LOSCALZO INSTITUTE
A KAPLAN COMPANY

FEI FINANCIAL LEADERSHIP SUMMIT

MAY 21, 2018

FRAUD FROM WITHIN

PRESENTED BY:
BERNIE BROWN, CPA

Biographical Sketch of Bernie Brown, CPA

Bernie Brown, CPA, licensed as a CPA in Delaware, is a discussion leader for ***Loscalzo Institute***. Bernie is a fractional CFO with Brown & Associates, LLC, a firm specializing in the improvement of small to mid-size businesses' bottom lines through strategy, improved execution, and better team dynamics. With more than 30 years' experience as a CFO, VP of Finance, Treasurer, and Risk Manager, Bernie has participated in fast-growing multi-national businesses. He has significant hands on experience with bank relationships, reorganizations, cost reductions, acquisitions and divestitures.

Bernie has worked with Tyco International, Noel Group LLC, Nomaco Inc., Holliston LLC. He is a graduate of Penn State University with degrees in Business Administration & Professional Accountancy, and has also taught Personal Finance 101, Health and Welfare Wellness seminars.

Bernie has been recognized as a leader in his local community, the chairman of the Finance committee at St. Raphael's Catholic Church, the Grand Knight for the local Knights of Columbus Chapter, Board member of Jim White Foundation helping the homeless, is a member of Delaware CPA Society, American Institute of Certified Public Accountants (AICPA).

Course Overview

- Fraud: This ever-evolving intentional act of deception is a threat to the stability of our capital markets.
- Every company must have a deliberate plan to prevent and detect fraud, and must never underestimate the potential of an attack from within.
- Gain best practices, implementing solid internal controls and processes, and technologies that can help combat this rising problem.

What We Will Cover

1. Information from 2018 Association of Certified Fraud Examiners (ACFE) report to the nations
2. Developing a plan to detect
3. Concern for attacks from within
4. Implementing solid controls & processes
5. Technology
6. Developing a plan to prevent

2018 Report Findings from Studying 2,690 Cases

- Survey estimates the problem could be as high as 5% of all revenues world wide. (Estimate from the members survey of the ACFE)
- The 2,690 cases studied represented fraud of *$7B+*
- Median loss *$130,000*
- Median duration of a fraud scheme 16 months
- 22% of cases caused losses of *$1M+*
- Small businesses lost twice as much per scheme
  - <100 employees median loss *$200,000*
  - 100+ employees median loss *$104,000*

THREE MAJOR CATEGORIES OF OCCUPATIONAL FRAUD

- *Asset misappropriation* only – 57% of cases with a median loss of *$114,000* (a scheme in which an employee steals or misuses the organization's resources, theft of cash, billing, inflated expense reports)
- *Corruption along with asset misappropriation* – 32% of cases with a median loss of *$250,000* (a scheme in which an employee misuses his or her influence in a business transaction to gain direct or indirect benefit, bribery, conflicts of interest)
- *Financial statement fraud* – 10% with a median loss of *$800,000* (a scheme in which an employee intentionally causes a misstatement or omission of material information in the organization's financial reports, recording fictitious revenue, understating expenses, or artificially inflating reported assets)

Asset Misappropriation

Type/% of cases	***Median loss***
1. Check and Payment tampering – 12%	$150,000
2. Billing – 20%	$100,000
3. Noncash – 21%	$ 98,000
4. Expense reimbursement – 14%	$ 31,000
5. Cash Larceny – 11%	$ 75,000
6. Payroll – 7%	$ 63,000

CORRUPTION

- 70% of corruption cases were perpetrated by someone in a position of authority (38% manager, 32% owner)
- 50% of corruption cases were detected by a tip
- Industries with highest proportion of corruption cases
  - Energy 53%
  - Manufacturing 51%
  - Government and public administration 50%

Duration of Occupational Fraud Schemes

1.	Payroll	30 months
2.	Check & payment tampering	24 months
3.	Financial statement fraud	24 months
4.	Expense reimbursement	24 months
5.	Billing	24 months
6.	Cash larceny	24 months
7.	Corruption	22 months
8.	Noncash	18 months
9.	Register disbursements	12 months

Plan to Detect

What Other Companies are Doing to Detect Fraud

Top Ten Methods of How the Occupational Fraud was Detected

1.	Tip	40%
2.	Internal audit	15%
3.	Management review	13%
4.	By accident	7%
5.	Account reconciliation	5%
6.	Document examination	4%
7.	External audit	4%
8.	Surveillance/monitoring	3%
9.	Notified by law enforcement	2%
10.	IT controls	1%

***Red numbers equal 77%*

Hotlines & Reporting Mechanisms

Types of Hotlines

Telephone hotline – 42%

Email – 26%

Web-based – 23%

Mailed letter form – 16%

Fax – 1%

Other – 9%

Not All Tips Come Through Hotlines

Direct Supervisor – 32%

Executive – 15%

Fraud investigation team – 13%

Co-worker – 12%

Internal audit – 10%

Fraud losses were 50% smaller at organizations with hotlines than those without $100,000 vs. $200,000

Top Eight Concealment Methods Used by Fraudsters

1.	Created fraudulent physical document	55%
2.	Altered physical documents	48%
3.	Created fraudulent transactions in the system	42%
4.	Altered transactions in the accounting system	34%
5.	Altered electronic document or files	31%
6.	Destroyed physical documents	30%
7.	Created fraudulent electronic documents	29%
8.	Created fraudulent journal entries	27%

Only 3% of all fraud cases did not try to conceal the scheme

Threats from Within

Threats from Within

- Review the facts of the ACFE survey
- Understand longer term trusted employees can end up in a pressurized situations – Review and understand the Fraud Triangle
  - Personal experience, 16 year employee of the year stole $119K
- Develop methods to communicate with and monitor your employees current life situations
- Review an understand the top red flag behaviors

According to the Last Ten Surveys

The top six red flag behaviors have not changed. While 85% of fraudsters displayed at least one behavioral red flag, 50% exhibited multiple red flags.

- 43% living beyond means
- 34% unusually close association with vendor/customer
- 23% financial difficulties
- 21% “Wheeler-dealer” attitude
- 18% Control issues, unwillingness to share duties
- 15% Divorce/family problems

How Does the Perpetrator's Tenure Relate to Occupational Fraud?

Length of employment/% of cases	***Median fraud loss***
Less than 1 year – 9%	$ 40,000
1-5 years – 44%	$100,000
6-10 years – 23%	$173,000
More than 10 years – 24%	$241,000

WHAT DEPARTMENTS POSE THE GREATEST RISK?

Department/% of cases	***Median loss***
1. Executive & upper management – 11%	$729,000
2. Information technology – 3%	$225,000
3. Warehouse & inventory – 3%	$200,000
4. Accounting & finance – 10%	$184,000
5. Facilities & maintenance – 3%	$175,000
6. Purchasing – 5%	$163,000
7. Manufacturing & production – 8%	$144,000
8. Sales – 12%	$ 90,000

Collusion by Multiple Perpetrators

# of perpetrators/% of cases	***Median loss***
One perpetrator – 52%	$74,000
Two perpetrators – 19%	$150,000
Three perpetrators – 30%	$339,000

THE FRAUD TRIANGLE

- Donald Cressey's findings came to be summed up in the Fraud Triangle
- The three components of the triangle are: pressure, opportunity and rationalization
- When all three of these elements are in place in an individual's life, he or she is very likely to commit fraud – or already has

THE FRAUD TRIANGLE

Why people steal:

- Pressure – in the context of the Fraud Triangle, typically is the direct result of financial difficulties
- Opportunity – exists when an employee discovers a weakness in the organization's anti-fraud controls
- Rationalization – person who has committed fraud convinces himself or herself that the act is not wrong

Methods to Check In with Your Employees

- *Birthday roundtables* – One company I worked for had a monthly birthday celebration for everyone born in that month. They then had a question and concern period with the plant manager, and HR representative.
- *Employee reviews* – This is a good time to check in and those with financial problems will be pressing harder for a bigger increase.
- *Company events* – It is an opportunity to check in with the spouse and see if everything is ok.
- *Employee surveys* – It never hurts to get feedback from your workforce, and some of these surveys provide for anonymity.

Best Practices

What are Companies Doing?

Top Ten Anti-Fraud Controls

1.	Code of conduct	80%
2.	External audit of financial statements	80%
3.	Internal audit department	73%
4.	Management certification of financial statements	72%
5.	External audit of internal controls	67%
6.	Management review	66%
7.	Hotline	63%
8.	Independent audit committee	61%
9.	Employee support programs	54%
10.	Anti-fraud policy	54%

IMPLEMENTING SOLID CONTROLS & PROCESSES

1 TRAIN YOUR STAFF

- Finance
- Line management
- Senior executives

2 CREATE A SPENDING AUTHORITY LIST

3 SEPARATION OF DUTIES IDEAS

- Vendor set up
- Cash functions
- AP/AR

4 MANDATORY 2 WEEK VACATIONS EVERY FIVE YEARS

CONTROLS & PROCESSES

5 DO YOUR ACCOUNT RECONCILIATIONS

- Create a quarterly revue process of the whole balance sheet

6 CLEAN UP YOUR VENDOR FILE

- Inactivate year one
- Delete year two

7 MONTHLY REVIEW YOUR NUMBERS AGAINST BUDGET AND PAST YEAR

8 DON'T CHANGE VENDOR PAYMENT INFORMATION WITHOUT CONFIRMATION

CONTROLS & PROCESSES

9 DON'T LET PEOPLE OVERRIDE CONTROLS, SUPPORT YOUR TEAM

- No last minute check requests
- Use positive pay

#10 THE NOTEBOOK STORY, INTERNAL AUDIT

- Most CFO/controllers in small companies sign all the checks

#11 DON'T WIRE MONEY UNLESS YOU TALK TO YOUR BOSS

- CEO fraud scheme mentioned earlier

#12 MAIL YOUR CHECKS

- U.S. Attorney prosecutes mail fraud cases

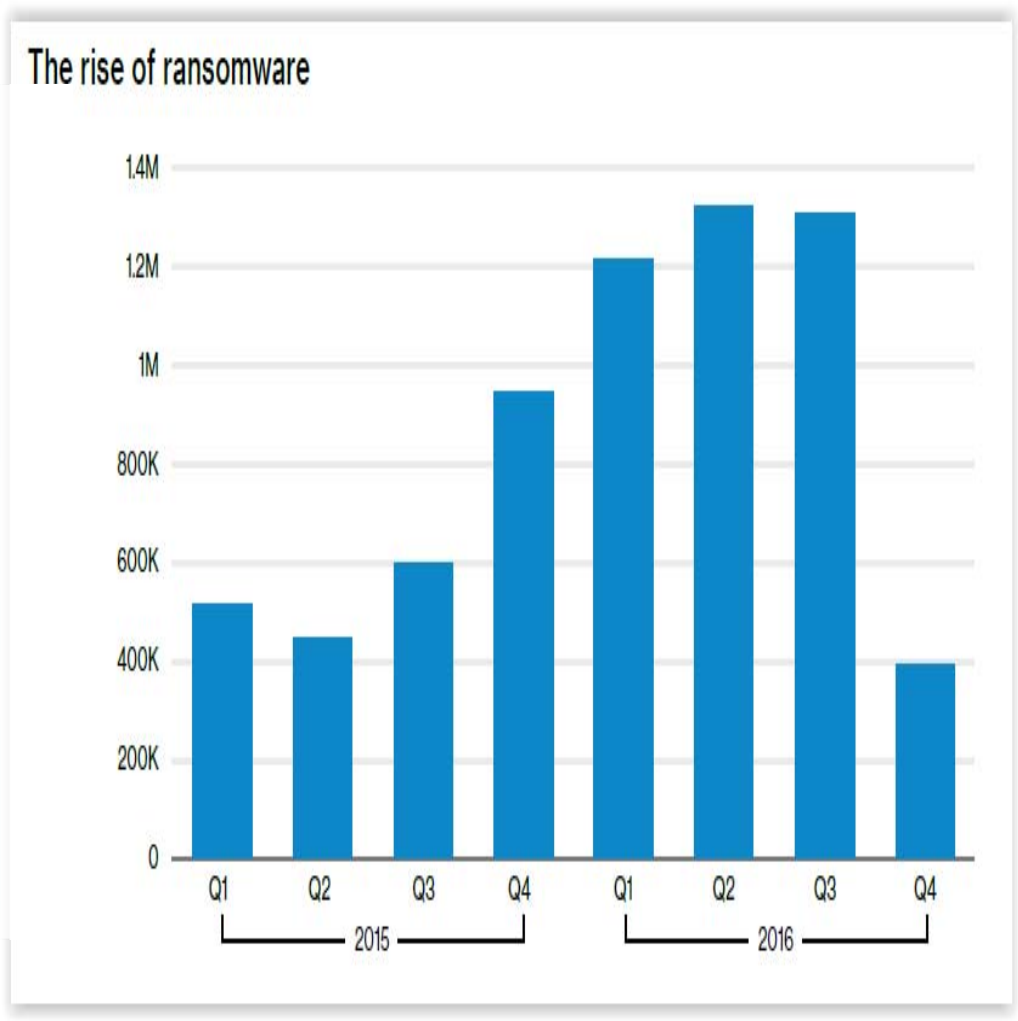
TECHNOLOGY

Drivers for Strong Security

- Meet regulation compliance
  - For regulated companies
  - For partners of regulated companies
- Prevent disruptive attacks
- Prevent lost or stolen key data
- Need to plug new holes or new attack types
  - Advanced attacks & ransomware attacks
  - Apps & data migrating to the cloud & mobile
  - IoTs
  - AI attacks slides from Tom

RANSOMWARE IS HERE TO STAY

- **Growing** (> 500,000 PCs)
- **Disruptive & Costly**
- **Attacks Small, Med., Ent.**
- **Lost Productivity, Lost Data**
- **72% of Healthcare Incidents**
- **Top Causes:**
  - Phishing
  - Untrained Employees
  - Insufficient Security



How Ransomware Works

Attackers Website
Download Malicious Code

Bad Web Link

Request

Download

- **Files Encrypted** (even Backup)
- **System Unusable**
- **Ransom Needed**
- **No Traces of Dr. Evil**

PDF

W

Attachment

Application or O/S Exploit

Ransomware

Compromised

RANSOMWARE SOLUTIONS

THREATS

- Phishing & Social
- Attachments/ Links
- Malicious Websites
- Browser Attacks
- App. Attacks
- Zero-Day Malware
- Botnets
- C & C

SOLUTIONS

Disaster Recovery

- Quality Systems/Data BDR
- Offline Backups

Education

- Security Awareness Training

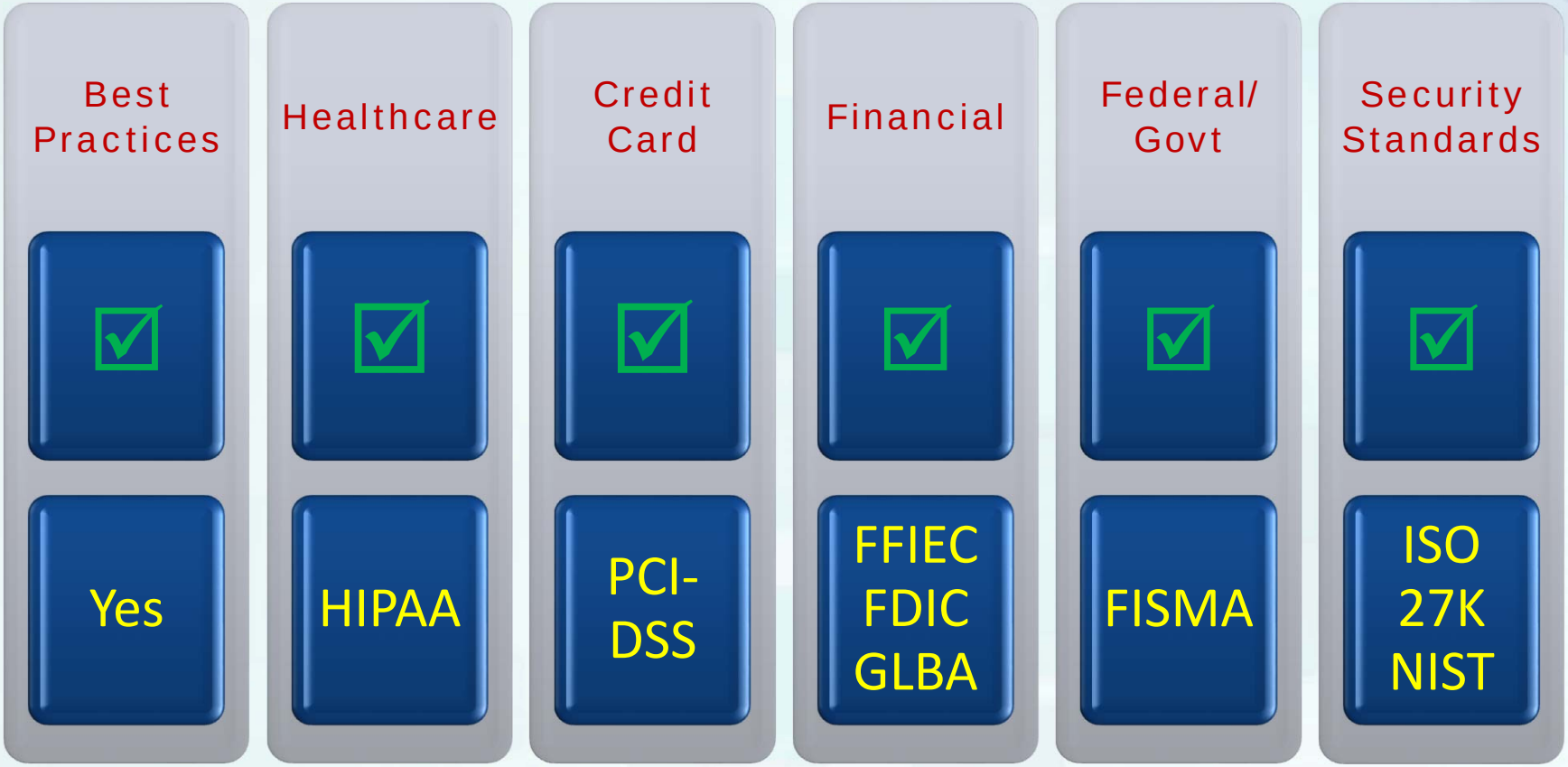
Prevention/ Defense

- Defense in Depth Strategy
- Strong Email/Phishing Security
- Advanced NextGen Endpoint
- Server Endpoint Security
- Strong NextGen Firewall
- Patch Management
- Restrict PC Program Access
- APT (Firewall or Network/Mail/EP)

Monitoring/ Alerting/Blocking

- SIEM (FIM, IDS, Vuln. Scan, C&C, Alerting, Forensics)
- Server/Storage Resource Monitoring

Where is Security Training Required?



Top Compliance Regulations

	Regulations	Who Needs to Comply	Security Areas Covered	Compliance Requirements	Penalties
Healthcare	**HIPAA** **HITECH**	**All Healthcare Organizations & Partners (Suppliers)**	Creating Storing & Transmitting electronic protected health info. (PHI)	All Major "Best Practices Security" Areas	$25,000/Person - General Non-compliance Penalty $50,000-250,000 Wrongful Disclosures
Public Cos.	**Sarbanes Oxley (SOX)** & Accounting Stds COSO, COBIT, SAS	**Public Companies**	Defined to secure the public against corporate fraud & Misrepresentation	All Major "Best Practices Security" Areas	Corporate & Personal Criminal Liability
Merchants/ Credit Cards	**PCI DSS** **(VISA/MC/AMEX/Discover)** (Also in by Private Data Breach Laws)	**Merchants who take Credit Cards**	Privacy of Customer Financial Data	Varies by size of Merchant Requires Best Practices plus 3rd Party Qtly Risk Assessments	Fines, Restrictions, Expulsion from Credit Card Cos. Potential Lawsuits, Public Disclosure
Financial Banks	**GLBA (Fin. Data Fed. Law)** **FDIC/FFIEC/NCUA** **FACT & U.S. Patriot Act (2001)**	**9,500 Financial Institutions (Credit Unions, Banks, Others)**	Privacy of Personal Info. Safety of Internet Products & Services Fair & Accurate Credit Anti-Terrorism	"Best Practices" Security Two-Factor Authentication Ensure Accuracy & Safety Identity Verification	Fines, Imprisonment, Lawsuits, Penalties as Imposed by Federal Regulators
Consumer Private Data	**Breach Laws in 46 States Including California SB 1386**	**Any Company storing, or accessing private consumer data**	Consumer Privacy - Security Breach Acts	All Major "Best Practices Security" Areas	Public Disclosure, Law Suits
Federal Government	**NIST Cybersecurity Framework** (V1.1 2017) Leverages (ISO, COBIT, NIST 800)	**Government Contractors/Suppliers**	Overall Security Framework & Improvement Process (Framework Core, Tiers and Profile)	Broad Assessment of Current & Target Maturity Level, Implementation Plan	Loss of Government Customers or Government penalties
International Standard	**ISO 27001/2** Used in NIST, Large Orgs, or as International Audit standard	**International Security Audit Benchmark**	All Areas of Cybersecurity	Best Practices Security per ISO Standard	None specifically
Education	**FERPA & CIPA**	**Educational Institutions**	Protect Student Records and Minors Web, email, chat access, Protect Data	Protection effort re: protection of Minors & Personal data	Federal Funding, Lawsuits
All Companies	**FRCP** (Federal Rules of Civil Procedure)	**All Companies Fearing Civil Lawsuits**	Requirements to Retain Electronic Data for the Purposes of eDiscovery	Retain emails, IM, Files for 3-7 years (archiving)	

Note that most security regulations also apply to the partners and suppliers of companies that must be compliant in order for those companies to comply. That means that it is becoming increasingly difficult for any company to avoid implementing and certifying a company's compliance with "Best Practices" Security at a minimum.

AWARENESS TRAINING & PHISHING SOLUTIONS

ONLINE TRAINING & SOCIAL ENGINEERING TESTING	
FEATURES	
Console & Reporting	✓
Security Hints & Tips, Posters	✓
Automated Training Campaigns[1]	
Core Classes	✓
Compliance Courses (PCI, HIPAA, FFIEC, SOX, FERPA, GLBA)	✓
Social Engineering Testing	
Unlimited Phishing Simulations[2]	✓
USB Drive Test	✓

Why is ID Control Important?

- Identity management may be your companies most important security control
- 81% of 2017 breaches involve stolen or weak passwords
- Loss of access control
  - Immediately bypasses all security & gives access to key company data, financial transactions, applications, personal data, IP….
  - Key to CEO fraud

Access Control Solutions

Need to Control Access to Key Areas:

- Financial applications onsite and in the cloud (ERP, accounting, payroll)
- Security systems (firewalls, monitoring systems, backups, Endpoint….)
- Computer systems (your network, servers, clients, mobile)

Most Popular Security Authentication Methods:

- Phone applications that are tied to you and your phone
- Device identity, location & behavior
- Text message and emails sent to your account/phone
- Biometrics: Finger prints, facial recognition

No real excuse to not have almost everything use at least 2-Factors to authenticate

Securing the Internet of Things

IoT Defined: The **Internet of things** (**IoT**) is the network of **Internet connected** physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data.

Threats:

- IoT devices attacked and
  - become zombie attackers in your network
  - provide access to your home, business, systems, data
  - initiate a distributed denial-of-service attack against someone else
- Mission critical IoT devices are attacked and affect your business continuity
- IoTs increasingly are controlling and automating our lives (Attack of the Machines?)

Securing the Internet of Things

Why are they vulnerable:

- 1,000s of manufacturers
- Manufacturers have low security experience
- No standardization of system software or hardware
- Devices are under the radar (for now)
- Low levels of access control

IoT Security

- Will be a combination of many things
- Will usher in a new set of solutions to protect diverse wireless devices that are connected to the cloud

CEO Fraud Attack Process

Reconnaissance

Criminals research your public and private information to understand your accounts used, process & people

Attackers try to spoof your email or impersonate your CEO, Attorney or other key people?

Phishing

Spoofed emails are sent to high risk employees requesting:

- Wire transfers
- Pay Invoice
- Transfer Money
- Send HR Records
- Other financial transaction

Response

Employee processes request since it is similar to ordinary course of business & from an authorizing superior

25% Respond

Damage

Money or private information is transferred to foreign accounts or people so it cannot be retrieved or traced

Impact

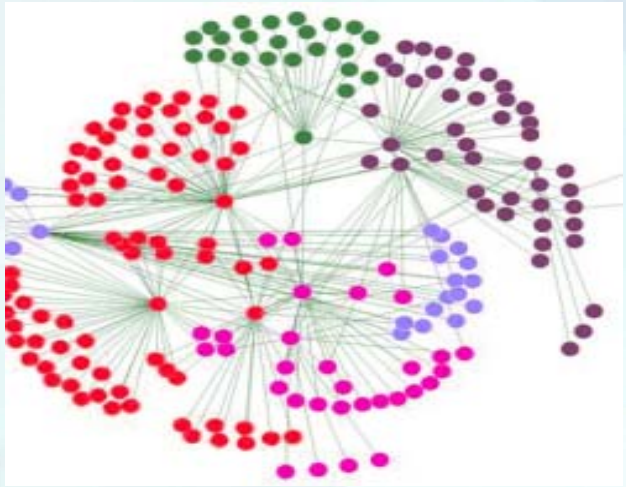
- Money is gone forever
- Private data is lost
- CEO is fired
- Employee terminated
- Lawsuits files
- Reputational loss

CEO Fraud Prevention

- **Install Strong Security**
- Email, web, gateway (firewalls)
- **Educate Employees and Executives**
- Employee online training & phishing simulations
- **Restrict What Key Employees Post on Public Sites**
- Social media is a mining goldmine
- **Implement 2-Factor Authentication (Computer & Processes)**
- **Register Similar Domain Names**
- **Verify Communications from Trusted Partners**

Do You Know Where Your Data Is?

It Used to be On Your Servers



THREATS & SOLUTIONS

Moving more and more of your data and systems to third party controlled cloud vendors can't make your security better… right?

Can you rely on third parties to:

- Secure your data?
- Provide 100% uptime?
- Control who accesses your data?
- Keep your data from being corrupted?

The cloud requires new specific solutions for:

- Cloud data centers (public & private)
- Access from anywhere – Do you know who is accessing your apps & data?
- 3rd party cloud applications & storage
- IoTs too

START BY

CREATING A PLAN TO PREVENT FRAUD

Deliberate Plan To Prevent

- Meet with the Board & Senior Management and show the facts
- Enlist support to take the problem seriously and set the proper tone from the top
- Review the top internal control weaknesses
- Review the Fraud mitigation cycle & conduct a fraud risk assessment
- Create a plan and align the resources in your organization to take action
- Execute & review the plan and its effectiveness on an annual basis

Show the Board the Facts & Enlist Support

- The Facts
  - ACFE – 2018 report
  - FBI – website of recent fraud cases
  - AICPA – website
  - Your state society website
- Enlisting support
  - Start with your CEO
  - We all know which board members are more concerned
  - Establish an audit committee

Internal Control Weaknesses that Contribute to Occupational Fraud

1.	Lack of internal controls	30%
2.	Override of existing controls	19%
3.	Lack of management review	18%
4.	Poor tone at the top	10%
5.	Lack of competent personnel in oversight roles	8%
6.	Lack of independent checks/audits	4%
7.	Lack of employee education	2%
8.	Other	9%

***Red items represent 85%*

CONDUCT A FRAUD RISK ASSESSMENT (FRA)

Fraud Risk Assessment (FRA)

Step 1: Create a FRA Team

Step 2: Identify the Organization's "Universe" of Potential Risks:

- What types of fraud have occurred or been suspected in the past?
- What types of fraud *could* be committed against the organization?
- What are the specific ways employees or managers could commit fraud by acting alone?

CONDUCT A FRAUD RISK ASSESSMENT (FRA)

- What are the specific ways vendors could commit fraud in your area?
- How could vendors working in collusion with your co-workers commit fraud?
- Incorporate fraud-audit testing and techniques into the audit to screen for "hard" evidence of the red flags
- Develop a list of red flags of the potential fraud risk identified by your FRA

Step 3: Analyze the Likelihood of Each Scheme or Scenario Occurring

Step 4: Assess Risks within the Context of Existing Anti-Fraud Controls

STEP 1 TO A SECURE ENVIRONMENT

3rd PARTY RISK ASSESSMENT

- ✓ Assess Your Security Posture
- ✓ Identify Risks
- ✓ Prioritized Security Gaps
- ✓ Prioritize Needed Controls
- ✓ eSecurity Solutions

Next Steps

- Submit results of the fraud audit to management
- Assist management in revising or devising effective anti-fraud controls for reducing the risks of the frauds that have been discovered as well as those that could occur, according to the findings of the FRA
- Meet with your team at least quarterly to assure the threats identified and the steps to prevent them are being implemented.
- Review with your audit committee and external auditors annually