KPMG

Forensic Focus

kpmg.ca/forensicfocus

Insurance plays an integral part in crisis management

By Karen Grogan, Senior Vice President, KPMG Forensic Inc.

From fraud to fire to cyber-attacks, organizations need to have a crisis management plan in place to respond efficiently and effectively to unexpected incidents. Part of any good crisis management plan is to ensure an organization has adequate insurance coverage. If adequate insurance is in place, it will be able to financially offset loses, or in many cases, put the organization back in the position it would have been in had it not been for the incident.

As a forensic accountant helping organizations make insurance claims, and working with those without insurance or inadequate coverage, it is apparent that clarification of insurance that is available, the coverage provided and the idiosyncrasies of the following insurance is required:

- Fidelity insurance
- Cyber insurance
- Business interruption insurance

Fidelity insurance

Organizations lose an estimated 5 percent of their revenues to fraud each year.[1] Many organizations do not realize they could have held insurance to cover losses due to employment fraud.[2]

Fidelity insurance, often referred to as employee dishonesty or crime insurance, generally covers losses resulting from fraudulent or dishonest acts committed by an employee, acting alone or in collusion with others. An insurance policy declaration page will indicate the limit of coverage and whether there is a deductible. Details of the policy will also indicate whether out-of-pocket costs related to accounting fees to investigate the alleged fraud will be covered and the extent of such coverage.

There may be some situations where an organization is able to obtain restitution from the fraudster but often the only route to recover losses is via insurance. Fraudsters often do not have the means or resources to repay organizations they have defrauded. Even if they do, the process to recover funds from the fraudster may require long drawn out civil litigation resulting in additional cash outlays and further losses to the organization.

A criminal complaint, may similarly take years and a conviction usually does not directly lead to a repayment to the organization.

Whether proceeding with an employment matter, civil litigation, criminal complaint or making an insurance claim, the quantification of the loss in respect of a fraud will be required, most likely in the form of a forensic accounting report. The burden of recovering losses in the case of employee fraud can be eased significantly by carrying adequate employee dishonesty insurance which covers both the losses from fraud and the cost of a forensic accounting investigation.

Cyber insurance

Every organization holds sensitive digital data such as personal customer information, contact lists, intellectual property and even financial data which can be accessed electronically. As such, organizations are under the persistent threat of cyber-attacks. As the threats from cyber criminals continue to grow in scale and sophistication, cyber-attacks are one of the highest impact risks that companies face. Common cyber attacks include hacking, phishing, malware that can steal or alter data and take computers and networks offline. It is not a question of whether a fraud or cyber-attack will occur within an organization, but when it will be detected.[3]

Fidelity insurance and commercial general liability (CGL) Insurance policies do not generally appear to cover losses from cyber-attacks. Therefore, although still in the early

1 *Report to the Nations* on *Occupational Fraud and Abuse. 2014 Global Fraud Survey, ACFE*

2 Most frauds against companies are committed by employees or former employees and many frauds include some collusion, often by persons external to a company. Further information on corporate fraud can be found in KPMG's 2016 Global Profiles of the Fraudster report: https://home.kpmg.com/xx/en/home/insights/2016/05/global-profiles-of-the-fraudster.html

3 See the following link to gain additional insight from KPMG into cyber risks and strategies: kpmg.ca/cyber

stages of development many insurance companies are now rolling out different forms of cyber insurance. It is meant to cover losses resulting from cyber-attacks, and many cyber insurance products can even imporve an organizations ability to respond to an attack. From cyber forensic providers, to external public relations agencies to breach coaches, cyber insurers often have a network of preffered providers that can be qickly assembled to support a customer through the containment, managmenet and recovery from a cyber attack.

Obviously the best risk management policy is to be proactive and ensure appropriate Cyber security controls are in place. However as a back-up, an organization may want to consider cyber insurance because the direct and collateral losses stemming from a cyber-attack can be very significant. Cyber insurance policies may also cover out-of pocket expenses such as legal counsel, information security forensic investigators as well as public relations expenses.

Business interruption insurance

Losses resulting from business interruption can be fairly minor, such as when there is a short electrical outage, or very significant when there is the complete destruction of a manufacturing plant due to a fire.

Business interruption insurance covers losses from incidents such as fire or flood where an organization stops operating for a period of time or at reduced capacity. Business interruption coverage may also be acquired that will cover indirect situations where, for example, a supplier or customer stops operating for various reasons causing losses to your company. The insurance policy will indicate which of the main two types of insurance apply to the organization, either "Gross Earnings" or "Profits". In either case, it is important to note that gross earnings or gross profit calculated for insurance purposes will be different than indicated on the organization's financial statement. It is important to be aware, when buying a business interruption policy, what expenses will and will not be covered and for how long.

Most business interruption policies will include some "co-insurance" provision which results in the insured organization sharing a portion of the loss if the organization is under-insured. In addition, the time period for which the organization is covered (the indemnity period) will vary depending on the policy. In some cases, the indemnity period ends when the damaged property is repaired or replaced (the period after reconstruction when the organization's sales may still be returning to normal is not covered). Under other business interruption policies, the insurance company will compensate the organization for losses until sales return to normal (usually to a maximum indemnity period of 12 months).

It is critical to make insurance part of an organization's crisis management plan. It can provide the funds to minimize the financial impact on the business of unexpected events and can help cover the costs of having outside professionals assist with claims investigations, the quantification of losses, public relations and most importantly will allow management to focus on getting the business back on track

KPMG Forensic

KPMG Forensic is a global network comprising of multidisciplinary professionals from KPMG International's affiliated member firms.

KPMG Forensic helps organizations in their efforts to achieve the highest level of integrity and to manage the cost and risk of litigation, investigations, and regulatory enforcement actions by assisting with the prevention, detection and response to fraud, waste, abuse and other forms of misconduct; the avoidance and resolution of disputes; and the collection, discovery and analysis of electronically stored information.

KPMG Forensic (Canada) has offices and qualified forensic professionals throughout Canada, with major offices located in Halifax, Montréal, Ottawa, the Greater Toronto Area, Southwestern Ontario, Calgary and Vancouver.

Contact us

Montréal
Stéphan Drolet
T: 514-840-2202
E: sdrolet@kpmg.ca

Ottawa
Kas Rehman
T: 613-212-3689
E: kasrehman@kpmg.ca

Greater Toronto Area
Colleen Basden
T: 416-777-8403
E: cbasden@kpmg.ca

James McAuley
T: 416-777-3607
E: jmcauley@kpmg.ca

Southwestern Ontario
Karen Grogan
T: 519-747-8223
E: kgrogan@kpmg.ca

Calgary
Paul Ross
T: 403-691-8281
E: pross1@kpmg.ca

Vancouver
Suzanne Schulz
T: 604-691-3475
E: saschulz@kpmg.ca