Control Risks

ARE YOU BRINGING A KNIFE TO GUN FIGHT?

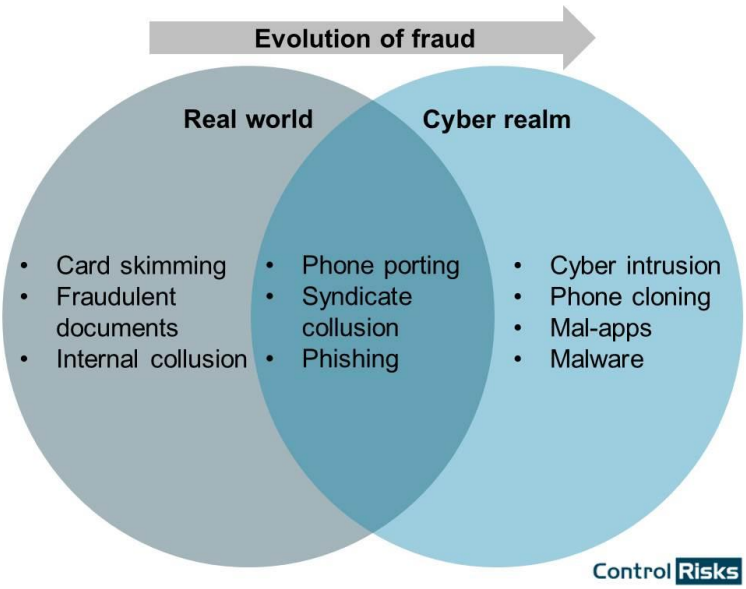
How to better manage fraud in an increasingly digital world

By Allanna Rigby

Evolution of fraud from the real world to the cyber realm

Fraud is big business. Global fraud losses in 2015 were estimated at USD 3.7 trillion[1] and are predicted to rise.

There is also an evident shift in fraud typologies away from traditional real world frauds, such as card skimming, fraudulent documents, social engineering, etc., towards cyber frauds, such as cyber intrusion, phone cloning, malware and fake apps (mal-apps). While these two realms don't exist in isolation and many fraud typologies span both dimensions, the trajectory is continuously heading towards the cyber realm.



Fraud in Asia Pacific

The fraud landscape in Asia Pacific is changing rapidly.

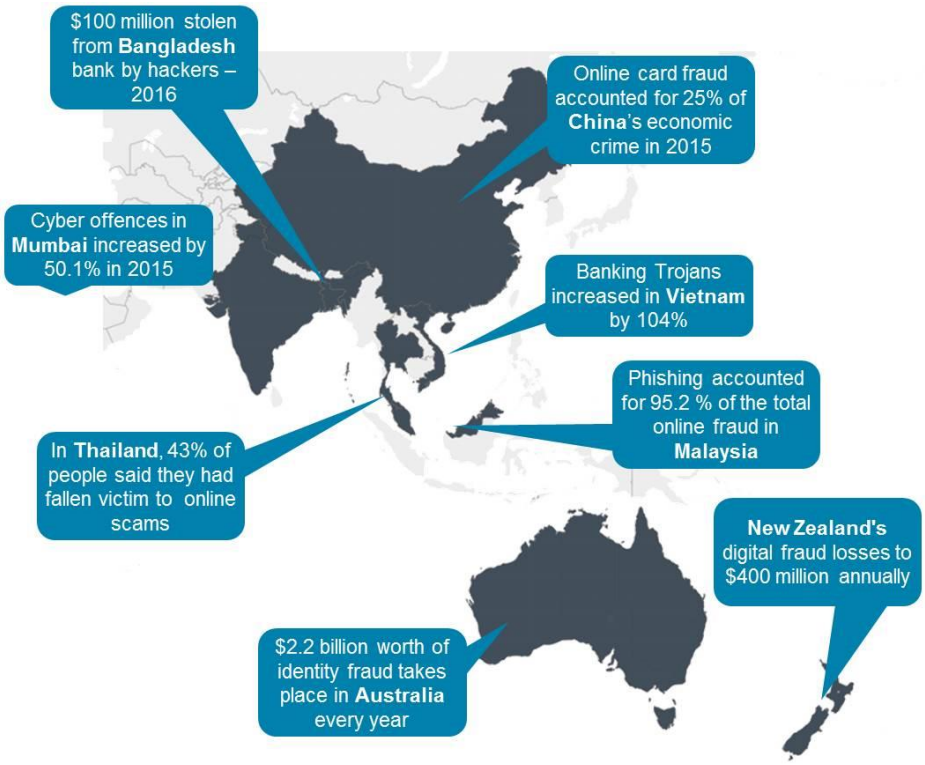
Financial losses from cyber fraud in the Asia-Pacific region came to USD 81.3bn in 2015 and exceeded losses in North America and the EU by about USD 20bn. Asia alone accounted for more than a quarter of the USD 315bn cost of attacks globally during this period. Reportedly, 90% of Asia-Pacific companies have been hit by some form of cyber-fraud last year.

Even frauds that have traditionally been real world in nature (such as collusion, mail theft, etc.), are adapting to the expansion of the cyber realm. As an example, internal fraud historically sits in the real world and is reported to cost on average approximately 5% of an average organisation's revenue. However, of late, it is adapting to leverage possible cyber vulnerabilities. This was demonstrated in the case of Morgan Stanley, where an employee was accused of stealing customer information with the intent to sell to cyber criminals. Whether employees steal customer information or intellectual property, the need to protect your data not just from external threats, but the insider threat, has never been greater.

[1] Based on applying a 5% fraud loss to the Gross World Product.

How to help protect your organisation

In this ever-changing environment, organisations need to ensure they are not only protecting themselves against real world frauds, but also against the growing cyber frauds. Traditional fraud detection, such as internal controls, red flag monitoring and internal audit, is still capable of protecting organisations against real world frauds; however, as fraudsters move into the cyber realm, fraud detection methods needs to follow.



The basis of cyber fraud revolves around an organisation's data and a criminal's ability to manipulate, access or steal that data. Whether this occurs through malware, intrusion or phishing, the result is nearly always, but not limited to, financial loss to the organisation.

Therefore, the key to better protecting your organisation against fraud is to have fraud detection methods that span the real world and the cyber realm. For example, predictive analytics, statistical analysis and machine learning can enable organisations to defend themselves in a more effective manner.

In its *Report to the Nations* (2016), the Association of Certified Fraud Examiners identified that organisations with proactive data-led fraud detection, were able to reduce their median fraud loss for an organisation by up to 54%. Data-led solutions, which leverage the power of the data that the criminals are so desperate to steal, provide a bright light at the end of the fraud detection tunnel.

As fraud moves towards the cyber realm, it is imperative that organisations follow and arm themselves with the right tools to better protect their organisations so they aren't bringing a knife to a gun fight.