

Managing the Perfect Storm for Fraud

Presented by:

Robert J. Rufus, DBA, CPA, CVA, AFI, CFF

The Perfect Storm for Fraud

Three forces in play:

- Advanced Technology --
Electronic Commerce
- Economic downturn
- Widening Gap Between
the Haves and Have-Nots



What is Risk?

Probability



Consequence

- Algebraically, risk can be defined as

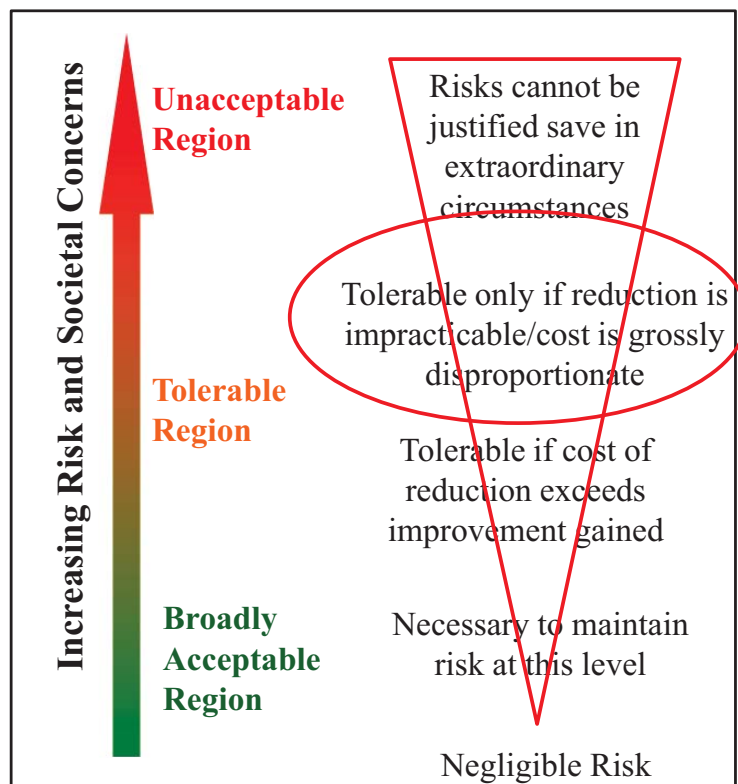
$$\text{Risk} = f(\text{probability}, \text{consequence})$$

- Risk equals the product of probability (P) and consequence (C), often expressed as

$$\text{Risk} = P \times C$$

What is Risk Tolerance?

- Commonly defined by three regions
 - **Intolerable Risk region, where action is required**
 - **As Low As Reasonably Practicable (ALARP) Region, where action is desired if economical**
 - **Broadly Tolerable Region, where no action is required**



Using Risk in Decision Making

- Basic Truths
 - There are risks with all operations.
 - Past performance is no guarantee of future success.
 - There is no such thing as “ZERO” risk; always residual risk.
 - \$ Risk control comes at a cost.
- Risk Mitigation Actions
 - Risk reduction - usually by lowering the probability
 - Risk elimination - usually by more inherently safe processes

Managing Fraud Risk (Cybercrime - Payments Fraud)

- Online fraud involves deception
 - It’s about tricking the system...
 - A transaction appears authentic when it is not
- Breach of information security
 - Failed preservation of confidentiality, integrity and access to information
- Most significant risks
 - Loss of reputation with customers and taxpayers
- 70% of all organizations have experienced payments fraud

Data Breaches

Who ?

- 70% by external agents
- 48% by insiders
- 11% implicated business partners
- 27% multiple partners

Data Breaches

How ?

- 48% privileged misuse
- 40% hacking
- 38% malware
- 28% social tactics
- 15% physical attacks

Data Breaches

Commonalities ?

- 98% of data breached came from servers
- 85% of attacks not considered highly difficult
- 61% discovered by 3rd party
- 86% had evidence of breach in log files
- 96% avoidable through simple controls

Data Breaches

Demographics ?

- Financial Services = 33%
- Hospitality = 23%
- Retail = 15%
- Manufacturing = 6%
- Technology Services = 5%
- Business Services = 4%
- Government = 4%
- Healthcare = 3%

Forensic Tools and Techniques:

1. Proactive Fraud Detection Monitors
2. Analytical Techniques and Data Mining
3. Proactive Employee Management

Proactive Fraud Detection Monitors

- Quest for transaction validation
- Monitoring system designed to identify high-risk activities in real-time
 - Detects, analyzes and scores each online transaction
 - Runs background server-based processes
 - Compares this information with a profile – normal behavior
 - Stops the transaction if actual behavior is too far out of the usual range of what is expected
 - Follow up – re-authenticate

Analytical Techniques and Data Mining

- Digital analysis using Benford's Law
- Joining diverse sources
- Duplicate testing
- Data mining / phishing – extracting patterns

Proactive Employee Monitoring

- Hiring – don't hire criminals
- Training – mindset, ethics, operational processes
- Monitoring – attitude and morale

Audit v. Forensic Audit Techniques

- Timing – regular v. nonrecurring
- Objective – overall opinion v. likelihood or magnitude of fraud
- Sufficiency – reasonable assurance v. support / refute allegations
- Audience – public v. engaging party

