FRAUD MITIGATION

Fraud can have a devasting impact on any size of Complementary Health related business. In this article we look at the different types of fraud businesses should be aware of and measures which could be undertaken to mitigate the exposure to the likelihood of fraud taking place.

To start with, there are fraudulent activities undertaken by employees. Let us look at Theft of Company Assets for example and the different forms this can take.

- Workers Compensation (faking a work injury).
- Inventory (stealing from the company's own stock).
- Unauthorised payments (avoiding formal processes in place).
- Expense reimbursement (fictious receipts).
- Theft of services (working for a Transport company and having your own car repaired by the mechanics for free).
- Payment fraud (setting up false accounts and orders).
- Data theft (stealing customers details & selling these to a third-party competitor).

To minimise your exposure to the above taking place you may need to:

- Have a procedure in place where you undertake random audits on your accounts.
- Review roles where employees' multi-task across different responsibilities, i.e., someone who orders stock, is not the same person who pays the bills.
- Make sure very thorough background checks are undertaken for any new employee starting in the business.
- Keep company items of value, cash & other negotiable instruments under lock and key.
- Check that the orders made and vendors invoicing match off and are authentic (if in doubt phone your usual vendor and confirm billing received).

- Make sure you are thorough when setting up your new vendors such as, collecting and confirming their ABN Number, correct Business Name, Contact Details, Location/Premises (does it exist?), Verification of Bank account(s).

Next, we have fraudulent activities that can be undertaken by third parties outside the Business and currently Cyber Crime tops the list. There are several types of Cyber Crime such as:

- Social Engineering (hackers who make direct contact with employees by phone, email, face to face, then build a relationship to gain your business information & records).

- Malvertising (where third parties employ the method of filling websites with advertisements carrying malicious codes. Employees may click on these advertisements when searching the internet at work and once they click these ads, they will be redirected to fake websites or a file carrying viruses and malware and will automatically be downloaded).

- Phishing (Cyber criminals create fictious emails which employees may click on to gain connections to business reports in their industry, surveys with incentives, special deals from stationary suppliers. Their intent is to seek important security information such as credit cards or personal details of employees).

- Spamming (ideally spam emails might be directed to your junk email box as an employee however, if not, these fictious emails are there to again, look for a way to access the company's records through your interaction with them).

With the above in mind, here are some tips of how to be more Cyber savvy to mitigate the eventuality of Cyber Crime impacting your business and how to reduce the cost of a Cyber-attack.

- Make sure that your employees are highly aware of any suspicious activity from third parties, be it strange looking URL addresses, 'click here' email invitations, unusual requests from people pretending to know your organisation, etc. Cyber Insurance (referred to below) can provide your Business with access to a range of content useful to train your employees so they can be more on guard and think twice when recognising something out of the ordinary.

- Have a strict regime around back-ups for your systems. Consider backing up external drives to the Cloud.

- Ensure you have a strong firewall backed by IT Professionals managing it.

- Install anti-virus and malware software on your systems.

Lastly, Cyber Insurance is a relativity new insurance where businesses can get help from professionals and mitigate Cyber related costs in the event they are hacked.

<u>Typically, Cyber Insurance includes cover for:</u>

Cyber Extortion
Cover for the damages and costs associated with mitigating a cyber extortion incident, including ransom payments where the law allows.

Theft & Loss of Data restoration
Covers incidents where an information asset went missing, whether through misplacement or malice. Includes cost of Data loss, restoration including decontamination and recovery.

Business Interruption
Cover for losses due to a network security failure or attack, human errors, or programming errors. Covers reasonable costs to bring your business back to the condition it was immediately before the cyber event.

Breach of Privacy Liability
Cover for liability arising from failure to maintain confidentiality of data.

Crisis communication expenses
Cover for crisis management and mitigation measures to counter a credible impending threat to stage a cyber event against your IT infrastructure. Incident response and investigation costs, supported by a **24/7 emergency assistance service** including Cyber learnings.

Access to an incident response hotline
Supporting clients throughout the process using a network of forensic, cyber extortion, legal, notification, fraud remediation and public relations experts. Access also to a range of tips, tools, and Cyber related information.

Social Engineering
When you or your clients' emails are intercepted by a hacker and bank account details are hacked.

How we can help you with Fraud mitigation
We urge all Complementary Health business owners to contact your insurers or brokers to help investigate and review your current insurance covers. Using an insurance Broker will save you time and money because they can provide you with expert knowledge, advice, and negotiate competitive premiums on your behalf.
If would like to know more about Insurance Programs we can assist and review for you and to discuss your own individual circumstances, please contact the friendly team at IME Insurance Brokers on **1800 641 260** or visit us at: www.imeinsurance.com.au

James Gillard
Managing Director

IME INSURANCE MADE EASY
BROKERS SINCE 1992

cma Complementary Medicines Australia