Damaging More Than the Bottom Line: An Overview of Fraud and Cybersecurity

We have all seen the figures placed on the cost of fraud and cyberattacks to businesses and the economy with some informed estimates putting the global cost at USD445 billion.[1] Less sensational than its financial implications, though, but far more disruptive, are the reputational damage and the business impact that arise in the aftermath of successful attacks

Protecting against the threats and attacks that fraud and cybersecurity pose is an ever-increasing concern for businesses today. For many, it has become imperative to safeguard their organisations from such dangers, especially considering that threats and attacks are continuing unabated as the methods of fraudsters and attackers evolve and change to reach their ends.

Available data indicates that instances of fraud and cybersecurity attacks are increasing not just in frequency but in severity and impact. Companies that fail to ensure that their employees are fully trained to recognise and tack action against this using adequate security processes, procedures and protocols, therefore, not only face a greater risk of financial loss, which includes loss of assets, but a greater risk of reputational damage and business disruption, which includes negative publicity.

How has the fraud landscape changed?

Fraud and cybersecurity threats continue to evolve as better organised and more sophisticated attackers have emerged.

As illustrated in diagram 1, fraudsters and cyber attackers have become much more sophisticated in recent years. There has been a noticeable shift in the profile of those behind attacks.

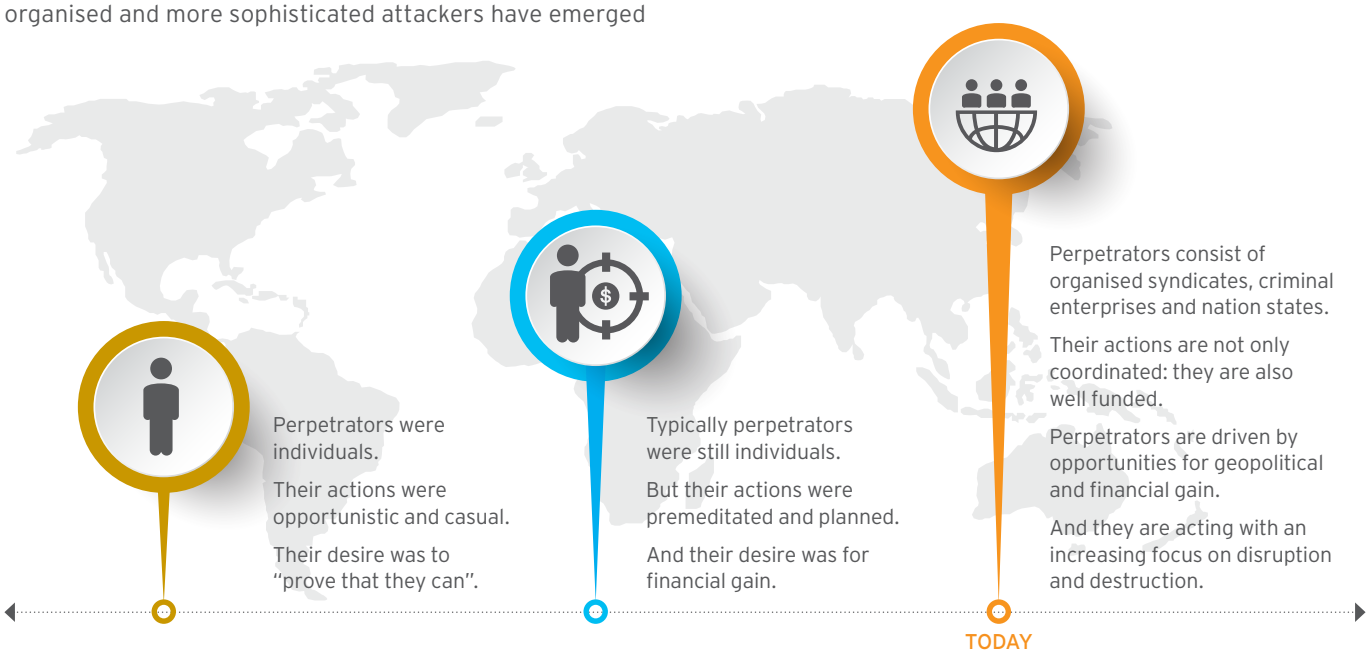
In the past, attackers were primarily individuals operating on an opportunistic, casual or ad hoc basis, largely driven by the desire to prove that they could successfully carry out a fraud attack.

Acting alone or in collusion to commit internal or external fraud, fraudsters increasingly perpetrate acts that are focused on disruption and destruction.

[1] From McAfee's Net Losses: Estimating the Global Cost of Cybercrime, last downloaded from www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf on 4 April 2016.

Diagram 1. From Past to Present: The Step Change in Information Security Threats

The cyber threat landscape continues to evolve as better organised and more sophisticated attackers have emerged



Today, attackers are highly organised syndicates and criminal enterprises that are managed in a similar way to businesses. These criminal enterprises are typically well organised and, importantly, well funded. Their motives are primarily for financial gain but in some instances for geopolitical gain. These fraudsters are also increasingly focused on disruption and destruction. There is also the risk of internal fraud and similarly internal fraud may be undertaken by an opportunistic individual or by an employee who operates in collusion with an organised criminal group.

Diagram 2 shows the changing nature of the various aspects of a fraud or cybersecurity attack. Most notably, attacks are becoming increasingly targeted with fraudsters undertaking a large amount of research and planning prior to attempting an attack. Attempted attacks have also moved from a pattern of one-off, opportunistic attacks to targeted, planned and continuous attacks. Attackers will continue their attempts on one target if there is a chance of success.

Attack methods are also continuously evolving and adapting to overcome the defences that organisations create. Unsurprisingly, there has been a growth in the use of technology by fraudsters. Attack methods tend to target weaknesses in technology and in human nature and in some instances both. It is for this reason that it is so important to frequently review internal procedures and processes and to ensure that all employees are fully trained and aware of their responsibilities in the event of an attempted attack.

What is the profile of a fraudster?

KPMG has developed the profile of an average internal fraudster based on an analysis of 596 cases of "white collar" crime between 2011 and 2013, with some telling statistics.

He targets his employers

The typical fraudster is male and is between 36 and 55 years old, and he tends to commit fraud against his own employer.

- 61% of fraudsters are employed by the company they attack.
- 41% are employed for a period greater than 6 years.

He works in collusion

He tends to work in a finance or in related role, including operations, or hold a senior management position. As such, he has typically been employed by his company for more than 6 years. During this time, he perpetrates frauds over 1 to 5 years in 72% of cases, where 70% of the time, he works in collusion, causing tens of thousands, hundreds of thousands and even millions of dollars' worth of damage.

- 18% are valued at between $50,000 and $200,000.
- 43% exceed $500,000, 16% of which exceed $5,000,000.

He also works alone

When this typical fraudster acts alone, a large majority of the frauds he commits occur over 1 to 5 years, also causing with significant monetary damage.

- 21% are valued at between $50,000 and $200,000.
- 32% exceed $500,000, 9% of which exceed $5,000,000.

Diagram 2. Evolving Threats: An Illustration of the information Security Challenge

Treasury and Trade Solutions
transactionservices.citi.com

GRA26733 04/2016