Cybercrime a lawyers picnic to be avoided

Banking Royal Commission's in tow, Australia's financial services sector flounders in ways suggesting there is more than something rotten in the State of Denmark.

It's not enough the Royal Commission reinforced what Australians have always suspected – greed and avarice for profit is the only motivating factor behind their seemingly unbridled existence, no matter how many lives are destroyed – it's the 'whatever it takes at all costs attitude' that is most disturbing. Now however, it seems the management and protection of client data and information is inconsequential. Or is it?

History is an important teacher of life's lessons, and the revelations of the Banking Royal Commission has created a rethink of the financial services sector on how they need to behave, rather than operating like lawless entities unhinged to do as they please. It's a path they no longer want to travel.

Enter the sector's new-found approach to cyber security and placing the interests of its customers ahead of its own. Some companies are now getting on the front foot and protecting client data from cyber breach attacks and hackers.

Cyber security and crime is now fashioned into the lives of every Australian, just like the banks and the financial services sector has touched us in ways we could never have imagined, cybercrime, has permeated its way into our lives through an osmotic process due to ignorance and the lack of importance corporations have and are placing on protecting our information.

And yet, it seems attitudes are changing, which makes the approach by various companies in the financial services and banking sector, along with other Australian corporates proactively seeking to batten down the hatches and secure their cargo pleasing, rather than running the gauntlet of starring down the barrel of damaging law suits - creating a picnic of legal fortunes for lawyers specialising in cyber security crime.

Lawyers picnics are picnics best not attended, its better to be absent than considered the main invited guest and centre of attention. Some lawyers see nothing more pleasing than adopting a game hunter's approach to those who choose to be ignorant of the law and their responsibilities.

How some in corporate Australia and the financial services sector are working to bolster security around data protection is through the engagement of a third-party risk assessment assurance scheme entitled CARR.

Based on a similar concept to the financial sectors credit score rating, CARR allows businesses to assess the security viability of organisations before partnering or entering into business.

The financial services sector and corporate Australia recognises it has a long way to go, but what has become impressively clear is the commitment to want to protect client data.

Implementing a third-party risk assessment assurance scheme, and through reviews conducted, it seems many companies are putting in place security protocols designed to prevent phishing attacks, targeting CFO's and trying to obtain CFO's credentials like username and password and access hundreds of millions of dollars in investments

The reviews companies are undertaking are beginning to bare immediate results to improve security by identifying a two-factor authentication and stopping unauthorised access to over 500 investment accounts worth over $400 million.

The world is an ever-evolving place, and cybercrime is a growth industry reaping trillions of dollars on the dark web, and the pot of gold is our personal information. Travelling the journey of a Royal Commission has helped members within financial services sector become proactive around the new issue of cybersecurity – it's not a far stretch to suggest if the practices that were unearthed during the Royal Commission were anything to go by, then proactively working to safeguard against breaches and prevent potential law suits wouldn't be too far front of mind. If anything, it's a lesson for all of corporate Australia and a way forward for all companies to follow.

The information corporate's store about us, is a treasure trove of fortune for cybercriminals, and while technology evolves with each blink we take, delivering us new experiences, it also comes with a dangerous price if not managed appropriately. Cybercrime continues to grow exponentially, and while Rome burns, Corporate Australia fiddles, we are left exposed without the right protection and security.

Research statistics show a damning urgent need for training around Cyber security, because what several companies have shown is that significant numbers of staff are needed to help reduce the risk of human error around Cyber Incidents - 70% of all data breaches in the previous quarter's report by the OAIC were as a direct result of human error.

As damning as statistics are, a light is shining brightly on the horizon as the wheels of CARR begin to turn slowly and the financial services sector and corporate Australia learn a valuable lesson from the Banking RC, and prove not everything is rotten in the State of Denmark and the advent of litigation can be avoided.

Ends.

Michael Connory Is CEO of Security In Depth