Protecting Your IT Network from Financial Fraud

Illinois Community College CFOs

Mark Wilson, CISSP, ITIL, CBCP, CCM
Director of Information Risk Management
Agenda

• What is Fraud?
• Interesting Statistics
• What I Would Do?
About Sikich

» **Multi-disciplinary**: An accounting, advisory, investment banking, technology and managed services firm with clients in the U.S. and internationally.

» **Excellent reputation**: With a reputation for professional excellence, Sikich provides unsurpassed client service as well as timely and cost effective services.

» **Strong talent**: We employ more than 500 talented people including 91 partners, all of whom devote their careers to a focused area.

» **Award winning**: *Accounting Today* ranks the Firm 40th nationally among the top 100 accounting firms and 11th in the top 100 VARs.

- **$97M** in revenue in 2013
- **6,976** public and private sector clients
- **8,635** individual clients
- **500+** total personnel
- **91** partners
- **1** collaborative and positive culture
Sikich Service Lines

**Accounting, Audit & Tax**
- Financial Reporting
- Employee Benefit Plan Audit
- Accounting Services
- Tax Planning

**Advisory**
- Business Valuation
- Dispute Advisory
- Human Resources
- Insurance Services
- Marketing & Public Relations
- Retirement Plan Services
- Risk Advisory
- Supply Chain
- Wealth Management

**Investment Banking**
- Acquisitions Advisory
- Sales Advisory
- Capital Raises
- Strategic Advisory

**Technology**
- Accounting & ERP Software
- CRM Software
- IT Infrastructure
- Cloud & Hosting Solutions
- Strategic IT Planning
- Communication & Collaboration
- IT Consulting

**Managed Services**
- Outsourced Accounting
- Managed IT
- Outsourced Human Resources
- Outsourced Marketing & Public Relations

Securities are offered through Sikich Corporate Finance LLC, a registered broker dealer with the Securities Exchange Commission and a member of FINRA/SIPC. Advisory services offered through Sikich Financial, a Registered Investment Advisor. General securities offered through Triad Advisors, Member FINRA/SIPC.
Industry Expertise, Tailored Approach

» Agriculture
» Manufacturing & Distribution
» Construction
» Professional Services
» Real Estate
» Retail
» Government
» Non Profit
» Healthcare
» Higher Education

Deep industry experience and longevity.

Cross sectional teams with a depth and breadth of experience to handle the complete solution.

Solution centric and product agnostic.
What is Fraud?
Legal Definition of Fraud

- Intentionally false representation
  - Not an error
  - Lying or concealing actions
  - Pattern of unethical behavior
- Personal material benefit
- Organizational or victim loss
When Does Fraud Occur?

THE FRAUD TRIANGLE

RATIONALIZATION-
Justification of dishonest actions.

FRAUD

OPPORTUNITY-
Ability to carry out misappropriation of cash or organizational assets.

PRESSURE-
Motivation or incentive to commit fraud.
Uniform Occupational Fraud Classification System
Uniform Occupational Fraud Classification System

Cash
- Larceny
  - Of Cash on Hand
  - From the Deposit
  - Other
- Skimming
  - Sales
  - Receivables
  - Refunds & Other
  - Unrecorded
  - Understated
  - Lapping Schemes
  - Unconcealed

Fraudulent Disbursements
- Billing Schemes
  - Shell Company
  - Non-Accomplice Vendor
  - Personal Purchases
- Payroll Schemes
  - Ghost Employees
  - Commission Schemes
  -Workers Compensation
- Expense Reimbursement Schemes
  - Mischaracterized Expenses
  - Overstated Expenses
  - Fictitious Expenses
  - Multiple Reimbursements
- Check Tampering
  - Forged Maker
  - Forged Endorsement
  - Altered Payee
  - Concealed Checks
  - Authorized Maker

Inventory and all Other Assets
- Misuse
- Larceny
  - Asset Req. & Transfers
  - False Sales & Shipping
  - Purchasing & Receiving
  - Unconcealed Larceny
Fraud Definition

• Violates the employee’s fiduciary responsibility to employer
• Is done secretly and is concealed
• Is done to achieve a direct or indirect benefit
• Costs the organization assets, revenue, or opportunity

Fiduciary – a person to whom property or power is entrusted for the benefit of another…
Vocabulary

• **Skimming**: Taking funds before they are recorded into company records
• **Cash Larceny**: Taking funds (e.g., check) that company recorded as going to another party
• **Lapping**: Theft is covered with another person’s check (and so on)
• **Check Tampering**: Forged or altered check for gain
• **Shell Company**: Payments made to fake company
• **Payroll Manipulation**: Ghost employees, falsified hours, understated leave/vacation time
• **Fraudulent Write-off**: Useful assets written off as junk
• **Collusion**: Two or more employees or employee & vendor defraud together
• **False Shipping Orders** or **Missing/Defective Receiving Record**: Inventory theft
But My Auditor Gave a Clean Opinion

• An unqualified audit opinion does NOT mean that there is no employee dishonesty or fraud occurring in the organization.
• Employee dishonesty and other acts of fraud can be significant and the books can still balance; often exists even when bank accounts are reconciled.
• SAS 99, professional skepticism and materiality
# Fraud Statistics

<table>
<thead>
<tr>
<th>Prevalence: Companies affected by fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>66%</td>
<td>60%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management conflict of interest (21%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information theft, loss or attack (20%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft of physical assets or stock (20%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory or compliance breach (17%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information theft, loss or attack (26%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft of physical assets or stock (24%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory or compliance breach (16%)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Increase in Exposure: Companies where exposure to fraud has increased</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>81%</td>
<td>66%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Complexity (44%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Complexity (35%)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loss: Average percentage of revenue lost to fraud</th>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.8% (IT)</td>
<td></td>
<td>1.1%</td>
</tr>
</tbody>
</table>
Fraud Statistics

The United States has an incidence of fraud below the overall average – 66% of companies were hit by one fraud in the last year compared to 70% globally – and a rate of loss that is also slightly under the norm – 1.2% compared to 1.4% for the survey as a whole.
Fraud Statistics for IT

- IT has the lowest fraud rate... 😊

- IT has the highest cost of fraud per incident ... 😞
A Response to Fraud
Who Do We Watch?

Kroll - 2013 / 2014 Global Fraud Report

1. H1B visa workers
2. Independent contractors and temps
3. Remote employees

Many Sources

- Insiders with power and opportunity
- Super Users (admin / root authority) are problematic. High value & high risk.

Non-network – asset misappropriation, bribery, financial statement fraud
Recommendations

1. Identify and contain sensitive data
2. Screen independent contractors and temporary workers
3. Encrypt or limit the use of unmonitored remote devices
4. Establish and enforce institution wide consequences for security violations
5. Engage conflict-free examiners to conduct investigations on insiders who abuse IT systems
6. Centralize, safeguard, and analyze computer logs
7. Establish thorough employee expectations and termination policies
8. Restrict the use of removable media
9. Run and require acceptance of terms on privacy banners
10. Backup and retain data – for analysis

Modified list from Kroll
What is Security?
Three Security Pillars

SECURITY – C.I.A.

- Confidentiality
- Integrity
- Availability
Security – another perspective

(ISC)²
International Information Systems Security Certification Consortium

“Security Transcends Technology”
High Level Security Controls

- Physical
  - Locks
  - Lights
  - Fences

- Logical (technical)
  - Firewall
  - Passwords
  - Motion Detectors

- Administrative
  - Policies
  - Audits
  - Training

Preventive – Detective – Corrective - Compensatory
High Level Security Controls

Triad of Security Controls

Preventive – Detective – Corrective - Compensatory
Where Do I Start?
Management Fundamentals

The Five Dysfunctions of a Team by Patrick M. Lencioni

- Inattention to Results
- Avoidance of Accountability
- Lack of Commitment
- Fear of Conflict
- Absent of Trust
The Five Dysfunctions

1. Absence of Trust
2. Fear of Conflict
3. Lack of Commitment
4. Avoiding Accountability
5. Inattention to Results
Executive / Senior Management Role
Management Should Challenge IT

How Can IT Help Us Deal With Fraud?

• Become more transparent to the organization
• Speak “business”
• Become auditable
• Develop security solutions
• Be our eyes and ears
• Engage trusted 3rd parties
Senior Management Responsibilities

- Mandate and define security in your institution
- Segregation of Duties
- Least Privilege Principle
- System, device, database, software and file based audit capabilities
Organizational Changes…

How Shall We Then Live?
Francis Schaeffer

• Cultural Changes
• Institutional Mindset

These are NOT Additional Initiatives!!!

• Security
• Recovery
• Resiliency
• Insource vs Outsource
Partner in the Absence of Expertise
Questions?
Mark Wilson
mwilson@sikich.com

www.sikich.com
Thank You