

Bridging the Gap - Employing Fraud Risk Assessment to Guide Investments in Fraud Mitigation

Presentation by:

Mr. Brian Nyali

Information Security Consultant, Serianu Ltd

Thursday, 19th September 2019

Presentation agenda



Session Agenda

- ❑ Interpreting and applying the outcome of your fraud risk assessment
- ❑ Applying targeted fraud risk mitigation initiatives to high risk areas.
- ❑ Integrating anti-fraud controls with control framework

Fraud Risk Assessment



What is a Fraud Risk Assessment?

- Systematically identify where and how fraud may occur.
- Identify who may be in a position to commit fraud.
- Creates a structured process that identifies fraud risk schemes and respective controls that may prevent or detect these schemes.
- Measures detective and preventative controls to ensure they are designed and operating effectively

Fraud Risk Assessment



- Crucial part of an entity's Enterprise Risk Assessment (ERM) process.
- Key element to any Anti-fraud Framework.
- Strengthens an organization's ability to evaluate, mitigate and monitor risks arising from fraud, corruption and misconduct.
- Proactively identifying and addressing fraud in an organization.
- Considers both internal and external threats. ☐ It is tailored to the organization and industry.
- It is an ongoing continuous process that never ends.

Fraud Risk Assessment



Bernie Madoff - \$21.2 Billion in Cash Losses



We all know that Bernie will spend the rest of his life in prison for orchestrating perhaps the biggest investment scam of all time, but his accountants and aides helped him do the dirty work. David Friehling, Madoff's accountant, plead guilty last year to a number of charges that he issued "rubber stamp" audits. Madoff's right-hand man, Frank DiPascali plead guilty to creating fake trade orders for Madoff and is facing up to 125 years in prison.

Fraud Risk Assessment



HealthSouth - \$2.7 Billion Accounting Fraud



The rehabilitation provider's former CEO, Richard Scrushy, was convicted of host of criminal and civil charges -- including [bribery](#) -- related to a massive accounting fraud that is believed to have [lasted seven years](#). Scrushy is currently serving a [seven-year prison sentence](#).

Fraud Risk Assessment



Tyco – Execs Steal \$120 Million, Inflate Income by \$500 Millions



Tyco's former CEO Dennis Kozlowski and former CFO Mark Swartz were convicted of misappropriating hundreds of millions of dollars in company funds. On top of that, the two ex-Tyco execs were involved in a scheme to inflate Tyco's income by more than \$500 million.

Fraud Risk Assessment



Satyam - \$1 Billion Accounting Fraud



In just one quarter, execs at the Indian outsourcing firm Satyam magically boosted revenue by 20 percent -- or \$1.04 billion -- by falsifying loans, the New York Times reported last year. Ironically, Satyam maintained back-office accounting functions for several high-profile companies including, General Electric and General Motors.

Fraud Risk Assessment



AIG - \$1.7 Billion in Improper Accounting



Long before AIG became a maligned bailout recipient, the behemoth insurance company was embroiled in a \$1.7 billion accounting scandal involving loans that were improperly booked as revenue. Ex-CEO Hank Greenberg was ousted over the controversy -- and ultimately paid \$15 million to settle fraud charges with the SEC.

Fraud Risk Assessment



- Where was Audit in all this?

Fraud Risk Assessment



Common Theme or Issues?

List as many common issues as you can think of.

1. Pressure to perform from Shareholders/Members.
2. Tone at the Top - Arrogance & Greed.
3. Lack of appropriate controls.
4. External Auditors not exhibiting professional skepticism and due care.
5. Where was Internal Audit

Fraud Risk Assessment



Why Conduct a Fraud Risk Assessment?

- ❑ A Fraud Risk Assessment helps Management understand risks that are unique to its business activities, identify gaps, weaknesses in controls and priorities of controls to manage those risks and develop a realistic plan for targeting the right resources and controls to reduce fraud risks

Fraud Risk Assessment



Why Conduct a Fraud Risk Assessment?

- ☐ Improve communication and awareness about fraud.
- ☐ Identify where the company is most vulnerable to fraud and what activities put it at the greatest risk.
- ☐ Develop plans to mitigate fraud risk.
- ☐ Develop techniques to monitor and investigate high-risk areas. ☐ Assess internal controls.

Fraud Risk Assessment



Why Conduct a Fraud Risk Assessment?

- ☐ Fraud exists in EVERY organization.
- ☐ Fraudsters are becoming more and more sophisticated.
- ☐ And estimated 95% of fraud goes unnoticed unless you are actively looking for it.
- ☐ Should be a component of larger ERM.
- ☐ Comply with regulations and professional standards

Fraud Risk Assessment



Pitfalls & Obstacles

- ☐ “No Fraud here” mentality.
- ☐ “He / She would never.” Believing an individual is a control.
- ☐ Assessment is not risk-based.
- ☐ FRA is too broad, not focused.
- ☐ Approach isn’t aligned with corporate culture.
- ☐ Organization does not have appropriate skill sets to perform assessment properly
- ☐ Not systematic and reoccurring.

Fraud Risk Assessment



- The best way to prevent and detect fraud is by first of all understanding the threats of fraud relevant to your organization.
- We must identify risks relevant to internal business and the potential threats from outside your business.
- When an assessment is being done questions are asked, questions such as:
 - 1) How might a fraud perpetrator exploit weaknesses in the system of controls?
 - 2) How could a perpetrator override or circumvent controls?
 - 3) What could a perpetrator do to conceal the fraud? (never leaving their work station, clearing logs or never enabling logging, using other peoples credentials, using generic usernames)

Fraud Risk Assessment



- A fraud risk assessment generally includes three key elements:
Identify inherent fraud risk —
 - Build a repository of fraud risks that could apply to the organization. Included in this process is the explicit consideration of all types of fraud schemes and scenarios, incentives, pressures, and opportunities to commit fraud and IT fraud risks specific to the organization.
 - i.e cheque fraud .. likely scenarios being altered values , stolen blank cheque, Altered payee, Forged signatures

Fraud Risk Assessment



Assess likelihood and significance of inherent fraud risks —

- Assess the relative likelihood and potential significance of identified fraud risks based on historical information, known fraud schemes, and interviews with staff, including business process owners

Respond to reasonably likely and significant inherent and residual fraud risks —

- Decide what the response should be to address the identified risks and perform a cost-benefit analysis of fraud risks over which the organization wants to implement controls or detection procedures.

Fraud Risk Assessment



- There should be a prioritization of risks based on their significance and likelihood of occurrence and labeled as High, medium or low.
- This should give you an idea of where to start or what needs to be handled immediately.
- This does not mean that items with a low significance and low likelihood of happening should be thrown out the window, we still need to keep an eye on them.
- Risks always change and thus the need to reassess frequently comes into play whether annually or twice a year.

Fraud Risk Assessment



**❑ What are the high risk areas (fraud areas) for the following industries
(What avenues for fraud exist within the following industries):**

 **Insurance**

 **Banking**

 **Manufacturing**

Fraud Risk Assessment



- ❑ **Employing Risk Quantification and Cyber Security Visibility Framework for Fraud Assessment**

Fraud Risk Assessment



What is Cyber Visibility and Exposure Analysis?

The process of adequately measuring the effectiveness and efficiency of implemented cyber security controls to safeguard the organization.

What is Cyber Risk Exposure?

Cyber risk exposure refers to the potential loss an organization faces based on security controls implemented to safeguards its assets

Fraud Risk Assessment



The Serianu Visibility monitoring framework is designed to provide visibility on the following aspects of cyber security planning:

1. What devices are on the network?
2. Who is on the network?
3. Who manages the configurations on these devices?
4. Who can access what devices in the network?
5. How can they access these devices on the network?

Fraud Risk Assessment



Asset Controls	User Controls	Incident Controls	Continuity Controls
Asset Inventory	User Access Management	Incident Response	Performance and Availability
Configuration Controls	Privileged Access Management	Fraudulent Transactions	Operational Considerations
Vulnerability Management	Training & Awareness	Monitoring and Analysis	Disaster Recovery
Malware Defenses			

Fraud Risk Assessment



The Visibility controls testing considers the following

- ☐ **Existence of control:** The assertion is that a control exists.
- ☐ **Completeness of control:** The assertion that the existing control covers all the requirements and is therefore complete. In other words there has been no understatement of controls implemented.
- ☐ **Timeliness of control:** The time that elapses between identification and notification of an incident.
- ☐ **Reporting:** Does the system provide reports on the incident?
- ☐ **Visibility Score:** This is the average of Existence, completeness, timeliness and reporting.

Fraud Risk Assessment



Breach Scenario Analysis entails understanding what can go wrong and putting measures in place to ensure you adequately anticipate, detect, respond and contain any threats that may arise thereafter.



What can go wrong in with our current business processes?

Which systems are most likely to be used to leverage the attack?

Who is most likely to attack us? Insider?

How will the attack us?

Increased Complexity and Risk

Potential Gaps with Traditional Security Operations:

- Correlate risks with degree of data sensitivity
- Appreciate the impact of users and identity protection
- Consider infrastructure outside of security
- Visibility into emerging threats
- Optimize resources for compliance
- Keep pace with changing landscape

Remote Employees

Partners

Customers

Endpoint

IP
no

S

Post Or

d Disk



Business
Analytics

Replica

SharePoint
eRoom, etc.

Disk
Arrays

Backup
Disk

INFORMATION ASSURANCE QUALITIES

Integrity	Confidentiality	Availability
Data stream could be intercepted.	Insecure e-mail could contain confidential information.	Files stored in personal directories may not be available to other employees when needed.
Faulty programming could (inadvertently) modify data.	Internal theft of information.	Hardware failures could impact the availability of company resources.
Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons.	Employee is not able to verify the identity of a client, example: phone masquerading.	A failure in the data circuit could prohibit System access.
Data could be entered incorrectly.	Confidential information is left in plain view on a desk.	Act of God - Tsunami/hurricane
Intentional incorrect data entry.	Social discussions outside the office could result in disclosure of sensitive information.	Upgrades in the software may prohibit access.

IDENTIFYING CONFIDENTIALITY REQUIREMENTS

What would happen if everyone knew about this information/system?

- It would seriously affect the way we do our job.
- It would impact us, but we could easily continue to do our jobs.
- It would not significantly impact the way we do our job.

What would be considered a confidentiality breach?

- If it leaked to an individual outside of a tightly restricted group.
- If it leaked to an individual outside of our company and partners.
- If it becomes widely known.

IDENTIFYING THE INTEGRITY REQUIREMENTS

What would happen if information/transaction/system were inaccurate or corrupted?

- It would seriously affect the way we do our job.
- It would impact us, but we could easily continue to do our jobs.
- It would not significantly impact the way we do our job.

How inaccurate can the information/transaction/system become before it causes issues (or can be caught by other means)?

- If it is in any way inaccurate, it is useless.
- As long as it is in the ballpark, then it is still useful.
- Its accuracy is not of paramount importance.

IDENTIFYING LEGAL REQUIREMENTS

Regulatory requirements

- CBK, Insurance, Privacy, CMA, NSE, ICT Authority, Communications Authority

Third Party requirements

- Contractual agreements, NDA etc..

Other internal or international agreements

Addressing User Security

**Who has
access?**



manage process

HOW

did you get access?



monitor

WHO

are you, really?



correlate

WHAT

are you doing?



consolidate

Broader, More Complete View



Fraud Risk Assessment



❑ Financial statements vs Cyber-risk Matrix

Balance Sheet

As of December 31, 2016 (000s)

Assets

Cash	481
Marketable Securities	1,346
Accounts Receivable	1,677
Inventory	2,936
Prepaid Expenses	172
Other Current Assets	58
Total Current Assets	6,670
Gross Value of Property, Plant & Equipment	2,019
Accumulated Depreciation	(664)
Net Property, Plant, Equipment	1,355
Note Receivable	349
Total Assets	8,374

Liabilities

Accounts Payable	625
Current Portion L-T Debt	1,021
Taxes Payable	36
Accrued Expenses	157
Total Current Liabilities	1,839
Long-term Debt	2,332
Total Liabilities	4,171

Owner's Equity

Common Stock and Paid-in Cap	194
Retained Earnings	4,009
Total Shareholders' Equity	4,203
Total Liabilities and Equity	8,374

What the Company Owns

What the Company Owes

Shareholders' Equity

Paul's Plumbing Co.

STATEMENT OF CASH FLOWS

January - September, 2016

TOTAL

OPERATING ACTIVITIES

Net Income	2,091.53
Adjustments to reconcile Net Income to Net Cash provided by operations:	
Accounts Receivable	0.00
Inventory Asset	-2,000.00
Accounts Payable	0.00
Bank of America Visa, x7421	300.00
Wells Fargo Credit Card	7,220.20
Total Adjustments to reconcile Net Income to Net Cash provided by operations:	5,520.20

Net cash provided by operating activities **\$7,611.73**

INVESTING ACTIVITIES

Truck	-10,000.00
Net cash provided by investing activities	\$ -10,000.00

FINANCING ACTIVITIES

Loan payable - Truck	10,000.00
Opening Balance Equity	2,255.99
Net cash provided by financing activities	\$12,255.99

Net cash increase for period **\$9,867.72**

Cash at beginning of period **5,500.00**

Cash at end of period **\$15,367.72**

Fraud Risk Assessment



Business Reporting

- What the company **OWNS** (Assets)
- What the organisation **OWES**
- Total **PROFIT** made that year
- How the organisation **COMPARES** with competitors
- **PROJECTIONS** in revenue

CURRENT _ IT/Security Reporting

- High **VULNERABILITIES**
- **TOOLS** needed by IT department
- **AUDIT** findings for the year

Fraud Risk Assessment



Business Reporting

- What the company **OWNS** (Assets)
- What the organisation **OWES**
- Total **PROFIT** made that year
- How the organisation **COMPARES** with competitors
- **PROJECTIONS** in revenue

IT/Security Reporting

- THE RIGHT APPROACH - FUTURE
- Visibility – **ASSETS**
- Exposure – **LIABILITIES**
- Profit – **GAINED VISIBILITY**
- Loss – **GAINED EXPOSURES**
- Cash Flow – **INCIDENT TRENDING**

Current State



Risk

Inherent Risk management

Technology

Processes

People



Controls

Controls management

Risk Management
(Anticipate Risks)

Vulnerability Management
(Detect Vulnerabilities)

Incident Management
(Respond to Incidents)

Threat Management
(Contain Threats)



Visibility



Deficiencies

visibility management



Exposure

Residual Risk management

Asset Controls	User Controls	Incident Controls	Continuity Controls
Asset Inventory	User Access Management	Incident Response	Performance and Availability
Configuration Controls	Privileged Access Management	Fraudulent Transactions	Operational Considerations
Vulnerability Management	Training & Awareness	Monitoring and Analysis	Disaster Recovery
Malware			

Fraud	IP Theft	Sabotage
Email Based Fraud	Data Breach	DDOS
Online Fraud	Hacktivist	Botnet
Wire Transfer	Extortion	Misconfiguration
Mobile Fraud	Domain Theft	Rogue Personnel



Incident Monitoring



Potential Loss

Fraud Risk Assessment



- Inherent risk incorporates the type, volume, and complexity of the institution's operations and threats directed at the institution. Inherent risk does not include mitigating controls.

Technology



- External connections
- Wireless connections
- Third parties
- Applications
- Asset inventory
- Channels
- External Threats

Process



- Mergers and Acquisitions
- Change management
- Policies



People

- Staffing
- Training
- Culture

Fraud Risk Assessment



The Cyber Visibility and Exposure Statement

The Cyber-Security Balance Sheet as at 31st March 2019

Overall Visibility						41.4%
Control Areas	Year	Existence	Completeness	Timeliness	Reporting	Visibility Score
Asset Controls						
Asset Inventory, Configuration Controls and Vulnerability Management Malware	Q1 2019	75%	50%	25%	15%	51.5%
	Q4 2018	50%	40%	35%	15%	40.5%
	Q3 2018	40%	30%	25%	20%	32%
User Controls						
User Access Management, Privileged Access Management, Training and Awareness	Q1 2019	75%	70%	55%	45%	66.5%
	Q4 2018	45%	35%	30%	25%	37%
	Q3 2018	50%	40%	35%	30%	42%
Incident Controls						
Incident Response, Fraudulent Transactions, Monitoring and Analysis	Q1 2019	65%	50%	45%	30%	53%
	Q4 2018	55%	40%	35%	35%	44.5%
	Q3 2018	60%	50%	45%	30%	51%
Continuity Controls						
Performance and Availability, Operational Considerations and Disaster Recovery	Q1 2019	60%	53%	50%	40%	53%
	Q4 2018	78%	76%	50%	45%	62.8%
	Q3 2018	40%	35%	35%	20%	35.5%

Legend:

■ Low Visibility - 0%-25% |
 ■ Minimal Visibility - 26%-50% |
 ■ Moderate Visibility - 51%-75% |
 ■ High Visibility - above 75%