Rethinking Cyber Security

Businesses are facing a growing cybersecurity problem. While our cybersecurity needs have been evolving rapidly for years, the COVID-19 pandemic has opened new vulnerabilities and made existing issues more apparent. More people and businesses than ever are relying on technology and the internet to operate even on a basic level. This not only puts potential victims at greater risk of suffering data breaches but also magnifies the scale of the disruption that a cyberattack can cause.

On an even greater scale, cyber-attacks can and have disrupted financial services, major online merchants, and governments, resulting in astronomical losses. In many cases, such as the DDoS attacks on NZX in 2020, businesses and institutions of all sizes continue to underestimate the danger posed by cyber threats, and the impacts that even relatively uncomplicated attacks can have. At Trustees Executors, we know that the importance of technology and the associated people and processes in today's financial services sector cannot be underestimated. We continue to invest in this area to protect both ourselves and our clients.

All businesses and private individuals are more vulnerable than ever
As a result of the pandemic, we spend more time online than ever working, interacting socially, and managing our affairs. While working from home might keep us physically away from the public, though, it means that our information has to travel much further to reach us. In order to do our jobs from home, encrypted and purely internal work servers have to be made accessible online. Moreover, more people will be logging into those servers from more locations, more often, and from more computers - often saving confidential information on their computers directly.

This provides cybercriminals with a wealth of potential leaks. Each computer represents a vulnerability that can be exploited to gain access to secure systems, or just to glean some valuable information.

Cyber threats are diverse and evolving faster than ever
Large businesses, governments, and organisations are bureaucratic behemoths and need to take much more time to make and implement decisions than individuals or small businesses. This reveals an almost global systemic vulnerability that will need to be addressed in the near future. In January, RBNZ suffered a significant data breach that compromised a large amount of third party data, affecting many of their customers. The bank had been warned of a critical vulnerability in the affected application in December but failed to act in time.

Cybercriminals are creative and diverse, resulting in a wide variety of different types of attacks. Many, such as ransomware, DDoS attacks, phishing scams, and simple data theft are familiar, but new approaches are being developed and refined all the time. As technology improves, new kinds of attacks become possible, and a greater variety of new attacks can be developed more quickly.

- Botnets - Botnets which are systems of computers infected with malware are growing increasingly sophisticated and dangerous, allowing cybercriminals to launch larger and more damaging operations.
- Deepfakes - A political group in Belgium used a deepfake (a fake video) of the Belgian Prime Minister in an attempt to impersonate him and to sway public opinion. Similarly, cybercriminals create deepfakes to extort victims, threatening to display them in compromising scenarios.
- Ransomware with double extortion - Cybercriminals are increasingly finding ways to extract even more money from victims by first stealing a victim's data, then encrypting the victim's computer. The victim is then first extorted for the recovery of their systems, and then again to prevent the stolen data from being published publicly. In some cases, the data is then sold on the dark web for a third payday regardless.

At the same time, 5G technology and an ever-growing repertoire of always-on gadgets are making it possible to gather and transmit more information over the internet than ever. This could allow criminals to track a victim's movements, purchases, and behaviours, and to gather other highly specific personal information.

DDoS attacks can disrupt financial markets

Traditionally, DDoS attacks cause damage by preventing their victims from doing business. For example, every minute that Twitter, Spotify, or Netflix servers are down translated to lost revenue. The financial services industry, however, is even more vulnerable because of the extent to which it relies on reliable low-latency internet communications.

In New Zealand last year, NZX, Westpac, and TSB Bank were targeted by cybercriminals for DDoS attacks. Often, as was the case with NZX, these attacks are accompanied by a ransom demand, with the attack commencing if it isn't paid. The resulting attack overwhelms the victim's servers with traffic, resulting in delays and server shutdowns. In the financial services industry, particularly securities trading, precise timing is essential. Even an attack that only results in some lag can result in significant financial damages.

Because of this, it's essential for major financial services actors to stay on top of cybersecurity, and to do everything they can to protect themselves and their customers. Failing to do so is not only dangerous and expensive, it can also lead to reprisals from regulatory agencies.

Unprepared institutions face reprisals from regulators

Under the Financial Markets Conduct Act (FMC Act), licensed market operators are legally required to have sufficient technology resources to operate their licensed markets properly, including arrangements to ensure market disclosures are made available. A successful DDoS attack can prevent an exchange from making disclosures in a timely manner, meaning that they need to take reasonable steps to protect themselves from these kinds of attacks.

In January, the Financial Markets Authority (FMA) released a review of NZX regarding the disruptions it suffered due to the DDoS attacks a few months before. It found that the stock exchange "failed to meet its licensed market operator obligations due to insufficient technology resources." Specifically, FMA Chief Executive Rob Everett indicated that NZX was slow to act, and failed to take responsibility and to engage with industry feedback.

The stock exchange's crisis management planning and procedures were "basic" and insufficient for dealing with a DDoS attack that the FMA found to be foreseeable. NZX itself was aware of this, rating its own IT security profile as "basic", which indicates that it had not adopted a number of best practices.

Our View

Cybersecurity systems and experts are facing their greatest challenge yet due to the extraordinary changes brought on by coronavirus globally. While some businesses and institutions may be hoping to simply wait it out, we understand that cybercrime is here to stay. More importantly, cybercriminals will continue to develop new methods, and discover new tools to reach their victims. Safety from cybercrime can only be achieved by keeping up with—or staying a step ahead of—cybercriminals, which necessitates a significant amount of investment and attention on the part of businesses, governments, and private individuals.

At Trustees Executors, we remain alert and aware of the threat that cybercrime poses to our sector, our clients, and the economy at large. Going forward, data security will necessarily become a more important factor for customers in choosing which businesses and organisations to engage with. More importantly, data security is essential in order to be a reliable business partner and to help facilitate your long term

financial goals. Because of this, we continue to invest in cybersecurity, stay on top of best practices, and work to stay abreast of new developments.