Fraud Prevention

A Strategic Approach to Minimizing Fraud Risk

The risk of business fraud today is higher than ever. The main contributing factors are the growing complexity of organizations, emerging technologies, and evolving accounting practices, which combined, make it challenging for businesses to monitor the increasingly sophisticated fraud tactics of criminals.

Why Fraud Prevention should be viewed as a Strategic Corporate Activity

Today, criminals are targeting commercial businesses for various types of fraud, knowing that many companies are increasingly vulnerable. The following presents fundamental and compelling reasons why fraud prevention and detection requires a strategy with a full set of policies and procedures.

Fraud is more common and easy than you think:

- 60% of organizations were exposed to actual or attempted payments fraud in 2013[1]
- 27% of financial professionals that experienced payments fraud in 2013 report the number of fraud incidents increased from 2012[1]
- 82% of survey respondents report that cheques were the primary target for fraud attacks at their companies[1]
- The typical financial loss incurred by companies due to payments fraud in 2013 was $23,100[1]
- Internal accounting fraud, or otherwise known as defalcation, is the misappropriation of cash, supplies, inventory or other tangible property from within the business by its employee(s), or other acting partners
- Data theft/fraud occurs when one obtains business information without consent to commit fraud for financial gain or for other criminal purposes, such as leaking business information, which can lead to indirect monetary losses
- Other common methods of fraud are deposit fraud, transaction instruction fraud, and payroll fraud, among others

Fraud has more than just the financial costs:

- Impact on reputation
- Management time and loss of morale
- Erosion of trust within teams

Fraud happens close to home:

- 85% of the most serious fraud incidents are committed by company insiders[2]
- Over half of the perpetrators are from management ranks[2]
- One in five North Americans are personally aware of co-workers stealing from their employers[2]

Elements of a Fraud Prevention Strategy

Corporate Policies:

Many corporations have already implemented formal fraud prevention policies. Strategies for dealing with fraud range from codes of Corporate Governance to Employee Conduct Policies, including a whistleblower hotline.

Implementation and Education:

Issuing a policy by itself is insufficient. Employees need to be educated and held accountable to these guidelines or their behaviours are unlikely to change. Risk of discovery becomes a meaningful deterrent.

Internal Controls:

More often than not, an internal control, which should have prevented or detected fraud, was either overridden or misunderstood by staff responsible for the control. Internal process controls and limits must be specified as well as methods implemented to ensure accountability and compliance with these controls.

Implementing a Fraud Prevention Program

It is essential to understand not only fraud risk, but also the tools and risk management practices available to control fraud risk and reduce it to an acceptable level. Interestingly, aside from internal/external audits and internal controls, fraud is often detected by accident or through employee, as well as customer, vendor, or anonymous tips. Finally, perhaps the most effective control against fraud is to *ensure that people know that they will be caught*.

Documented Procedures:

A Procedures Manual or Desk Book derived from a Corporate Risk Policy can help organizations define and implement daily treasury activities. The activities include daily responsibilities, controls, and management reporting.

Clear Segregation of Duties and Responsibilities:

Defined segregation of duties and responsibilities enable the organization to ensure no single person controls all or multiple segments of a process, which can increase the potential for fraud.

Restrict Physical Access to Documents and Information:

Documents and information (e.g., cheque stock, lists of authorized cheque signers, specimen signatures of signers, procedures for operating cheque printing equipment) should be maintained in a restricted location.

Limit Physical and Technical Access to Systems:

In addition to restricting access to documents and information, physical and technological access to systems should be limited. Treasury should designate security administrators responsible for granting individuals access only to modules needed to perform their duties.

Best practice organizations may also review fraud risk exposure in the following areas:

- Timely bank account reconciliation and resolution of discrepancies
- Independent audits of payment process and transactions
- Disaster recovery plans
- Defined internal payment request procedures
- Employee hiring practices

Payment Solutions that Help Stop Fraud

Electronic Payment Solutions (e.g. CIBC's Cash Management Online)

- Eliminate the fraud opportunities that cheque payments create, by moving from detective to preventative capabilities

"Positive Pay" and "Positive Pay Plus"

- Cheque issuing files are sent to the bank daily, and as cheques arrive for clearing they are reconciled with the record of cheques issued, and then items not found on the issuing file are held for instructions

Corporate Clearing

- Provide daily notifications of items clearing against your accounts
- Reduce risk by accelerating the time between clearing and reconciliation

To get started:

- Come see us; if you need further information regarding fraud prevention, and how to protect your business, your CIBC business advisor is here to help. We can help make sure that you have the adequate fraud policies, procedures, checks & controls in place to counter any fraudulent criminal activity
- Review the contents of *Top 10 Ways to Avoid Cheque Fraud*, which can be found on cibc.com at http://www.cibc.com/ca/commercial/business-insights/avoid-cheque-fraud.html
- Remember, CIBC offers a variety of products and services that can help businesses reduce their exposure to external and internal fraud risks. Chief among these are electronic payments tools and positive pay chequing

For more information, talk to a CIBC business advisor, visit your nearest branch, call 1 800 465-2422 or visit www.cibc.com.

[1] J.P. Morgan. 2014 AFP Payments Fraud and Control Survey. https://www.jpmorgan.com/cm/BlobServer/2014_AFP_Payments_Fraud_Survey.pdf?blobkey=id&blobwhere=1320639355606&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs

[2] Ernst and Young. Fraud: The Unmanaged Risk. http://208.254.39.65/ernst/global_fraud_survey.pdf