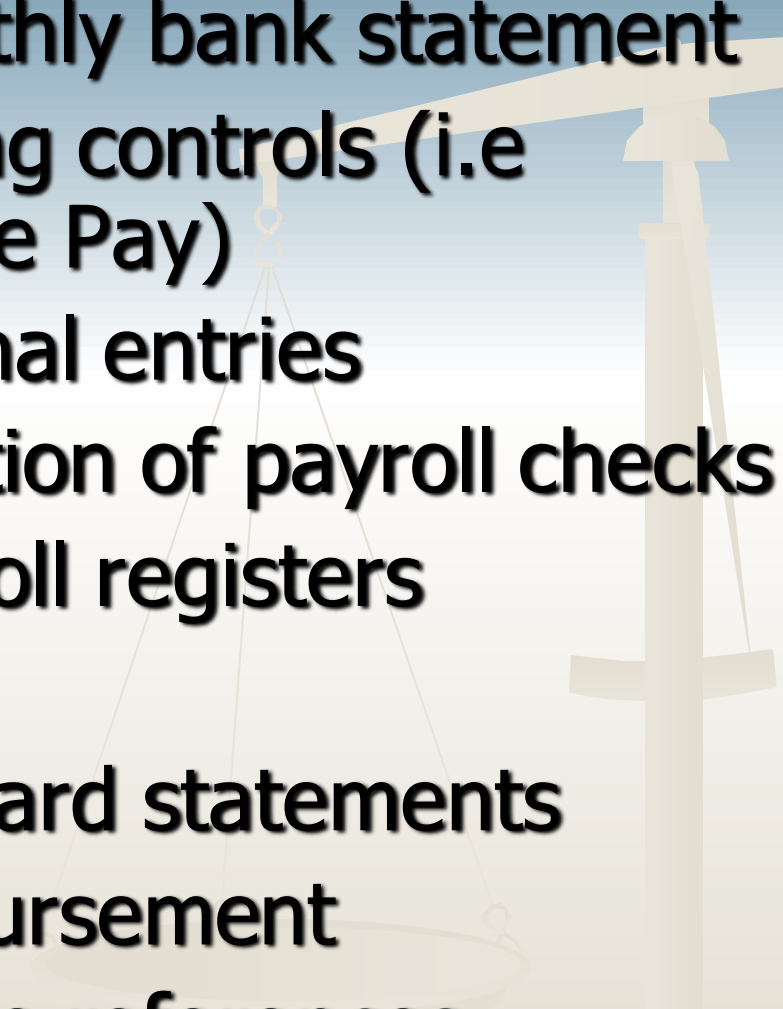
# HOW TO PREVENT FRAUD & EMBEZZLEMENT

- Enforce system of internal controls
  - Segregation of duties
    - Response to fraud = 61% add segregations
  - Accounting procedures manual
  - Minimize cash transactions
  - Keep petty cash to a minimum
  - Require dual signatures on checks
  - Review of bank reconciliations
- 

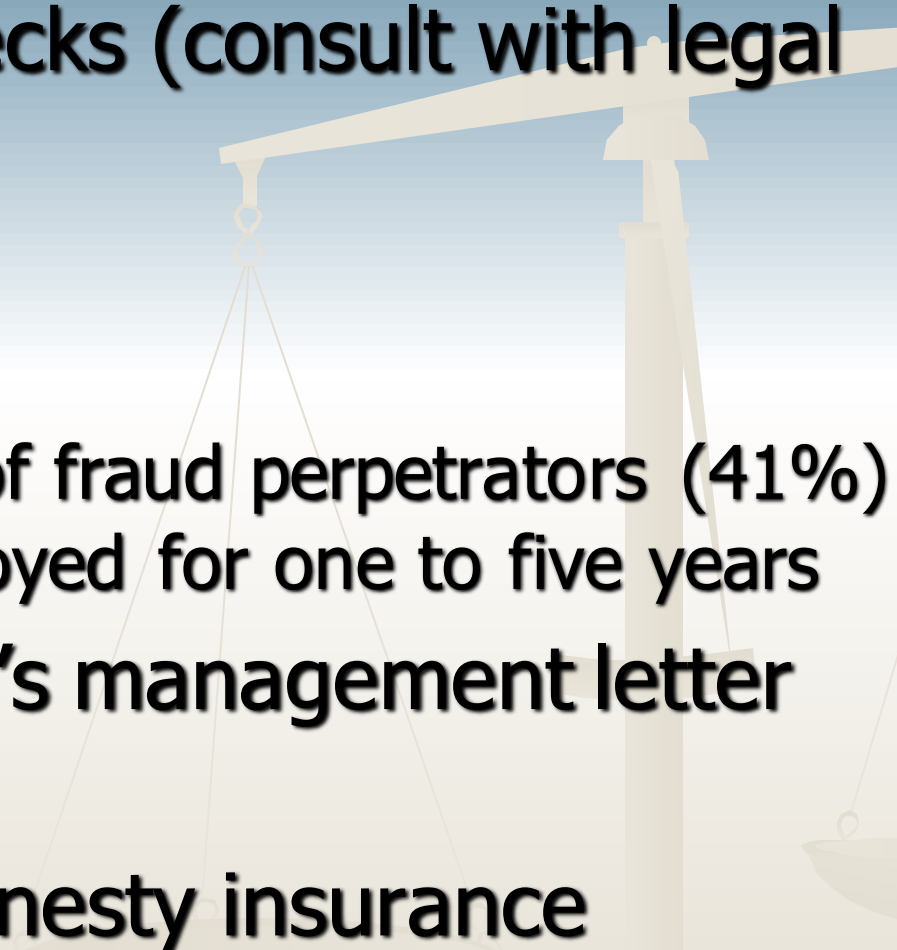




# HOW TO PREVENT FRAUD & EMBEZZLEMENT

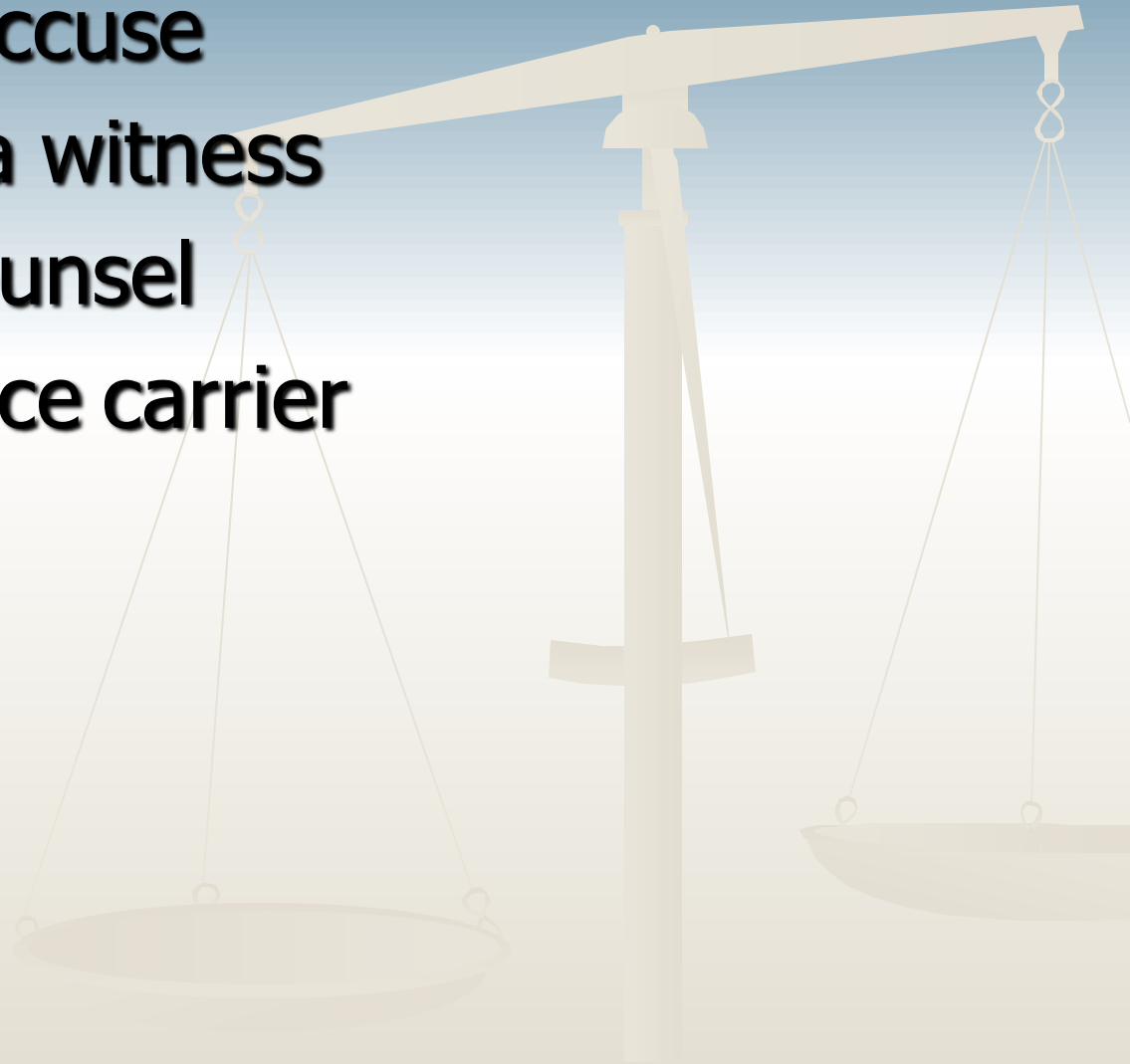
- Review of monthly bank statement
  - External banking controls (i.e Tokens/Positive Pay)
  - Review of journal entries
  - Rotate distribution of payroll checks
  - Review of payroll registers
  - Payroll payoff
  - Review credit card statements
  - Expense reimbursement
  - Check employee references
- 

# HOW TO PREVENT FRAUD & EMBEZZLEMENT

- Background checks (consult with legal council)
    - Financial
    - Criminal
    - Largest group of fraud perpetrators (41%) had been employed for one to five years
  - Address auditor's management letter comments
  - Employee dishonesty insurance
- 

# REPORTING ILLEGAL ACTS

- Do not falsely accuse
- Interview with a witness
- Consult legal counsel
- Contact insurance carrier





# REPORTING ILLEGAL ACTS

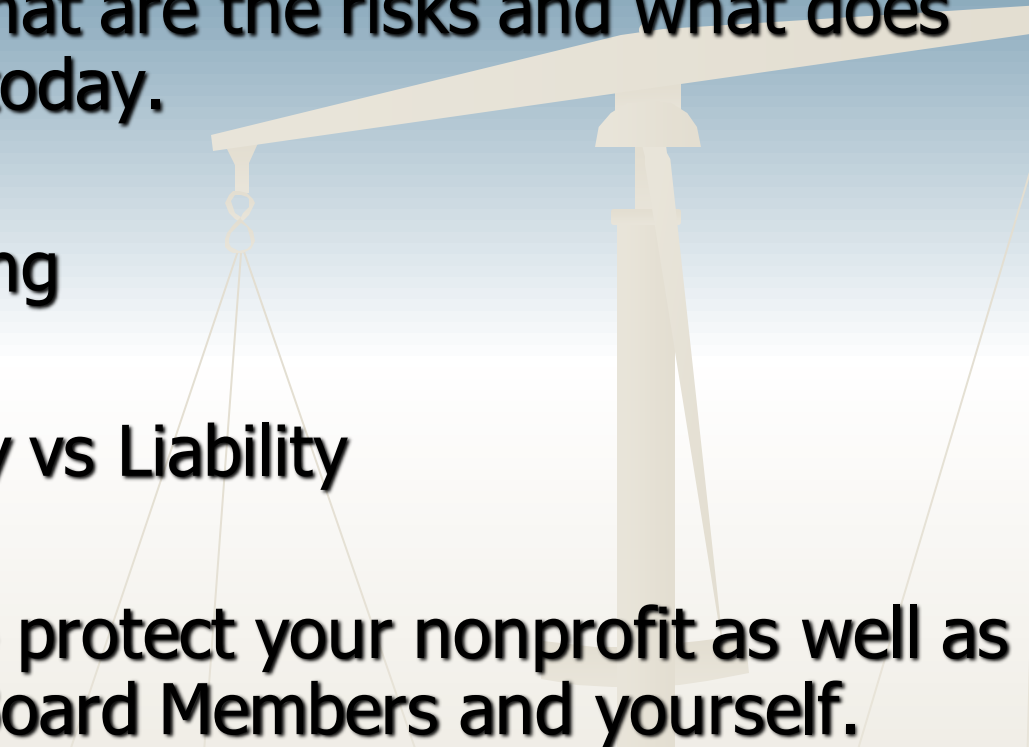


- **Form 990 Return of Organization Exempt From Income Tax Part VI Section A**
  - **Question 5 - Did the Organization become aware during the year of a significant diversion of the organization's assets?**
- ❖ **Details of this event will be disclosed on Schedule O of the Form 990.**

# Cyber Threats and What you can do about it



# Areas to Cover

- **Cyber Security – What are the risks and what does the world look like today.**
  - **Farming and Phishing**
  - **Social Responsibility vs Liability**
  - **What you can do to protect your nonprofit as well as your donors, your Board Members and yourself.**
- 

# The Cyber Threat – Landscape for 2015

Michael's®

Where Creativity Happens™

Anthem®

P.F. CHANG'S  
CHINA BISTRO®



Neiman Marcus



SONY

SALLY  
BEAUTY  
SALLY  
BEAUTY SUPPLY

STAPLES®

CHS Community  
Health Systems

JPMorganChase



# The Cyber Threat – Landscape for 2015



**Reported in the New York Times and CNN –  
May 27, 2015**

- On Tuesday, the Internal Revenue Service announced that organized crime syndicates used personal data obtained elsewhere to access tax information, which they then used to file \$50 million in fraudulent tax refunds.
- The news that the IRS data breach is believed to have originated in Russia comes on the heels of the disclosure that Russian hackers had infiltrated both the White House and State Department computer systems.
- The security of taxpayer data has been an IRS problem for years. In an October report, the IRS' independent watchdog called it the agency's number one problem. Going so far as to say "Computer security has been problematic for the IRS since 1997".
- With the I.R.S., it was not the agency's own system that was hacked. Criminals had already obtained individuals' Social Security numbers, addresses and birth dates and then used the information to trick the network and gain access to taxpayers' returns and filings through an application on the I.R.S. website.
- Between February and May, criminals tried to access the tax accounts of 200,000 people, succeeding in about half the attempts, the IRS said. The agency said it plans to notify all 200,000 people to tell them that third parties appear to have access to their Social Security numbers and other personal information.



## ORIGINS

Country

United States

France

Germany

Italy

Netherlands

Spain

Hong Kong

India

Australia

## ATTACK TARGETS

#



Country

5840 United States

220 Thailand

215 Hong Kong

156 Canada

150 Portugal

139 Australia

104 Singapore

92 Netherlands

91 United Kingdom

88 Austria

## ATTACK TYPE

#

Service

796 sip

689 ssh

558 ms-sql-s

541 http-alt

413 microsoft-ds

364 domain



# What our government is doing about it.

- **President Obama declares cyberattacks a National Emergency.** April 1, 2015
  - Sanctions against the nations behind the attacks
  - The president's order will give the Treasury Department the authority to impose sanctions on individuals or entities behind cyberattacks and cyber espionage. In effect, it would freeze targets' assets when they pass through the U.S. financial system and prohibit them from transacting with American companies.



# Farming and Phishing

- Social Media – Cyber Criminals will build a dossier on their target's employees
- Degrees of separation
- Cyber Criminals will look down stream from their target to their vendors, partners and customers. Anywhere there is a connection.
- Bots will be delivered and can remain dormant and undetected until they are needed to be put into action.

# Social Responsibility vs Liability

- Free WiFi – Sign an acceptance splash page waiving liability.
- Actually protecting those who are using the free WiFi.
- Hotel X Case Study



# Why the Public must take action to protect themselves

- 90% of all Critical Infrastructure is privately owned.
  - Energy
  - Transportation
  - Water Supplies
  - Banking and Finance
  - Agriculture
  - Chemical and Hazardous Materials Industry
- The new jihadist challenge



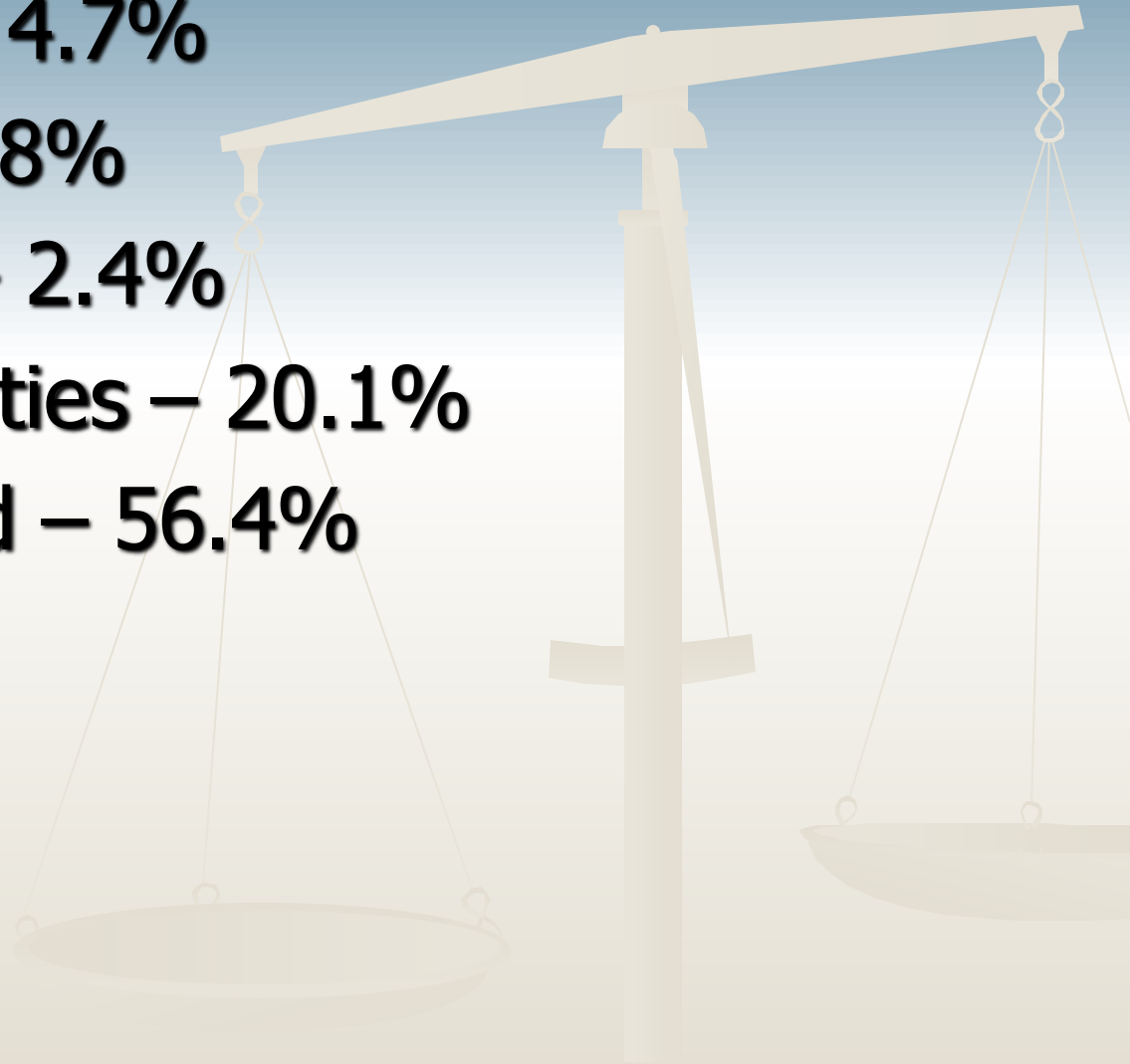
# What % of Dams in the US are owned by State and Federal government?

1. 45%
2. 70%
3. 10%
4. 32%

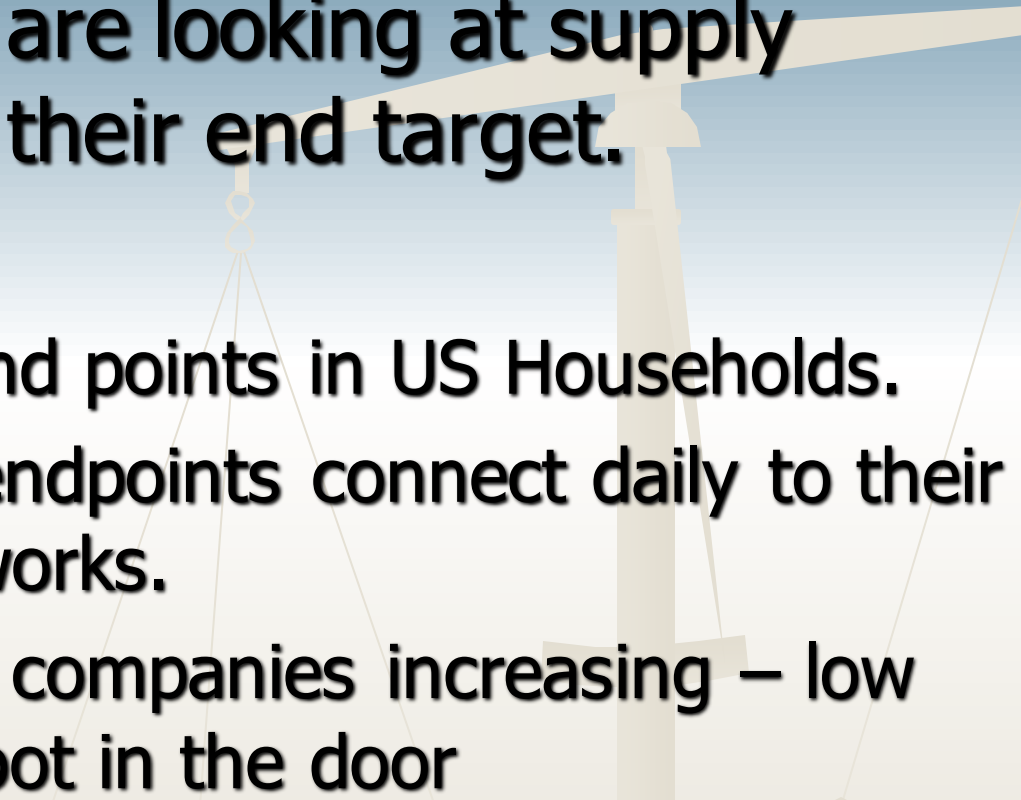


# 10%

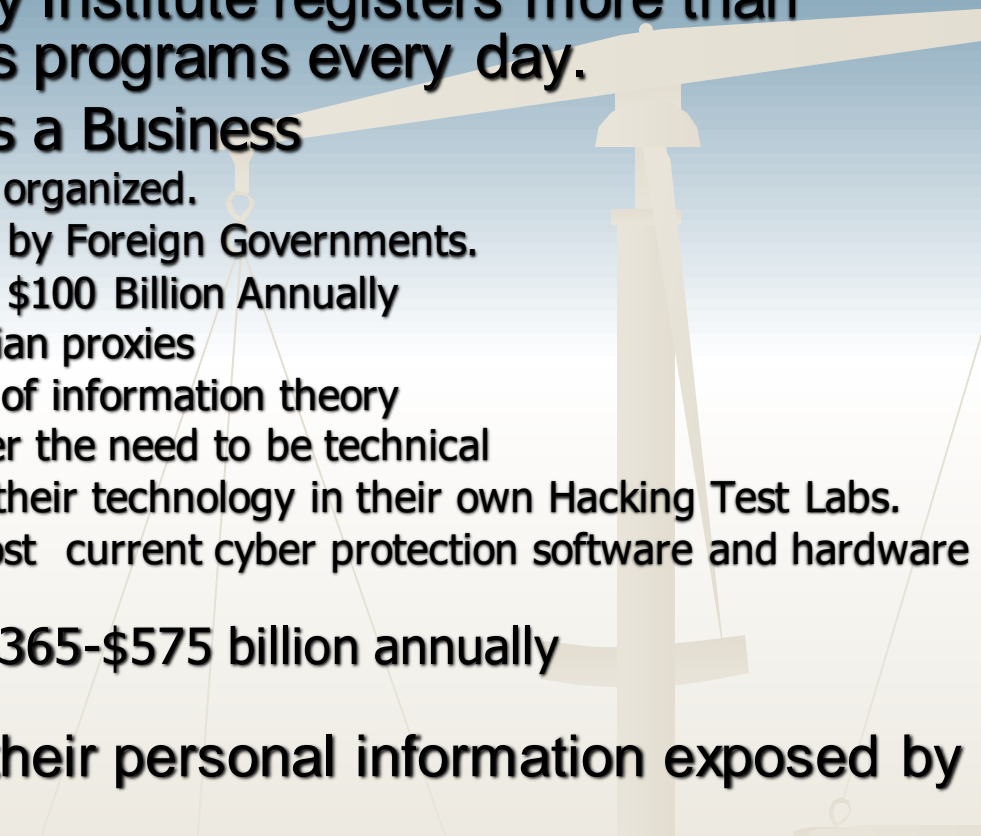
- Federal Govt. – 4.7%
- State Govt. – 4.8%
- Public Utilities – 2.4%
- Local Municipalities – 20.1%
- Privately Owned – 56.4%



# Why the Public must take action to protect themselves

- Cyber Criminals are looking at supply chains to get to their end target.
  - Soft targets
    - Over 1 Billion end points in US Households.
    - Many of these endpoints connect daily to their employers' networks.
    - Attacks on SMB companies increasing – low hanging fruit, foot in the door
- 

# The Cyber Threat – Landscape for 2015

- AVTest and IT Security Institute registers more than 390,000 new malicious programs every day.
  - The Hacking Business is a Business
    - Professionally run and ultra organized.
    - Executed either privately or by Foreign Governments.
    - Extremely profitable – Over \$100 Billion Annually
    - Cyber mercenaries and civilian proxies
    - Based upon building blocks of information theory
    - Anyone can get in, no longer the need to be technical
    - Hackers research and test their technology in their own Hacking Test Labs.
    - They have access to the most current cyber protection software and hardware on the market.
  - Globally costs businesses \$365-\$575 billion annually
  - 47% of US Adults had their personal information exposed by hackers in 2104
- 



# Crypto Locker – SMB Firms




# What can you do?



# What can you do?

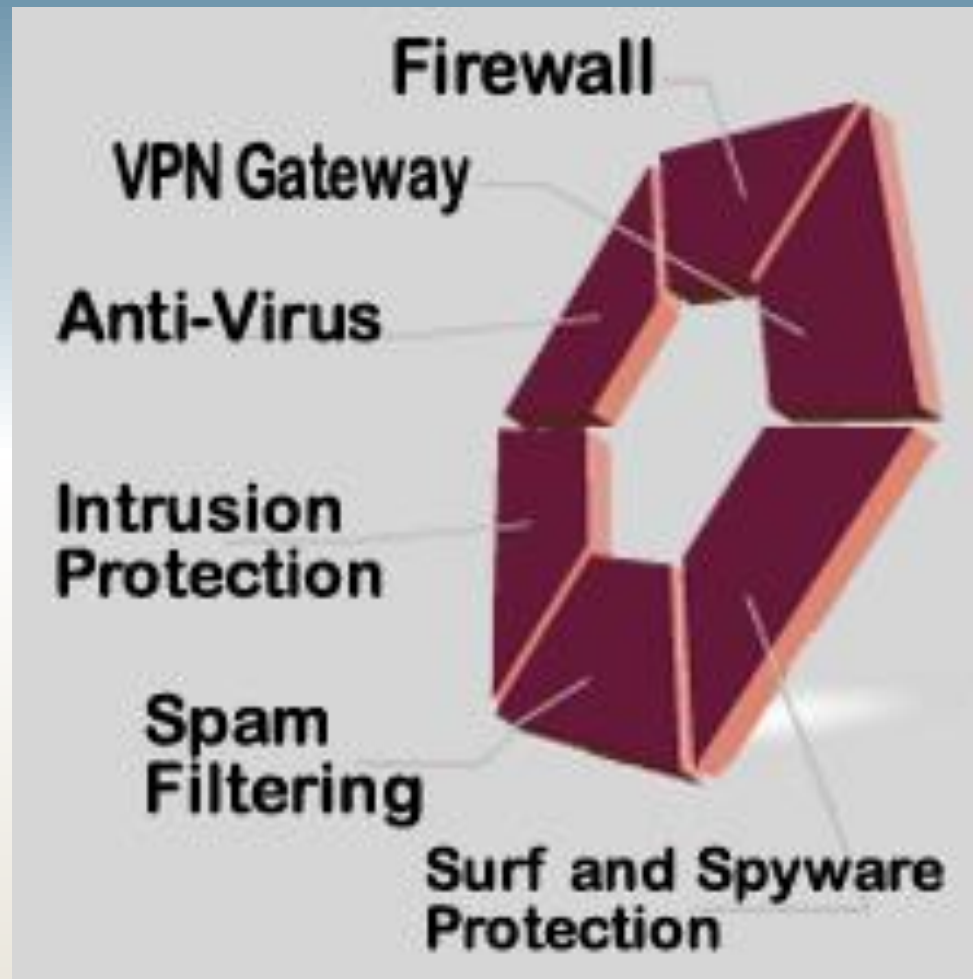


# What can you do?

- Understanding the vulnerabilities and creating a comprehensive plan to protect and secure your data is imperative.
  - This plan would include:
    - Hardware /Software Security Products
    - Secure Network Configurations
    - Enforceable and Monitored Policies
      - Including Penalties for not following policies
  - Regular, 3<sup>rd</sup> Party Security Audits
- 



# Hardware /Software Security Products

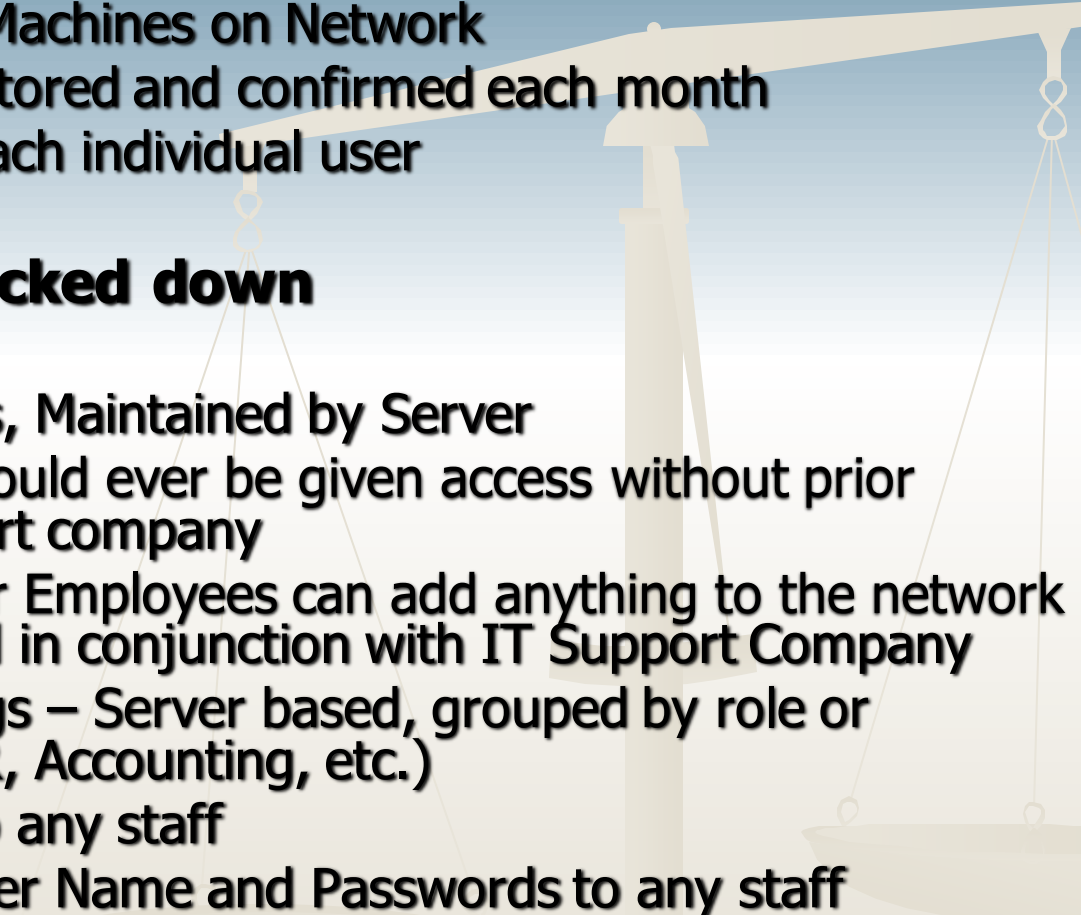




# Hardware /Software Security Products

- Cloud Based Protection – SPAM Filtering / AV
- Firewall – No longer just a firewall
  - Perimeter Defense Appliance
    - Intrusion Protection System
    - Anti Virus / Malware / Spyware Protection
    - Content Filtering
    - VPN Capabilities (For Secure Remote Access)
- Anti Virus Software – On Network
  - Must be installed on every laptop, PC, Tablet (Windows based) and Server.
  - Updates must be current
  - Updates must be automatic (no user interaction)
  - Updates must be monitored and confirmed

# Secure Network Configurations

- **Microsoft Operating Systems must be up to date and consistently patched.**
    - No Server 2003 or XP Machines on Network
    - Patching must be monitored and confirmed each month
    - Do not leave it up to each individual user
  - **Network should be locked down**
    - Secure Remote Access
    - Strict Password Policies, Maintained by Server
    - No 3<sup>rd</sup> Party Vendor should ever be given access without prior knowledge of IT support company
    - No 3<sup>rd</sup> Party Vendors or Employees can add anything to the network without permission and in conjunction with IT Support Company
    - Active Directory Settings – Server based, grouped by role or Management Level (HR, Accounting, etc.)
    - No access to firewall to any staff
    - No access to Admin User Name and Passwords to any staff
- 

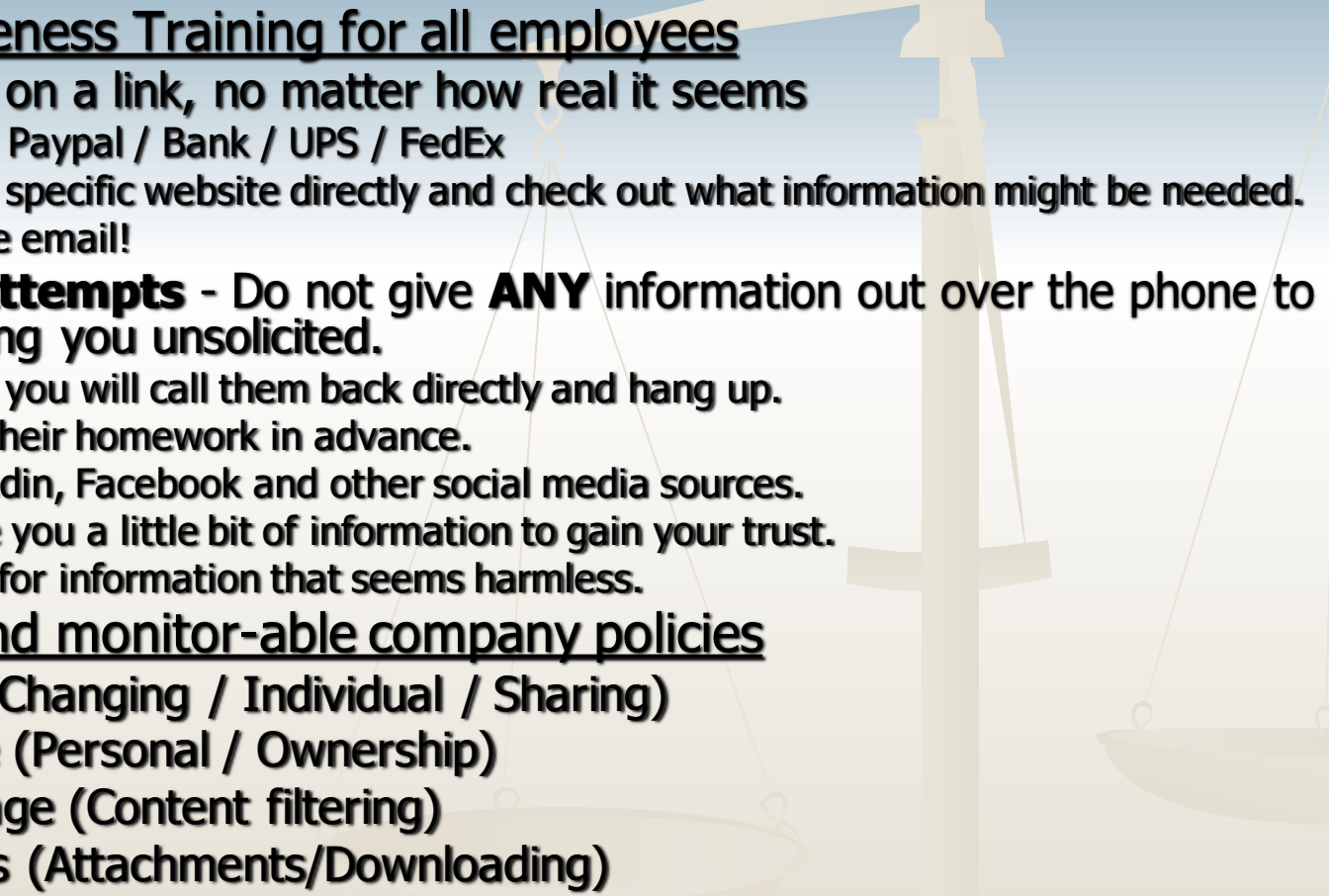
# Secure Network Configurations

## ■ Wireless

- Secure Private and Public Networks
  - Member / Guest Access – Password Protected
  - Splash Page – Liability waiver
  - Hot Spots allowed?
- Password Protected for Business Use (Private)
- Absolutely NO non-approved Access Points allowed on premises.
- Managed Wireless Solutions
  - Rogue Access Points / Denial of Service

# Enforceable and Monitored Policies

***95% of all security incidents involve human error!***

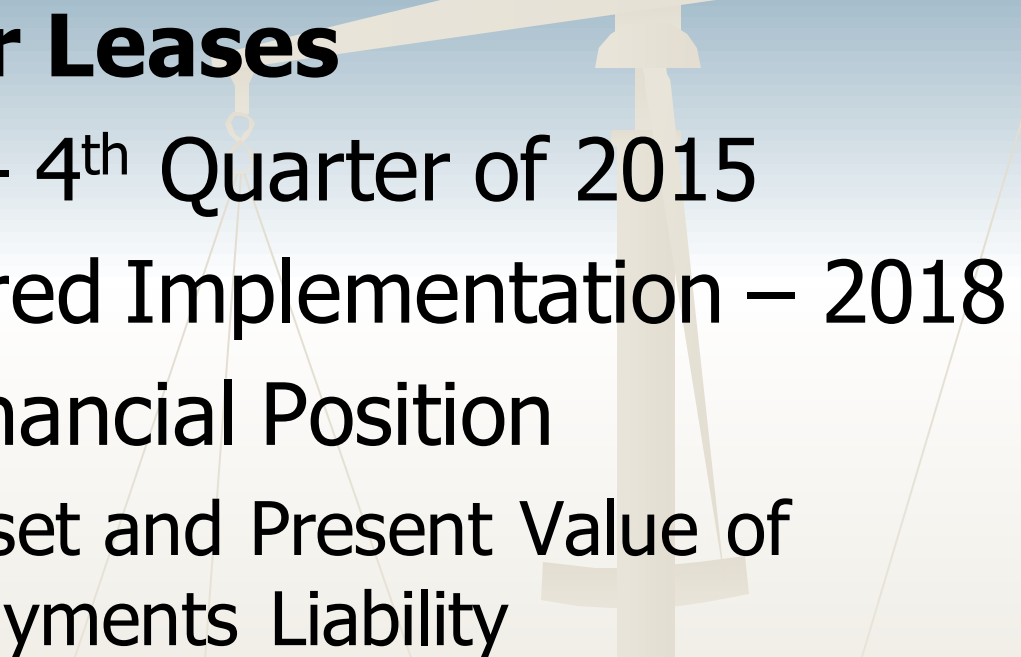
- 
- Security Awareness Training for all employees
    - **Never** click on a link, no matter how real it seems
      - Amazon / Paypal / Bank / UPS / FedEx
      - Go to the specific website directly and check out what information might be needed.
      - Delete the email!
    - **Phishing Attempts** - Do not give **ANY** information out over the phone to anyone calling you unsolicited.
      - Tell them you will call them back directly and hang up.
      - They do their homework in advance.
      - Use LinkedIn, Facebook and other social media sources.
      - They give you a little bit of information to gain your trust.
      - They ask for information that seems harmless.
  - Enforceable and monitor-able company policies
    - Passwords (Changing / Individual / Sharing)
    - Email usage (Personal / Ownership)
    - Internet usage (Content filtering)
    - Data Policies (Attachments/Downloading)
    - 3<sup>rd</sup> Party Applications

# Cyber Security Resources

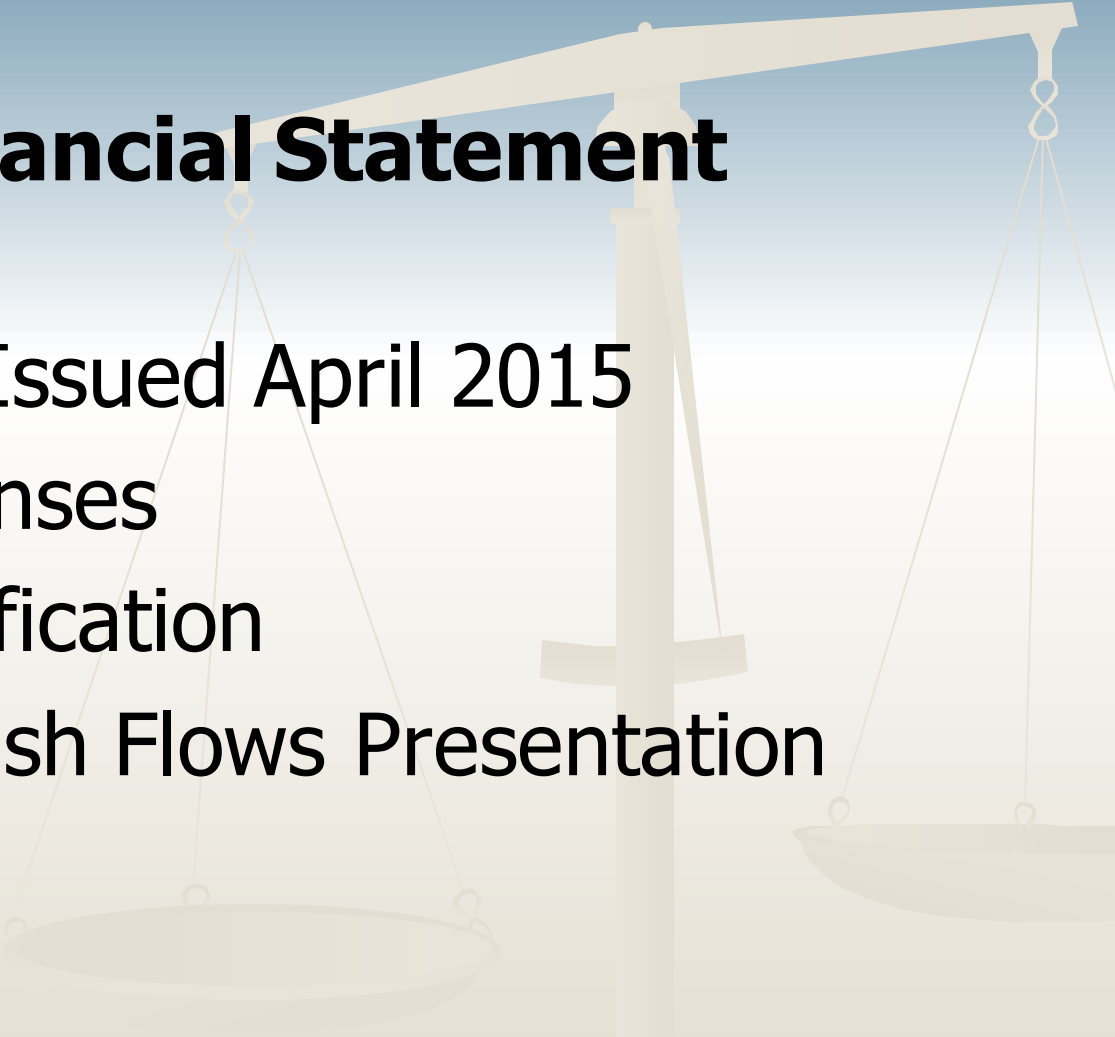
- Your IT Support Company / Trusted Business Partner
- The ***Identity Theft Research Center*** breach list is a compilation of data breaches confirmed by various media sources and/or notification lists from state governmental agencies. This list is updated daily, and published each Tuesday.
  - <http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html>
- Experian Data Breach Industry Forecast
  - [http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf?\\_ga=1.172114915.1943093614.1418003182](http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf?_ga=1.172114915.1943093614.1418003182)
- Homeland Security – Combating Cyber Crime
  - <http://www.dhs.gov/topic/combating-cyber-crime>



# Current Accounting Issues

- 
- **Accounting for Leases**
  - Final Standard – 4<sup>th</sup> Quarter of 2015
  - Expected Required Implementation – 2018
  - Statement of Financial Position
    - Right of Use Asset and Present Value of Future Lease Payments Liability

# Current Accounting Issues

- 
- **Non-Profit Financial Statement Presentation**
  - Exposure Draft Issued April 2015
  - Functional Expenses
  - Net Asset Classification
  - Statement of Cash Flows Presentation

# Current Accounting Issues

- Disclosures for certain Investments in Certain Entities That Calculate Net Asset Value per Share (or Its Equivalent). The standard also removes the requirement to categorize within the fair value hierarchy all investments for which fair value is measured using the practical expedient.