A hidden threat to any business

Someone breaking into your premises or stealing goods at knife point is an obvious threat to any business. But as claims reported to Guild Insurance show, they are not the only crimes occurring.

Case 1

When a trusted employee was away on leave, her replacement noticed some anomalies in payments made to contractors. A number of invoices didn't match up. Although the business name was the same, the layout of the invoice and the style of the font were different. There were also instances of two invoices for the same amount. Further investigation revealed different bank accounts for the same contractor. The Police were notified when it was discovered that the employee had been using company bank accounts to pay her personal bills of over $40,000.

Case 2

An employee was found to be stealing stock from the business in which she'd worked for many years. Subsequent investigation revealed she then sold the stock through an online business. She went to considerable lengths to systematically steal from her employer by using her unrestricted access to the building to install spyware and remote login software on a number of computers. It's alleged she used this software to login into the computer systems from her home and make unauthorized changes to business records. She was also found to have falsified other documents, such as logbooks and transaction receipts.

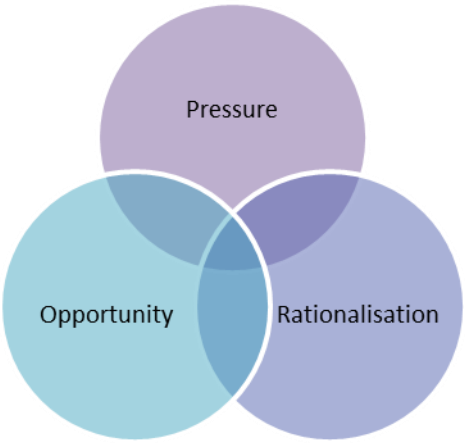
Case 3

A trusted employee used the Point of Sale (POS) system to divert the proceeds of sales back to her own credit card. In an effort to cover her tracks, she would report that some credit card receipts had been inadvertently misplaced during busy periods. Because she had volunteered the information, no one thought to investigate further. To make things worse, while the business did have CCTV directed towards the service counter, recordings were not retained. Footage was taped over every 24 hours.

While people are alert to the threat of crimes by strangers, many underestimate the risk of theft by employees. When it comes to security measures, successful businesses take steps to address both.

Employee dishonesty, or fraud, can be hard to manage as it's less obvious than a burglary or robbery. People who commit fraud make a conscious effort to deceive the business by concealing their activities. They avoid detection by making sure everything seems normal on the surface, while they are systematically stealing cash, stock or other items. Unfortunately by the time the theft has been noticed, some businesses have lost hundreds of thousands of dollars.

Three things are widely recognised as giving rise to fraudulent activity.



a) **Pressure** – mounting debts or other financial pressures in a person's life can motivate them to do things they wouldn't normally do, such as steal from their employer.

b) **Opportunity** – a work place that doesn't have systems and processes to protect against dishonest behaviour presents an ideal opportunity for fraud.

c) **Rationalisation** – individuals can easily justify their actions with beliefs such as … It's just a loan, I'll pay it back as soon as I can, or … I deserve something extra, no-one appreciates how hard I work.

While it can be difficult for employers to reduce the financial pressure employees' face, all businesses can take steps to reduce the opportunities for fraud.

Protecting your business against fraud

1. Don't fall into the trap of thinking it won't happen to you

It's tempting to believe that ***your*** people and ***your*** business are different to those in the case examples. After all, you've invested so much in developing a culture of trust.

While trust is important in any working relationship, it doesn't protect against fraud. People who commit fraud often conceal their activities by appearing reliable and trustworthy. That way, supervisors are less likely to keep a close eye on what they're doing.

2. Protect against fraud by establishing systems and processes

There are many things businesses can do to reduce opportunities for fraud. Work with your accountant to ensure you have the right measures in place. Ideas include but are not limited to:

- Ensure reconciliation of financial transactions is incorporated into daily work practices. For example, checking that 'sales' totals match with cash, cheque and EFTPOS receipts. Similarly, always reconcile bank statements against the figures recorded in the business' financial records.
- 'Separation of duties' is essential for combatting fraud. It's about putting the right checks and balances in place so that no one person has complete control over a single process. EG:

  While Kate is responsible for paying suppliers, she is unable to enter the supplier's details in the computer system. That way, she can't divert payment to another bank account by altering the supplier's details. Similarly, while Tran is responsible for entering supplier details into the system, he has no access to the payment process.

- Step by step procedures for key business practices, such as accounts payable, are a must. Good procedures help people to know what's expected of them while providing a baseline for monitoring business performance.
- Commit to good recruitment practices including background checks for new employees.

3. Lead the way – zero tolerance to fraud

The right work place culture is also needed to limit the chance of fraud. Owners, managers and supervisors must role-model desired behaviours and have a visible presence in the business. If they're not vigilant, no one else will be.

- Following fraud prevention procedures should be non-negotiable. Make sure it's reflected in everyone's induction, ongoing training and regular feedback. Periodically audit compliance – don't wait for something to go wrong.
- Often other people in the business know that dishonest behaviour is occuring. Establish an appropriate 'whistle blower' mechanism for staff to report any concerns. And ensure all employees have access to adequate support programs.

Finally, be on the lookout for suspicious or irregular activity such as:

- an invoice price differs from the amount approved for purchase
- lost receipts for credit card transactions
- negative inventory entries
- unauthorised bad debt write-offs
- excessive employee overtime
- unexplained access to buildings or systems

4. Regularly review all security measures

- Increasingly security measures require employees to have keys, access codes and IT system logins. But unless businesses are vigilant in managing these, security may be compromised rather than strengthened. Don't ever use generic logins or access codes.
- Invest in reputable security software (firewall, antivirus and antispyware). Access the Australian Government's **STAY SMART ONLINE** website for a free 'alert service', self-assessment tools and practical tips for protecting your business. **http://www.staysmartonline.gov.au/business**
- Cash should only be held overnight if an appropriate safe is available. Consider installing a quality 'cash safe' that complies with Australian Standards and is fitted by a licensed installer. The Australian Security Industry Association Limited (ASIAL) has information about the licensing requirements for each state or territory.

For further information on securing your business, please contact your Guild Insurance Account Manager on 1800 810 213.