CFO's need to see CYBER FRAUD *not as an* IT ISSUE

By George Hazim

As technology rapidly evolves and accessibility is its central theme, somewhere along the way, we have nurtured deception.

The world has become a pervasive place with a paradigm of accelerating change continually altering the rules of engagement.

From fake Facebook profiles, cat fishing and scamming, nothing is as it seems.

Technology has bred a culture of exploitation and nothing and no one is off limits. The Holy Trinity of masses of data, lack of privacy and the ability to defraud corporations is cybercrimes nirvana.

Since 2015, cybercrime has grown exponentially. Criminals are no longer bound by borders because there are none in the virtual world.

And while technology explodes, and cybercriminals rip billions from businesses, nothing better highlights the art of deception than the actions of Evaldas Rimasauskas.

Rimasauskas duped Google and FB out of more than $173m. He used a Business Email Compromise (BEC) scam.

BEC is a 'reverse play'. Rather than target companies, phishing mails are sent to obtain email login details of people in supplier organisations and then used to send, fake invoices or change of bank detail requests to the supplier's customers. As invoices and bank change requests come from the authentic email address and include prior trails of email correspondence and written in the same style as previous legitimate emails it makes it almost impossible for corporate clients to notice the fraud.

The scam relies on human behavioural psychology and knowing many departments won't question requests from legitimate suppliers, especially where a thread of prior communication is present.

If two of the world's most technologically superior corporates can be scammed, how exposed is corporate Australia?"

In the current environment, the answer is "extremely" through lack of knowledge and naivety, Australia's CFO's are unwittingly complicit in helping cybercriminals by expecting untrained staff to play detective. There is an abundance of unconscious incompetence in many accounts departments, where people simply don't know what they don't know.

Michael Connory, CEO of Cybersecurity firm Security In Depth and Australia's foremost expert in cybersecurity, says it's not a matter of 'if' but 'when'.

"We have seen, since 2018, cyberattacks rise and become more brazen. It's seems hackers are sending a message especially to the banks, they can hit us anytime, anywhere and penetrate at will. Investment in training is paramount. That's where the real problem lies," Connory says.

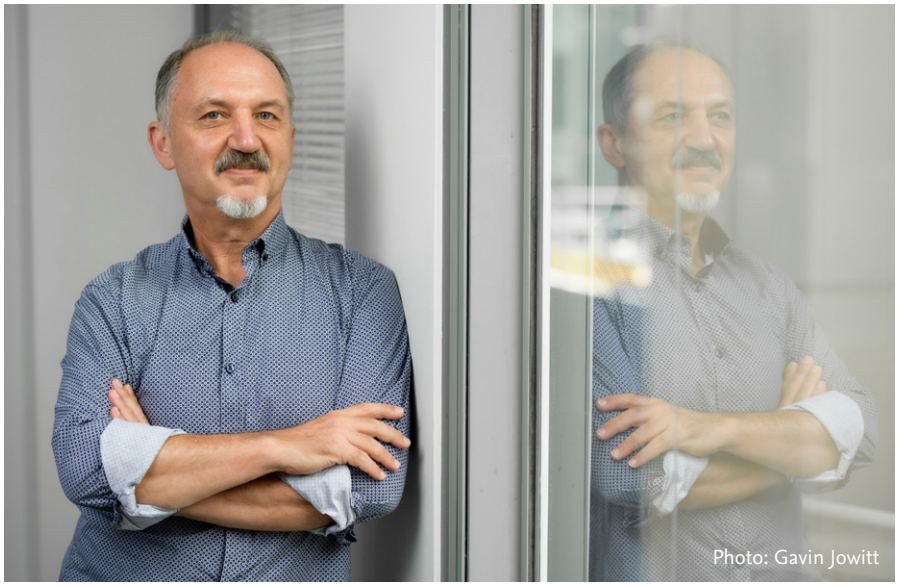
An advisor to corporates globally, Connory makes it clear staff training is imperative. *"Organisations need to implement good governance. The challenge is not to adopt a band aid approach to cybersecurity but lay solid foundations."*

eftsure is an Australian secure payments data platform, mitigating the risk of fraudulent business payments in the electronic payment process. It protects a business' assets and people through a cross-verified database combined with external data sources and independent verification procedures ensuring payments arrive at their intended recipients.

In recent months it has seen a significant rise in attempts to defraud corporations.

eftsure protected over $21bn of payments by Australian corporates from being diverted to fraudsters last year and is currently protecting more than $2.5bn a month of payments with its Know Your Payee (KYPTM) platform.

Mike Kontorovich, Co-Founder of eftsure says, *"based on what we are seeing, 2020 will be the year an Australian company will be hit with a cyber financial disaster,"* as most Australian businesses remain fully exposed to falling victim to the exact scam Rimasauskas ran. *"The figure will be unquantifiable, yet big enough to cause serious problems."*



Mike Kontorovich, Co-founder & CEO, eftsure

An increasing concern Kontorovich says, is the expectations CFO's have of staff to play detective. *"They expect them to identify fraudulent invoices they are ill-equipped to."*

Expecting staff with no training to identify illegitimate invoices or changes to bank details is asking for trouble. Greater investment must be made in training and technological resources to help them do what's expected. The attitude of CFO's is part of the problem,

Kontorovich says.

Both Kontorovich and Connory say hackers view Australia as easy pickings and a perfect storm is now brewing for a major attack. Australia is currently the third most targeted country for cyberattacks.

Kontorovich says an attack will happen because of the:

(i) pervasive use, reliance and misplaced trust in emails

(ii) ease with which identity theft is now occurring in the digital world

(iii) Australian banks don't match payee names to BSB and bank account numbers.

While digital business transformation strategies and technologies evolve, business, finance and accounting payment controls remain manual.

With technology's evolution and a commitment to defraud, it's like taking a knife to a gun fight. *"It's an unfair fight – professional fraudsters only need to succeed once to devastate a company, yet the company and their staff have to be successful each time at picking up a false invoice."*

eftsure has a joint business relationship with PwC Australia, through the firm's professional services Align program.

PwC boss Ross Thorpe said, *"Align, looks at technology from upcoming companies and introduces them to our larger clients. It is solving a big problem (for) a number of clients."*

Leading Australian Criminal Lawyer and National Practice Manager of Armstrong Legal, John Sutton, understands fraud better than most, *"but the cyberworld is a rapidly moving feast."* he says.

Battling cyber fraud, requires investment in training staff. It's the best form of insurance alongside effective protocols and technology.

"Little can be done legally," Sutton says once money is stolen by overseas hackers. *"It's better to be vigilant than discover you've been duped thousands of dollars. "This is really where a penny of prevention is better than millions of dollars of (loss and) cure."*

Fresh Supply Co, renowned for its governance protocols, is one Australian corporate leading the way in training staff around cybersecurity.

David Inderias, Fresh Supply Co's, Founder and CEO knows the importance of security and equipping staff with the resources needed to protect data.

Inderias, along with the company's Chairman Dr Ben Lyons, are working to ensure Fresh Supply Co remains ahead of the game around cybersecurity and fraud.

"Even in our emerging field of tracking food with blockchain technology, we have partnered with players like MasterCard to ensure we deliver our services at the speed, security and scalability of financial systems, that others cope with and work."

"Our business," Inderias says, *"is built on trust. Our investment in training must be equally significant. We have to ensure privacy and protection which means taking seriously all aspects of cybercrime and fraud."*

As Connory says,

Training is the foundation to cyber resilience.