Australian Standfirst

Cybersecurity for Family Offices:

Edge Servers, Airgaps & Common Sense

Risk Management

9th March 2022, HFI#840

Stirling Larkin, CIO

During the 1640's the Dutch residents of New Amsterdam constructed a formidable twelve-foot defensive wall, which in 1664 was trounced by the British, whom simply ignored the fortification and invaded the fledgling city by sea. Today New Amsterdam goes by the anglicised name of New York, where that wall was dismantled the ruined stones were repurposed for a new thoroughfare famously known now as Wall Street.

As sapient as the newfangled cottage industry of cybersecurity appears to be, no number of newer technologies has substituted for the human element of common sense and for single plus multi- family groups, parsing what may be needed versus what has been promoted to them is as timely a deliberation as any before them in 2022.

Cite:- Why cyber security will be key issue in 2020s, 15 January 2020

Cite:- Automation, Artificial Intelligence & Bionic Markets, 1 March 2019

A vast majority of family offices are not nor need not be complicated entities and imposing complex digital systems over what is often vanilla operations only invites unnecessary attention and more importantly, trouble.

Cite:- How 'Algo'/DMA Traders Backstop Major American, Asian & European Markets: The Past, Present & Future Of Investing Without Surrendering Your Human Edge, 8 September 2021

Cite:- Looking For Opportunity In Meeting The Challenges Of Cybersecurity, 10 September 2016

In the United States, this was made abundantly evident with the 2017 Lender Management LLC v. IRS and 2021 Swartz v. United States cases, whereby the expenses and claimed deductions of two relatively significant family groups where challenged in relation to necessity for their engaged trade and businesses – though cybersecurity is the buzz word of now, expenses incurred are still expected to be proportionate to the infrastructure and data sets being protected.

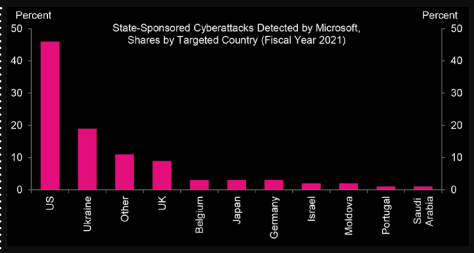
Insuring against the spectre of cyber intrusions has also become problematic for family offices in particular given their very existence as operational and commercial going concerns whom also manage pooled plus individualised investments for members ranging across multiple industries, asset classes and geographies.

Watch:- Bloomberg Kathleen Hays & Australian Standfirst Discuss Iran, Cyber, US Markets & Australian Bushfires, 18 January 2020

Cite:- Stress-testing The Bull Case For Israeli Tech In Australian Global Portfolios, 3 February 2021

Cyberattacks are malicious activity where an attacker attempts to harm an entity via its information and communications technologies.

Case in point, the landmark Merck judgment made public in February – during June 2017, inserted in an innocuous piece of tax software, a Russian virus known as "*Notpetya*" battered Ukraine before going rogue and worming its way from the computers of multinational firms with local outposts in Ukraine to their global operations, causing collateral damage to



victims ranging from Maersk, a huge shipping company, and Saint-Gobain, a French construction giant, to Mondelez International, owner of Cadbury chocolate.

Cite:- Power To Reprimand Russia Lies In The Hands Of Investors, 26 July 2014

The collateral damage was estimated in excess of US$10 billion, making it the costliest such attack to date and on 3 March, US FOMC Chairman Jerome Powell testified that cyber risk is the danger that the US Central Bank "*keeps its eyes on the most now*".

One of the most expensive blows of the 2017 intrusions fell on Merck, a New Jersey-based drugmaker whom subsequently lost forty-thousand computers in the blink of an eye and was forced to halt manufacturing of its human-papillomavirus vaccine.

Merck sought to cover its cyber-losses with a US$1.4 billion property-insurance claim, however, its insurers refused to pay, invoking a clause in the contract called war exclusion.

The matter ultimately ended up in a New Jersey court and Merck's insurers, including firms like Chubb, argued that there was ample evidence that *NotPetya* was an instrument of the Russian government and part of ongoing hostilities against Ukraine.

In other words, it was an act of warlike behaviour covered by the war exclusion and thus the court, sidestepped the question of whom was responsible for the assault.

Instead, it said that insurers did nothing to change the language of their contracts to suggest that the war exclusion included cyber-attacks and ergo it was reasonable for Merck to think that the exclusion applied only to "traditional" belligerence.

In response, insurers are now seeking to strengthen the language in policies to better shield themselves from payouts related to state-sponsored cyber-mischief.

But more nuanced than simply a question of deterrence, since the onset of the *Global Corona Crisis*, or *GCC*, there has been a significant shift in workforce habits both for operating businesses that family offices maintain but also specialised investment teams either inhouse or external, with more of these workforces working from home or working remotely, exposing these family groups to a much broader "*attack surface*".

One part-way solution to this *Achilles heel* has been the transition to air gapped remote working systems or if internet-based file or data sharing is essential, edge servers in lieu of generic cloud-based platforms.

Cite:- Edge vs Cloud Computing, 7 November 2018

Cite:- How Australian Investors Should Navigate Asia's Fintech Race, 8 May 2019

Edge computing architecture places high-performance computer, storage and network resources as close as possible to end users and devices; for an isolated Australia, this is not an immaterial factor.

This arrangement reduces the burden of data transport to the cloud, decreases transfer delays and increases locality, which common sense suggests aides' cybersecurity, especially with the spectre of *Sino* espionage and intrusions increasing across South East Asia.

Cite:- Military Conflict With China, 6 November 2019

Cite:- Taiwanese War & Markets Fallout, 30 January 2019

Cite:- Taiwan's Looming Crisis Is A Much Bigger Threat Than Markets Realise, 20 June 2018

With the opportunity for better productivity and efficiencies, the real potential of edge computing to displace the cloud has financial consequences for those already vested in cloud-aligned capital investments.

Air gapping in kind, albeit a blunt instrument for smaller single family offices working remotely, has several unique benefits including mobility, genuine privacy and is immune from the increasing threat of zero day attacks.

Ultimately for family groups the most significant cyber threats may emanate from within the established financial sector at-large, with the nascent but worrying moves of *Developed Market*, or *DM*, Central Banks towards *Central Bank Digital Currencies*, or *CBDC's*.

All eyes were on China's CBDC, the e-CNY, during the Beijing Winter Olympics Games, with the US Federal Reserve testing akin via their overly-pensively dubbed "*Project Hamilton*" and Australia's Reserve Bank's stupidly named equivalent, "*Project Atom*".

In cyberspace, adversaries are growing more sophisticated and outpacing advancements in policy, education, and defence technologies and thus during an era of great-power hegemonic competition, it is a clear and present danger to all money managers if all official fungible wealth is digitalised, which no family group or individual can ringfence nor cyber protect at a state-actor level; the intrusion of State in the affairs of the individual have, without question, gone well *beyond the pale*.

Cite:- Socialism Lacerates Australia: Wealth Creation Without Liberty Is Extralegal Servitude In All But Name, 21 September 2020

To boot, States are increasingly turning their attention to developing quantum computers to gain a technical edge in cybersecurity, intelligence operations, and economic industry.

Cite:- Quantum Supremacy: Complicated Technologies Define Realpolitik, Hegemony & Wealth, 22 October 2020

Cite:- Chinese Internet Megatrend Going Global, 4 December 2018

Quantum computers are highly advanced machines that can solve complex maths problems like factorising large numbers and performing unstructured searches exponentially faster than conventional computers.

Although the practical applications of quantum computing aren't quite here yet, theoretically they hold tremendous potential for philanthropy, artificial intelligence, machine learning, financial market analysis but also ominously cyber-attacks and cracking digital currency private keys.

Cite:- The Lucrative Investment Question Of Our Time: Chinese Technology – Sino Semiconductors, Digital 元 & Cyber-Sovereignty, 26 April 2021

Cite:- Is Investing In Bitcoin Really A Good Idea? Question Marks Remain, 1 November 2017

As Henri Frederic Amiel concluded, "*Common sense is composed of experience and prevision; it is calculation applied to life*".