AUSCSEC

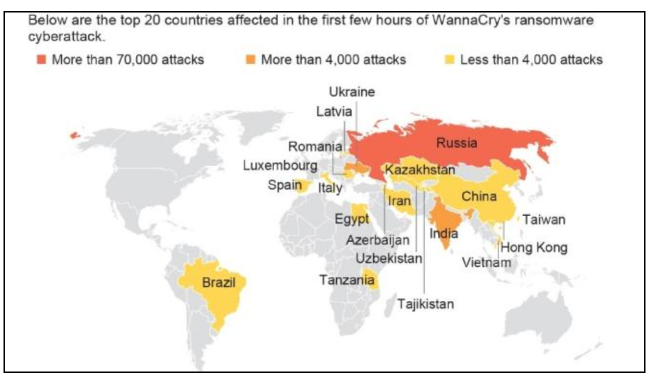
The year of living dangerously with COVID 19 - 2020.

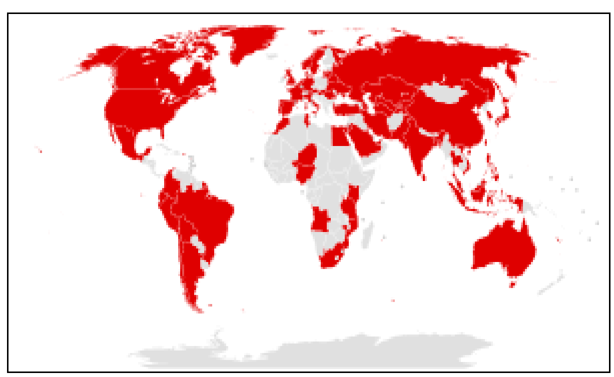
If the past ten months are anything to go by COVID 19 has provided evidence that we as a nation are at high risk of impact and disruption by both a biological pandemic, and a cyber pandemic. According to the World Economic Forum (WEF) the lessons learned in comparing both could provide us with some major insights on how our nations' leaders could prepare better for a major cyber event.

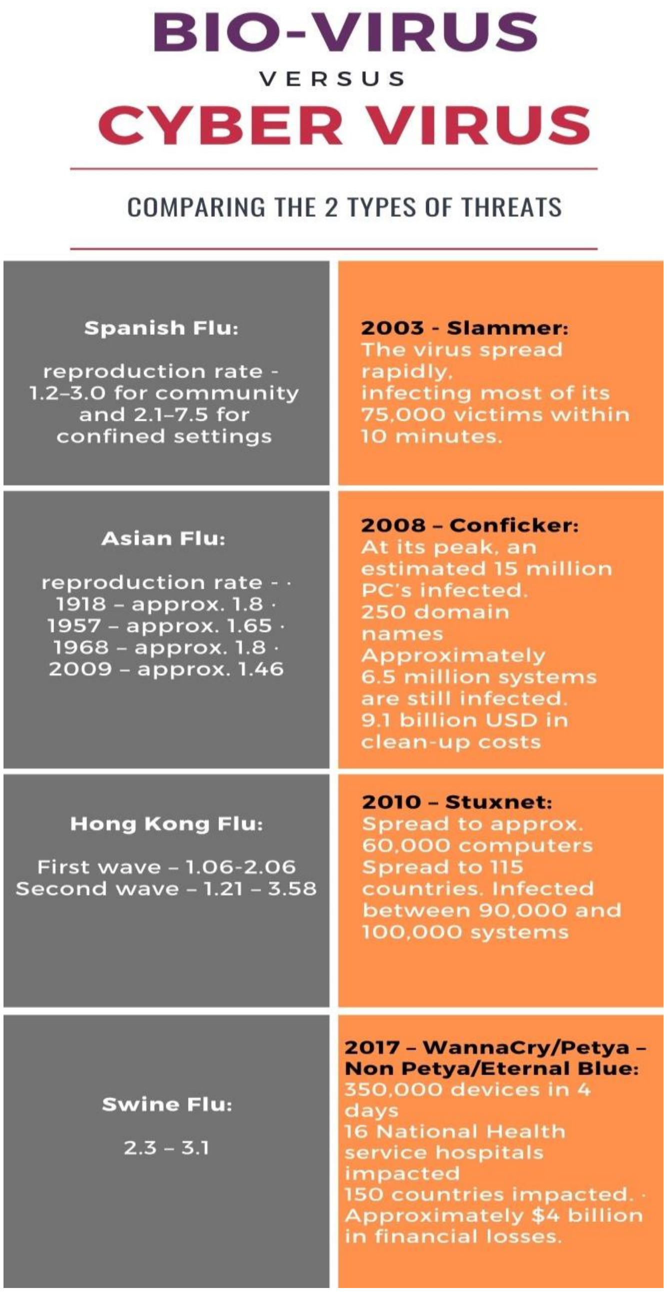
Comparing the infection rate of a biological pandemic to that of a cyber pandemic can help us understand the speed at which virus would spread across the globe and enable a greater understanding in terms of logistical readiness and in the case of a cyber event, enable planning on a granular scale ahead of any Disaster Recovery and Incident response planning post an event.

One of the lessons from the WEF note that a cyberattack with characteristics similar to the coronavirus would spread faster and further than any biological virus.

- The reproductive rate of COVID-19 is somewhere between two and three without any social distancing, which means every infected person passes the virus to a couple of other people. This number affects how fast a virus can spread; the number of infected people in New York state was doubling every three days before lockdown.
- By comparison the reproductive rate estimates of cyberattacks are 27 and above. One of the fastest worms in history, the 2003 Slammer/Sapphire worm, doubled in size approximately every 8.5 seconds, spreading to over 75,000 infected devices in 10 minutes and 10.8 million devices in 24 hours.
- In 2008 the Conficker worm spread to millions of unpatched PCs in 2008. It spread by exploiting a buffer overflow vulnerability in the Windows Server service. That flaw was patched by Microsoft on October 23, 2008 — 29 days *before* Conficker began its assault.
- In 2010 Stuxnet virus targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran. Stuxnet used four separate zero day exploits and hid inside systems for 18 months before attacking.
- The 2017 WannaCry attack exploited a vulnerability in older Windows systems to cripple approximately 230,000 computers in 150 countries within a four day period. Any systems that were unpatched and running old software would have been highly vulnerable to this type of attack and the consequences devastating.







Something as simple and easy to hide as a small USB drive can control our critical systems with just one mouse click. Attackers can determine when to release the virus once inside the network, for example the Stuxnet virus used four separate zero day exploits and hid inside systems for 18 months before attacking. Imagine if it were to be released now during this COVID 19 pandemic, it would not take much for the virus to become prevalent on a social networking application and without even knowing could spread rapidly.

A greater level of awareness and understanding of the critical risks are needed in order for us to maintain and secure our complex infrastructure. The challenges that exist today require the collective understanding and awareness to ensure we, as a society don't rely on technology alone to solve for a collective resilience.

Ask Taiwan's Digital Minister Audrey Tang, how to solve for COVID 19 and she will tell you ***"Reliable data is the foundation of trust".*** In an interview with WIRED correspondent, Adam Rogers, Minister Tang spoke about her vison to empower the public to take up the baton to build a safer Taiwan by releasing supply-chain data to the public and knowing that this ***data was an asset*** she asked civic-minded hackers to use it to help work their way out of a pandemic and that's exactly what they did. By building 140 applications that included real-time tracking of pharmacies and their locations where masks were still in stock and applications that identified how many masks had been distributed to the public and where. Providing the supply-chain data to the public empowered the people to find ways of getting the masks and other hygiene products to the rural areas where access to pharmacies was limited or non-existent. Only 150 people have contracted the virus to date with a national death toll of only seven proving that the real innovation and miracle comes when you empower people with the right tools and ask for their help to secure their own nation. People, Process, Technology and a young Minister's trust in her citizens secured Taiwan's future.

Key Takeaways

- WEF note that a cyberattack with characteristics similar to the coronavirus would spread faster and further than any biological virus;
- Learning from these lessons could enable planning on a broader scale, we could achieve a greater level of granularity around logistics required and know in advance where and what is considered critical and priority.
- Cybersecurity awareness and a strong understanding of our critical risks as a nation are needed right now to keep our critical infrastructure safe.
- We as a nation are taking too long to formulate our collective understanding to make any progress on a collective national resilience that will enable us to secure our citizens data, our communities and their businesses, our economy and our nation.
- We could all take a leaf out of Taiwan's Digital Minister Audrey Tang's book and trust our citizens to work with Government to recognise the value of reliable data and use it as you would other valuable assets, in doing so build the trust that is needed to enable real learning and cyber awareness to ensure we hand the batten over to our next generation and not the legacy vulnerabilities.