



Special Edition!

CRIME LOSSES – Who will be Next?



In a survey conducted during 2003 in the United States, about 50% of corporate Chief Executive Officers (CEO's) and other executives contend that accidental discoveries of fraud are just as likely as discoveries made by internal or external auditors. The prevention

strategies that were deemed to be the most effective included:

- **risk management programs focusing on financial risk identification;**
- **tips from outside and inside sources;**
- **well trained and capable management**

in number of claims occurring since 1998. This is combined with a dramatic 10-fold increase in the average cost of each of those claims in the same period. Since 1992, OSBIE has paid out more than \$2.5 Million on more than 80 claims involving thefts or misappropriation of funds, security or property by employees and volunteers.

According to Statistics Canada, the overall crime rate in Canada has been steadily declining over the past 10 years. However, OSBIE's Crime claim experience for employee dishonesty does not seem to be following the national trend, with an overall increase in yearly claims frequency (number of claims per exposure unit) of 67% from 1992 to 2003, with the sharpest increase

This Special Edition of the Oracle is dedicated to identifying and explaining the risks school boards face and to promote an awareness of the need for effective risk management strategies to curb the dramatic increase in claims activity that has been observed in the past few years.

David Beal,
Risk Manager

**Crime Claim Analysis
Claims by Loss Category
(1991-2003)**

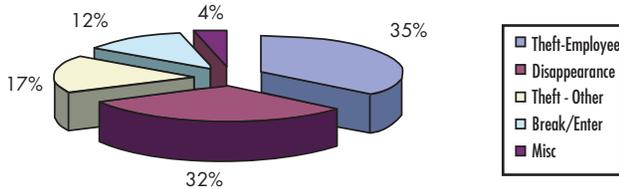


Exhibit 1



(1) Risk Identification - Where Are Your Crime Risks?

Based on Exhibit 1, for the period 1991-2003, approximately 2/3 of the Crime claims originate from two Loss Categories - Employee Theft / Misappropriation of cash and Mysterious Disappearance of Cash and board property. The latter category consists of high frequency low severity losses, as illustrated in Exhibit 2 - the losses in this category mostly involved small amounts of petty cash (such as school fund raising proceeds) or

the use of school funds to purchase personal items.

By far, the category of most significance, from both a frequency and severity standpoint is the Employee Theft, as supported by Exhibits 1 and 2. The losses in this category include large scale pre-meditated and fraudulent actions by employees, and a further break down of these loss categories is provided in Exhibits 3, 4 and 5.

**Crime Claims Analysis
Incurred Costs by Loss Category
(1991-2003)**

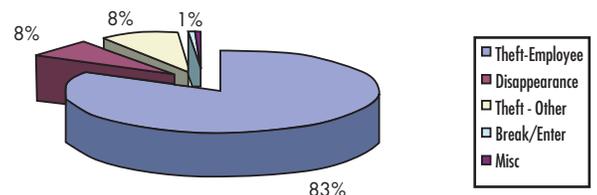


Exhibit 2

Continued on page 2...

(2) Risk Analysis - Employee Theft

Although the other categories of Crime losses are of significant concern, it is evident that a reduction in the Employee Theft category can provide the most immediate benefit to a school board.

A further analysis of this category provides a breakdown of these losses into sub-categories, as illustrated in Exhibits 3, 4 and 5.

The Comparative Analysis provided in Exhibit 5 provides an indication of the categories of loss which would benefit the most from focused risk management strategies. The following 4 categories would attract remedial risk management strategies:

- **Misappropriation of Funds**
- **Payroll (fraud)**
- **Theft - Cash**
- **Theft- Property**

The first 2 categories listed would be losses that would be characteristic to the school board office

administration environment, where employees have access to the administrative instruments (computer systems, signing/funds transfer authority, budget and payroll, tender processes, cash disbursements, etc.). The risk management strategies for these risk exposures are described in the following section, and are different than what would be effective for the second two sub-categories of losses.

The second two sub-categories of losses (Theft of Cash/Property) would be more likely associated with a school-based environment, where small amounts of petty cash or board owned property/equipment would be present. These types of losses are usually characterized by a high number (frequency) of low value (severity) losses. The risk management strategies for this group would focus on different elements of risk than what would prevail in a "corporate" or administrative environment.

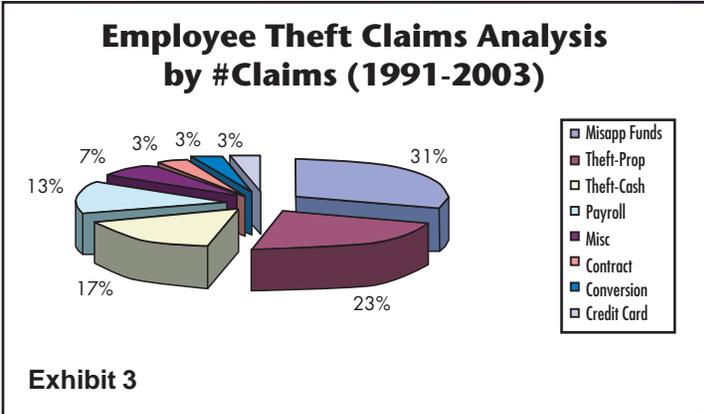


Exhibit 3

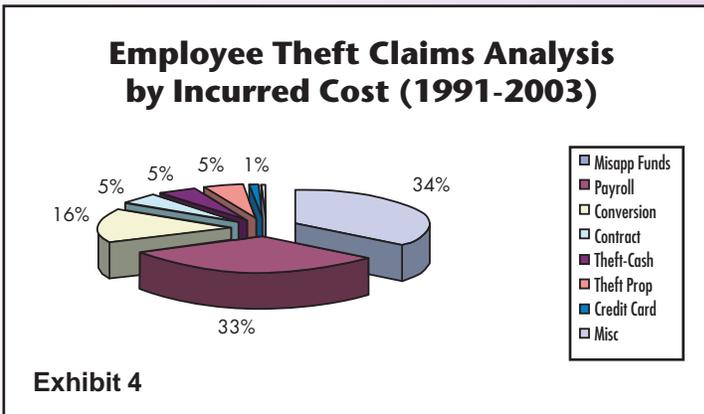


Exhibit 4

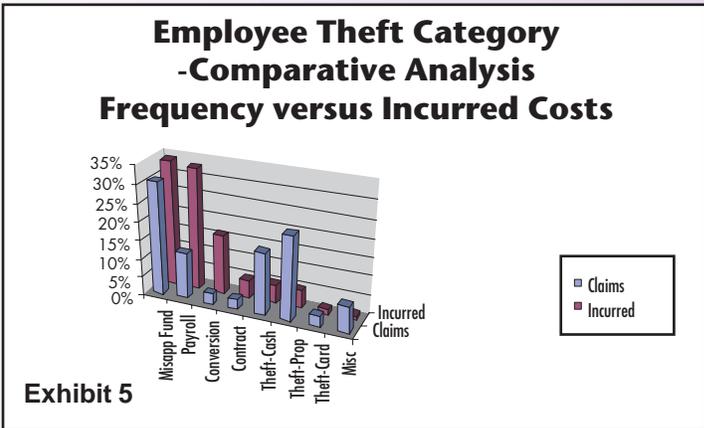


Exhibit 5

(3) Risk Strategies

(a) Corporate/Administrative Risks:



The risk strategies for employee crime associated with the corporate/administrative environment would be aimed at the following elements of risk, including but not limited to the following:

- the presence or absence of checks, balances and monitor-

ing functions that would identify the risks present for each administrative function;

- avoid high risk circumstances, such as policies and procedures where it is common practice for unaccompanied employees to

handle or transport large amounts of cash or bearer type securities off premises;

- the presence of policies and procedures that select and control the necessary risks;
- segregation of decision making

authority/access to financial systems (electronic or manual), inventory or contracts; and

- staff hiring practices and appropriate compensation programs.

Continued on page 3...

(3) Risk Strategies (Contd.)

The following risk management recommendations can reduce a school board's exposure to fraudulent actions by corporate/administrative employees:

- Computer security – restrict global access to computer systems (segregated passwords limiting access to job-specific tasks/functions/data), “no-share” policy for passwords, frequent password changes. As school boards use different types of computer systems for various financial functions, it is difficult to provide one set of recommendations that are applicable to all systems. However, involving Information Technology specialists in the process of an annual risk identification exercise can isolate weaknesses or fraud risks that are unique to each type of computer system.
- Segregation of duties – dual signing authority on cheques, disbursements, electronic funds transfers; separate duties between staff approving payments and staff producing cheques or enacting the transaction;
- Procurement Practices – Policies and procedures for awarding tenders, RFP's or contracts should be reviewed to ensure that committees are used, that the criteria set by the board are relevant to the local situation (e.g. size of contract, construction vs purchase of supplies, etc.), and that these criteria are being followed, with proper documentation to support the procedure. No employee should be solely responsible for the selection and awarding of contracts or tenders, and members of selection committees should not have sole authority over producing cheques or payments for awarded tenders or contracts.

Procurement practices should be included as part of both internal and external audit programs.

- Staff issues – regular rotation of financial duties, spontaneous internal and external audits, monitor excessive staff vacation accumulation, monitor sudden changes in staff lifestyles (frequent trips, frequent large purchases, extensive or luxurious home renovations, expensive vehicles, frequent gambling excursions, etc.), monitor staff references to personal financial difficulties, etc.

- Adopting generally accepted principles for managing financial functions.
- Establish policies and procedures that address hiring practices – employee screening, back ground checks, previous employer references, etc.
- Competitive salary/compensation package.

(b) School-based Risks:

Although the possible size of loss occurring at the school level is gen-

erally lower than what could occur at the board administration level, the risk exposures for employee crime associated with the school environment are still quite significant. School staff and volunteers frequently handle cash from fund raising and sporting events, and without proper cash handling procedures and supervision, the risk of a loss is significant to the school. The following sample cash management procedure can be effective in reducing the exposure to this peril in a school environment:

SAMPLE CASH MANAGEMENT PROCEDURE FOR SCHOOLS:

- (1) A bank account must be set up for Fund Raising Activities;
- (2) All bank accounts will have at least two signing officers at the school level, one of whom must be the principal;
- (3) All bank accounts will be in the name of the school, with the account referenced with the name of the activity involved;
- (4) Schools will maintain a suitable ledger showing all activity in each bank account, with reconciliation to school records at least monthly, initialed by the principal to signify approval;
- (5) The principal of each school will submit a copy of all bank statements and a full reconciliation of all accounts to their respective Superintendent of Schools on June 30th and December 31st of each year;
- (6) The principal of each school will submit a copy of all bank statements and a full reconciliation annually to the appropriate representatives of all School Advisory Committees for those accounts involving fund-raising activities;
- (7) Schools will keep on file all cancelled cheques (unless held or kept by the respective banking institution), and copies of all deposits and related information for audit purposes.
- (8) Internal Audit programs should include school fund raising accounts and school cash management procedures.

The preceding is a simplified sample of a cash management system. Schools should consider adopting the “*Guidelines for School Generated Funds*” document developed by the Ontario Association of School Business Officials (OASBO). This document provides more specific procedures for each of the various scenarios under which schools may be handling the proceeds from fund raising activities.

For further information, or to obtain copies, contact OASBO on line at: www.oasbo.org

WHEN EMPLOYEES STEAL FROM THE COMPANY



Employees embezzle from organizations for many reasons—gambling debts, an expensive lifestyle, shopping addiction, blackmail. Some even feel they must augment an inadequate income by pilfering from the employer. And the methods can be as varied as the motivations:

- A payroll supervisor uses her computer expertise to manipulate temporary employee data so that tax rebates from source deductions go into her personal bank accounts.
- A shop teacher at a high school uses building materials and other board of education resources in his private construction business, and sells class-built projects and excess building materials for his own profit.
- A financial manager uses the company's cash, petty cash, credit card and vendor accounts for personal purchases.

Risk management and loss control

Employers may not be able to prevent all such theft, but they can make it harder for staff to steal, and thereby minimize the chance of having to file a fidelity claim.

The most fundamental risk management strategy is to make sure that employees are treated with respect and fairness, and are adequately paid so that they do not feel compelled to steal. Management should set an appropriate ethical example for staff to follow.

Basic internal controls are the next line of defense:

- Check the credentials of all new vendors and periodically review vendors to identify improper

eties. You have to be concerned with bribery, illegal gratuity, conflicts of interest and false or inaccurate statements.

- Verify all new employees—consider criminal background checks and be sure to check references, prior employment and reasons for leaving, if there have been many employers in a short time.
- Make sure that your systems are designed so that one person doesn't have complete control over finances—segregate such duties among key personnel. Movie theatres are an example—one person sells the ticket, another person col-

lects it. Fast-food drive-throughs are another—one person collects the cash, another fills the order. The person who collects the money should not also be the person who prepares the bank deposit and then reconciles the bank statements.

Watch for red flags, and encourage other workers to do this as well. Such tip-offs include:

- Driving a very expensive car that is not proportional to income from employment
- Talking about going to the casinos all the time
- Discussing triactors, quinellas,

exactors—all suggesting numerous trips to the racetrack

- Taking a taxi to and from work every day
- Wearing a \$25,000 Rolex watch
- Expensive home, clothes, habits
- Never taking a vacation and routinely working long hours
- Never delegating or sharing duties.

Remember, though, that red flags are not proof of dishonesty—there are often explanations, such as inheritances or gifts.

WHAT TO EXPECT IF YOU HAVE A CLAIM:



As the employer, you will be interviewed and expected to provide the following information in the event of a fidelity claim:

- Name and position of the suspected dishonest employee (the "principal")
- Date, time and circumstances of the discovery of dishonesty
- Your operations as they pertain to the loss—how is business conducted?
- Records and documentation—how did the employee allegedly steal the money or property, what safeguards were circumvented?
- Present employment status of the employee—terminated, resigned, suspended, still active
- Employee's reaction to the allegations

- Employee's lawyer, if any (name, address, phone number)
- Witnesses to the theft—name, location, time
- A copy of the employee's employment folder
- A copy of any notification given to governing bodies, such as the Ontario College of Teachers or the Certified General Accountants Association
- Known financial status of the employee—real and personal property, assets versus liabilities, lifestyle
- Present whereabouts of the employee
- Community and family ties—married, single, divorced, separated
- Other known employment of the employee (such as part-time jobs)

- Is there other insurance? If so, types, limits and names of other companies
- Recoveries, if any—refund or partial refund, returned goods, vacation pay, back pay, service gratuity.

A blank proof of loss form will be provided to you. The adjuster will not complete the form. You may get assistance if you do not understand the form itself, but you—the employer—will be accusing the employee of theft. The insurance company and the adjuster will not make any accusations against any employee.

After the proof of loss is submitted, the adjuster may contact the employee or his lawyer to get their comments on the proof submitted. The employee is given the

Continued on page 5 ...

CASE STUDIES



Based on the premise that we learn best by example, the following employee crime cases are taken from actual OSBIE claims files. These are only two examples of the many cases that may not have occurred if the risk of this type of loss were acknowledged, and more vigilant risk management strategies had been in place.

WHAT TO EXPECT IF YOU HAVE A CLAIM.

...from page 4

opportunity to comment on the claim. Sometimes, the employee confesses and agrees regarding the amount; sometimes, the employee can explain part of the claim; and sometimes, the employee denies everything.

Usually, if the claim is covered, the insurance company makes payment and has the legal right to pursue the employee in civil court.

Luis Copat is a Surety & Fidelity Specialist in Crawford Adjusters Canada's Technical Services Division.

Crawford Adjusters Canada is a wholly owned subsidiary of Crawford & Company.

Luis Copat, BSc, FCIP
Crawford Adjusters Canada

CASE # 1

– Woman Steals \$182,000 from School to Feed Gambling Addiction

In this case, an accounts clerk at a school was caught after an audit of the school's bingo lottery revealed that more than \$182,000 was missing from the school fund raising account. The loss was spread over a two year period, and the investigation found that the clerk was creating fictitious deposit slips and cheques to cover up the theft.

During the investigation, it was revealed that the stolen funds included bingo proceeds, as well as fees paid by students for activities and year books, funds raised by the school band, computer club and various teams. The clerk admitted that more than \$25,000

of the total funds stolen were used to feed a gambling addiction. After an investigation by the Ontario Provincial Police's Alcohol and Gaming Commission branch, the clerk was fired from her position and was charged with stealing the funds. She pleaded guilty to the charges.

In analyzing the elements of risk that prevailed, it was clear that the school would have benefited from the following risk management strategies:

(1) A proper cash management procedure, as outlined in an earlier section of this publication, would have required the principal (or a designate) to provide a periodic reconciliation of the account to the Superintendent of Schools. This could have served as both a deterrent and a detection strategy. The lack of a periodic financial reconciliation process, in this case, enabled the

fraudulent employee to continue stealing for prolonged periods of time without being discovered.

(2) Conducting a periodic internal audit could have acted as both a deterrent and detection factor, as it sends a clear message that all financial transactions for the school are being monitored, as well as increasing the "risk" of discovery for any dishonest employee/volunteer who may attempt to test the system that is in place.

(3) The need for a segregation of duties requiring the principal or some other authorized person to co-sign cheques and validate/reconcile deposit slips to the account would also have been beneficial in this situation. These missing factors enabled the employee to have complete control of the entire financial process without being subject to scrutiny from an objective party.



CASE # 2

– Payroll Fraud Exceeds \$500,000 Policy Limit

In this case, over a 6 year period, an employee diverted more than \$690,000 from the payroll system using dormant employee records into bank accounts that he controlled.

He first selected 3 temporary employees who had no current earnings, but who were still active on the system, and who would have submitted time sheets in the past. This created the appearance of legitimate payroll activity in the board's computer system.

Using the User ID and password "borrowed" from his supervisor (he was not authorized to access

the payroll system under his own), the next step was to change the names and Social Insurance Numbers (SIN) for the dormant employees, and set up the electronic funds transfer to divert the funds into his own bank accounts. Computer or paper records leading back to the offending employee were deleted periodically to reduce the chances of tracing the deposits to him as the owner of the bank accounts.

Each payday, using the borrowed User ID and password, the employee would access the payroll records and make a change that resulted in the reduction of income tax

being deducted from the employee's gross earnings. Since the "employees" had no gross earnings, and no income tax payable, the appearance was that the "employees" were receiving a tax refund. The bi-weekly pay slips were intercepted by the fraudulent employee, so the unclaimed slips did not attract attention.

At the end of each year, again using his supervisor's User ID and password, he deleted the transactions that had been posted to alter the "phantom employee" payroll files, leaving no electronic record of the transactions.

To further cover any trace of the fraud, the unscrupulous employee

Continued on page 6...

... from page 5

CASE #2 Payroll Fraud ...

who was responsible for preparing the annual reconciliation of T-4 forms for the Canada Customs and Revenue Agency (CCRA), adjusted the annual amount of the board's Employment Insurance contributions, and then deleted the transactions. Although discrepancies began to show, they were unexplainable, as the supporting transactions for these adjustments were deleted from the computer system.

Over the six year period, the unresolved discrepancies continued to grow, but the employee was able to successfully explain or defer any reconciliation, and had rationalized some of the discrepancy as being the product of a school board amalgamation that was ordered by the Ministry of Education and Training during the late 1990's.

The fraud was finally discovered accidentally when a senior Information Technology (IT) employee was running some routine system checks which took place at the same time the fraudulent employee was in the process of one of his computer "adjustments". The routine system check was run before the correcting adjustment could be made, and this raised a red flag when an out-of-balance situation was observed. The IT person referred it to a senior staff member, who then confronted the individual, who then admitted to the fraud.

LESSONS LEARNED:



Although no computer system or internal process can be made 100% secure against the fraudulent activities of a determined employee, some lessons can be learned from this case that may prevent or lead to early discovery of an employee's manifest intent to commit fraud:

- (1) The unauthorized use of a supervisor's Computer User Identification and password allowed the unscrupulous employee the access to the payroll system, which enabled him to commit his crime, and then to delete any record that would have led to the discovery of the fraud.
- (2) Computer access and User ID's should be restricted to specific functions within any computer system. Staff at all levels need to be aware that their computer access codes/passwords are security features, and school board policy should prohibit staff from sharing, lending or borrowing computer access codes.
- (3) The discrepancy between the Employment Insurance deductions and the remittance to CCRA had been observed and allowed to be carried over for a number of years based on the fraudulent employees' misleading explanations.

Although account discrepancies are common in the early stages of any financial reconciliation process, they are usually the result of employee error, which are quickly corrected. However, the practice of allowing these discrepancies to be carried forward without proper investigation and resolution leave an organization open to employee fraud, as there is an implication that management will not investigate.

- (4) The employee had control of a financial process from the beginning (setting up employee files on the payroll system to deposit funds to an account) to the end (reconciliation of any unbalanced disbursements or remittances to CCRA).

Segregation of financial duties has long been proven to discourage the opportunity for fraudulent activities, as the more individuals that must be involved in the completion of a financial transaction, the more difficult it becomes to achieve collusion between those individuals, or to preserve the secrecy of any fraudulent acts.

The O.S.B.I.E. Oracle is a publication of:

The Ontario School Boards' Insurance Exchange
91 Westmount Road. Guelph, Ontario N1H 5J2

<http://www.osbie.on.ca> Editor: David Beal (E.& O.E.)