World Events, State Actors and Cyber Risk?

Michael Demery - Managing Director of Seccom Global

Often business becomes complacent to the risks of cyberwarfare. With the saturation of these events in the media, it is easy to become desensitised to conflicts between countries. However, these world events should be a consideration when companies implement their cyber strategy.

The current military tensions between Ukraine and Russia seem half a world away, yet the potential for the Australian government or Australian organisations to become collateral damage is real. Recently there has been a string of cyberattacks on Ukrainian government and banking targets believed to be from Russia. If tensions increase, the potential for these attacks to target NATO member states is almost inevitable. Although not a NATO country, our relationship with NATO countries makes Australia a target for cyberattacks inspired by acts of patriotism by Russian cybercriminal gangs linked to the Russian intelligence service.

In December 2015, hackers infiltrated power stations in Ukraine, causing a blackout that affected over 200,000 households. The attacks were later attributed to Russia. In 2017, malware known as NotPetya targeted financial, energy and government institutions in Ukraine; the U.K.'s National Cyber Security Centre said Russia's military was responsible for the attack. NotPetya targeted vulnerabilities in Microsoft operating systems and spread internationally.

Cyberattacks do not need to be directly targeted at organisations to cause harm. NotPetya, for example, caused disruption costing hundreds of millions of dollars for many global companies. Maersk – shipping, Merck – pharmaceutics and Saint Gobain – construction were all majorly disrupted due to NotPetya.

Closer to home, tension builds in the South China Sea. Beijing claims self-ruled Taiwan as its own and has threatened to use force if necessary to unify the two sides. China is suspected of targeting Taiwan's government and micro-chip manufacturer's websites to the extent of 200,000 to 400,000 attacks per day.

In late January, China was also the chief suspect for hacking into News Corps U.S. and U.K. email accounts. The attack was likely an attempt to gather intelligence for Beijing's benefit, said News Corp media advisor.

For many years the U.S. Government has cautioned that products from China's Huawei Technologies Co. pose a national risk for any countries that use them. In 2012, Australian intelligence officials informed U.S. counterparts that they had detected a sophisticated intrusion into the countries telecommunications systems after a software update from Huawei was loaded with malicious code. The incident substantiated suspicions in both countries that China used Huawei as a conduit for information gathering.

In 2021, hackers backed by the Iranian government targeted exploits discovered in both the Microsoft and Fortinet operating systems. Although both Vendors quickly patched all vulnerabilities, organisations that failed to implement these security patch updates remained vulnerable.

Many Australian organisations were targeted as a result of these exploits. Several of these companies were later susceptible to follow-on operations. These included data exfiltration or encryption, ransomware, and extortion. In addition, many random and opportunistic attacks occurred.

This article's point is to highlight that many countries are using cyber as a weapon. Be it for political gain, to do damage, or for information gathering, it's important to be aware it is happening with increasing frequency. Being cyber aware, educating your people and following an excellent cyber hygiene strategy all go a long way to protecting your sensitive information.

> **Cyberattacks do not need to be directly targeted at organisations to cause harm.**