Fraud awareness is everyone's business

What you don't know can hurt you

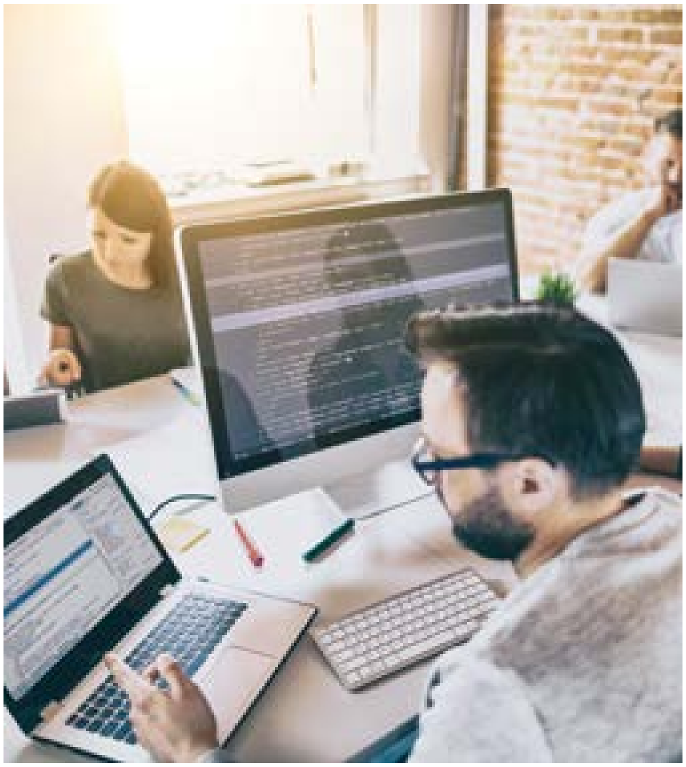
Did you know?

The average organization loses five percent of its revenue annually to fraud—for a median loss of USD $130,000 per case[1], according to the Association of Certified Fraud Examiners. Beyond taking a toll on your company's bottom line, this can damage your culture, reputation and even your ability to keep operating.

Raising the level of fraud awareness within your organization can help you identify potential risky behaviour down the road and safeguard your profits.

At Grant Thornton, we work alongside Canadian businesses of all sizes, and across all industries, to help them identify—and mitigate—the risk of fraud.

In this article, we outline what you need to know about both external and internal fraud and offer practical takeaways to help protect your business. You can reach out to our advisors at Grant Thornton to help ensure you're on the right track as you implement these steps.



What you need to know about **external** fraud

There are various types of fraud you may or may not have heard about, including cyber fraud, ransomware, data theft, banking malware and business email compromise, which we outline here.

Cyber fraud: According to the Canadian Anti-Fraud Centre (CAFC), cyber fraud is considered "any false, deceptive, misleading or fraudulent act that potential victims may come across while using the internet."[2]

Ransomware: Also known as "cyber extortion," ransomware penetrates a company's computer systems and encrypts a company's data. The fraudsters then demand a ransom from the affected company in exchange for access to its computer systems. Sometimes, the criminals will threaten to release the data to the public if the company fails to comply.

Data theft: Beyond stealing actual cash, fraudsters also target your data. This data can include

- financial information they can use to commit secondary fraud;
- proprietary data they can sell to a competitor; or
- personal confidential information (e.g. health records, social insurance numbers of your customers or employees, financial accounts, passwords) which they can sell
- on the dark web to identity thieves.

Banking malware: This type of fraud occurs when sophisticated cyber criminals target your bank's online banking facilities— essentially hijacking the connection between an online banking user and the bank. After logging into your banking portal, you'll come across a page that looks like your bank's website when, in fact, it's a replica being managed by criminals on the back end—allowing them to steal your passwords and information.

Three ways to protect your company from external/cyber fraud

1. **Install and maintain a robust, commercially -available anti-virus, anti-malware software program.** While it won't cover everything, it should catch at least a reasonable number of threats.
2. **Password protect everything.** Your servers, VPNs, email accounts, routers—virtually everything connected to the internet—should be protected with a secure password, not the default password which came with the product when purchased.
3. **Boost staff and management awareness.** All of your staff should learn how to identify common forms of cyber fraud and protect the personal information they share on social media.

Business email compromise (BEC): Also known as CEO or CFO email scams, this type of fraud usually targets senior employees of a company. The FBI reports that BEC scams cost companies more than $1 billion in losses in 2016.[3] Hiding behind a fake—but very real-looking—email, thieves request an urgent wire payment from the user. More recently, they have even begun claiming that a known supplier has changed its banking information—and then inserting their own account details instead. When the next payment is sent, it goes to the thieves rather than the supplier.

RED FLAGS

If you receive an email request including payment instructions, verify the details independently. Email instructions are not sufficient authority on their own to support payment, processing and protect you from fraud.

RED FLAGS

If you receive a request from a vendor to change their payment details and you notice an increase in change orders, or if vendors you don't recognize are submitting invoices, verify the activity with the actual company—either over the phone or face-to-face—as soon as possible. Review your internal controls and payment processes regularly and make sure they rigorously protect your business.

What you need to know about **internal** fraud

Internal or occupational fraud is fraud committed from within an organization's walls and can be divided into three primary categories: asset misappropriations, corruption and financial statement fraud.

Asset misappropriation: Asset misappropriation accounts for 89 percent of internal fraud that's been reported,[5] and occurs when individuals responsible for managing valuable business assets choose to steal them. In this instance, "assets" refers to either cash or inventory.

Cash misappropriation typically includes an employee or manager stealing cash-on-hand or cash receipts that never make it to internal documentation, but can also include more schemes. For example, someone could create a ghost employee, add them to the payroll and pocket the new employee's salary. Or, similarly, a manager could add a phantom vendor into the system—and collect tens of thousands of dollars if the company pays the vendor without confirming its existence or having payment processing controls. Inventory misappropriation could include someone in the shipping and receiving department failing to scan an item as it comes in—and opting to steal it instead. In many cases, the company may just assume it was lost in transit.

Corruption: Corruption broadly covers many types of fraud. Most commonly, it refers to employees or managers who form personal alliances with external parties and then put those relationships ahead of the best interests of the company. This type of fraud occurs in 38 percent of occupational fraud cases, according to the ACFE, and costs companies a median loss of USD $250,000.[6] It can include conflicts of interest (e.g. purchasing and sales schemes); illegal gratuities; and bribery, such as vendor kickbacks. A clear, transparent code of conduct should draw the line for your employees. Are sports tickets from a vendor okay? Up to what dollar amount? What if the sports tickets are for an event in a different location and all the travel costs are being covered as well? The answers to these questions will depend on your business, the nature of relationships and what you are willing to allow.

Financial statement fraud: Overstating an organization's net worth/net income typically involves falsifying the records surrounding revenues, liabilities, expenses and asset valuations. While there are numerous motives for this type of fraud, it's often done for personal gain—for instance, to inflate organizational performance to receive a larger bonus, to make the organization look better in the eyes of investors or lenders, or to cover up other types of fraud/risk.

Three ways to protect your business against internal fraud:

1. **Conduct a fraud risk assessment.** Conduct a fraud risk assessment. A phased approach with a few initial steps can strongly support and increase the level of fraud awareness for yourself and your employees

2. **Develop a fraud awareness training program.** Fraud awareness training is about empowering your workforce so they can be your eyes and ears in all areas of operations. To do this effectively, they must understand what fraud is, how it can happen and the red flags to look for.

3. **Implement a whistleblower hotline.** A properly-managed—and well-communicated—whistleblower hotline is an effective and inexpensive way to encourage fraud reporting within your organization and reduce the amount of time it takes to identify incidences of occupational fraud.

RED FLAGS

Keep an eye out for personal risk factors that may heighten the risk of fraud. For example, employees or managers who refuse to take vacations or share duties should raise red flags for fraud.

RED FLAGS

Legitimate vendors generally maintain corporate websites, Better Business Bureau registrations and HST numbers. If you can't find this type of evidence of a vendor's existence, fraud may be occurring.

Ready to start protecting your business?

We can help you to get started. It's important to take steps now to protect your company, your people and your reputation. We know from years of experience that raising the level of fraud awareness within your business can really have a huge impact.

To defend your business from fraudsters, Grant Thornton's fraud risk assessment process can help you understand prevailing business risks, your most at-risk assets, and the current state of your processes and controls. It can also help you identify glaring gaps and establish a plan to strengthen your anti- fraud controls. This could include anything from implementing a more robust fraud awareness training program to investing in fraud insurance.

For instance, a fraud risk assessment may include an awareness session to help staff identify risks and adopt common terminologies; brainstorming sessions that encourage staff to identify the organization's fraud exposures; workshops to enhance internal processes and controls; and reports outlining specific steps your organization can take to build a sustainable anti-fraud program.

Know how to respond—and recover

Should the unthinkable happen, you can't afford to be caught off-guard. Having a response and recovery plan in place can not only shorten the duration of a fraudulent act and save money in the process, but it can help your company get back on its feet faster. Knowing how to preserve the evidence of a fraud can also give investigators a decent opportunity to catch the perpetrator and help you strengthen your defenses to prevent history from repeating itself.

To learn more about how we can help protect your organization against fraud, visit grantthornton.ca

1 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 4. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf
2 Canadian Anti-Fraud Centre. April 27, 2017. "Fraud Types". Government of Canada. http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/index-eng.htm
3 Better Business Bureau. November 9, 2017. "FBI Says Business Email Compromise Scams Continue to Grow in U.S., Cost Companies More Than $1 Billion". https://www.bbb.org/stlouis/news-events/news-releases/2017/11/cftf-bec/
4 Hermann, Penny. January 23, 2017. "CRA scam continues, but with a new twist". Royal Canadian Mounted Police. http://www.rcmp-grc.gc.ca/en/news/2017/23/cra-scam-continues-a-new-twist
5 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 4. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf
6 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 10. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf
7 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 4. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

Grant Thornton

Audit | Tax | Advisory

About Grant Thornton LLP in Canada

Grant Thornton LLP is a leading Canadian accounting and advisory firm providing audit, tax and advisory services to private and public organizations. We help dynamic organizations unlock their potential for growth by providing meaningful, actionable advice through a broad range of services. Grant Thornton LLP is a Canadian member of Grant Thornton International Ltd, whose member and correspondent firms operate in over 100 countries worldwide.