Cyber Attacks will make you Wanna Cry

June – July 2017

Today, it is not unheard of for commercial and industrial companies to come under the same level of sophisticated attack that was once reserved for states. The increasing use and reliance on technology and the proliferation of new technological devices have made us more vulnerable now than ever before. To make matters worse, sophisticated crime syndicates are using encryption to hide their activity. Consequently, any company, government entity, non-profit organisation, or individual that uses computer systems or the Internet is susceptible to a cyber attack. The drivers for these crimes are varied and include extortion, commercial sabotage, hacktivism, cyber spying, cyber terrorism, and cyber warfare. There is particular concern about the vulnerability of the healthcare sectors in many countries as they process vast amounts of sensitive personal data.

Attacks in the Middle East

The Middle East has long been a target for various types of cyber attacks.

The Shamoon attack on oil giant Saudi Aramco in 2012, described by former US defence secretary Leon Panetta as the most destructive cyber attack on a private business then seen to date, is believed by US officials to have been the work of hackers working on behalf of the Iranian government. In that attack, the virus crippled 35,000 computers at Saudi Aramco within hours by overwriting the master boot record and rendering their computers inoperable. Earlier this year, the Saudi government warned organisations in the Kingdom to be on the alert for variants of the Shamoon virus, following attacks on various ministries and government agencies. Given the continued conflicts in the region, such attacks are expected to increase.

At the time of writing, the WannaCry ransomware hack has indiscriminately hit 200,000 targets in at least 150 countries. Ransomware is a type of malicious software that blocks access to a computer system until a sum of money is paid. According to Symantec, Saudi Arabia is the most targeted country for ransomware attacks in the Middle East and Africa region, followed by the UAE.

Potential losses resulting from cyber attacks

The frequency and severity of cyber attacks increases year-on-year, and it is now imperative that organisations take a proactive strategy to manage them. Such strategies need to be targeted to ensure:

- the preservation and continuity of commercial operations;
- protection of commercially sensitive information and valuable intellectual property;
- protection against the theft and misuse of sensitive and personal information of employees and staff;
- prevention of fraud; and
- minimal brand damage and loss of good will.

Protecting against, and recovering from, cyber attacks

A multi-pronged approach should be taken to deal with this threat in a way that covers all bases, including:

- using information technology systems and products that were originally designed with security in mind;
- finding and fixing vulnerabilities before an attacker can try to exploit them;

- properly vetting new employees, agents and contractors who have access to information technology systems;
- deploying both proactive and reactive cyber security solutions;
- establishing internal security policies and plans for defending against attacks (and testing such plans through the use of exercises);
- preparing and promptly implementing disaster recovery in the event of a cyber attack;
- placing ‘best effort’ obligations on service providers to perform remedial action against virus contamination. This includes ensuring restoration of data from backups maintained by the service providers, locally stored data, and backups maintained by the customer as well as reconstructing lost or corrupt data;
- obtaining cyber security insurance. Note however that this type of insurance can be difficult to source as only specialised underwriters and IT experts have the requisite expertise to even come close to appropriately pricing the insurance risk. Even then, the actuarial estimate of the insurable risk is unlikely to be accurate as estimates of total annual loss due to cyber risk vary greatly from around $100 billion to over $1 trillion; and
- a right to terminate the contract where the service provider is not able to restore the service promptly following an attack. This leverage ensures immediate attention, and as a last resort, allows the customer to engage another service provider to restore the services.

Customers should review their existing IT contracts to ensure they contain sufficient obligations on the technology vendor or IT service provider to comply with the measures above. Where the contract does not address these issues, the customer should seek to raise these concerns with vendors and service providers with a view to having terms amended to address these types of essential concerns.

Conclusion

Organisations can no longer afford to ignore cyber security threats and must put in place systems and processes to defend against and recover from cyber attacks. The recent global Wannacry ransomware hacks are a clear reminder of this. Financial institutions, healthcare providers, government agencies, airlines and online businesses are particularly vulnerable and should undertake an internal review to identify and address any weaknesses.