Investment Insights

June 30, 2023

Cybersecurity: The Virtual Threat is Real

"Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense."

White House National Cybersecurity Strategy, 2023

IN A NUTSHELL

- As global activity continues to shift online, vastly more human behavior is today being conducted in digital environments whose safety is in jeopardy - cyber criminals pose a sophisticated, and growing, danger to countless activities.
- Fortunately, policy makers, corporations, and individuals are taking these risks seriously, and, although new cyber threats from innovative and evolving forms of attack continue to proliferate, the resolve to fight cyber-crime clearly exists.
- For the investor, three things are critical considerations : understanding the scope of the problem, discerning the spending plans and strategies of those most impacted, and accessing ownership to companies that will provide solutions.

I'm From the Government, and I Need Help

The U.S. government is not generally given to exaggeration. And that sobering thought puts a lot of weight on the above quote which is taken from the President's signed introduction to the *White House's National Cybersecurity Strategy* [1].

The clear and critical role that cybersecurity will play in the U.S. (and therefore globally) is abundantly evident from the report, which, it must be said, evokes a degree of sympathy for the Luddite mentality. A brief mention of the purported benefits of technology, is followed by a damning list of its deficiencies, from theft of property and data, through the dissemination of misinformation, harassment, and exploitation, to violent extremism and threats to peace.

The point though is that these are the unfortunate, but inescapable, realities of a cyber world which is advancing at a breakneck pace. And idly wishing for a return to a simpler world (which, to be fair, also had criminality) is neither realistic, nor useful. A better approach is the one that the government is laying out – to be painfully aware of the problems, but to resolve to fight them.

The final section of the report discusses this fight, and we believe it is arguably the most relevant for investors. It contains this quote:

"Building a more defensible and resilient digital ecosystem will require generational investments by the Federal Government, allies and partners, and by the private sector."

This last point is important. What the government appears to be saying, and we would agree, is that the solution to cybercrime will need both a public, and a private market, solution.

The title of this section alludes to Ronald Reagan's notorious assertion that the scariest words in the English language are spoken when governments show up to assist ("I'm from the government, and I'm here to help"). Our take, on reading the Cybersecurity Strategy document, is that, in the case of cybercrime, the government is at least as aware of the need to seek help too. For an investor hoping to identify areas of the broader economy that could grow at a faster rate than others, this should be interesting.

[1] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Lopping off the Hydra's Head

Government officials are not the only ones who are worried. According to a recent report from McKinsey & Co[2], there are three key metrics to consider.

The first is the sheer scale of the problem. They forecast that the economic cost from cyber-crime will grow to US$10.5tn by 2025, representing around a 300 percent increase from 2015 levels. At the same time, as Figures One and Two demonstrate, the total number of incidents, and the average cost per incident have also increased, with what appears to be a lurch higher that coincided with the pandemic (perhaps cybercrime lends itself nicely to work from home?). Of course, part of these trends are explained by increases in inflation and economic activity over the same period, as well as the proliferation of digital activity in society, but the point remains – cybercrime is becoming more pervasive, and more expensive.

The second is the gulf that exists between this economic cost, and the amount that organizations globally are actually spending on cybersecurity solutions. McKinsey estimates that this spend was at around US$150bn in 2021. They rightly note that *"such a massive delta requires providers and investors to "unlock" more impact with customers",* and that *"the current buyer climate may pose a unique moment in time for innovation in the cybersecurity industry."*

On this second point, the World Economic Forum's *Global Cybersecurity Outlook 2023*[3] provides some equally concerning reading. Amongst other sources, they received 117 survey responses on the topic of organizations' Cyber Outlook. The gulf in preparedness is highlighted when one considers that, although 86% of Business Leaders believe that "a far-reaching, catastrophic cyber event is at least somewhat likely in the next two years", only between 27-36% were confident that their organizations were "cyber resilient", with the range depending on the frequency with which the issue was discussed internally. More optimistically, the report highlighted the growing trend for Chief Information Security Officers (CISOs) to report directly to CEOs, a sign surely of the increasing weight that leaders are putting on this role, and its remit.

Aside from the scale of the problem, and the gulf in addressing it, there's a final important point with cyber-crime, and the title of this section alludes to it. Just as the many-headed Hydra of Greek myth grew two more heads each time one was cut off, so cyber-crime proliferates. McKinsey surveyed 4,000 companies, and found that nearly 80% of the "threat groups" (i.e. the bad actors), that were identified in 2021, had not been seen before. The same was true for 40% of the identified malware. The point the companies were making is that this is an area of criminal activity that is not just *growing* rapidly, but also *evolving* rapidly. The victors in such a war therefore will likely have to be nimble, prescient, and well-resourced.

Investing in the E-Sentinels of Tomorrow

In an ideal world, there would be no need for cybersecurity solutions, or companies that provide them. But, unfortunately, that is as redundant a sentiment as its real-world equivalent that we shouldn't need police, or the military. The inescapable fact is that cyber-crime is becoming more prevalent, not less. For investors and for society, owning a broad swathe of companies that are providing solutions to cyber-attacks can be a potential win-win, offering the prospect of a commensurate return on capital, and, at the same time, enabling firms to fund the innovation and growth that cybersecurity necessitates.

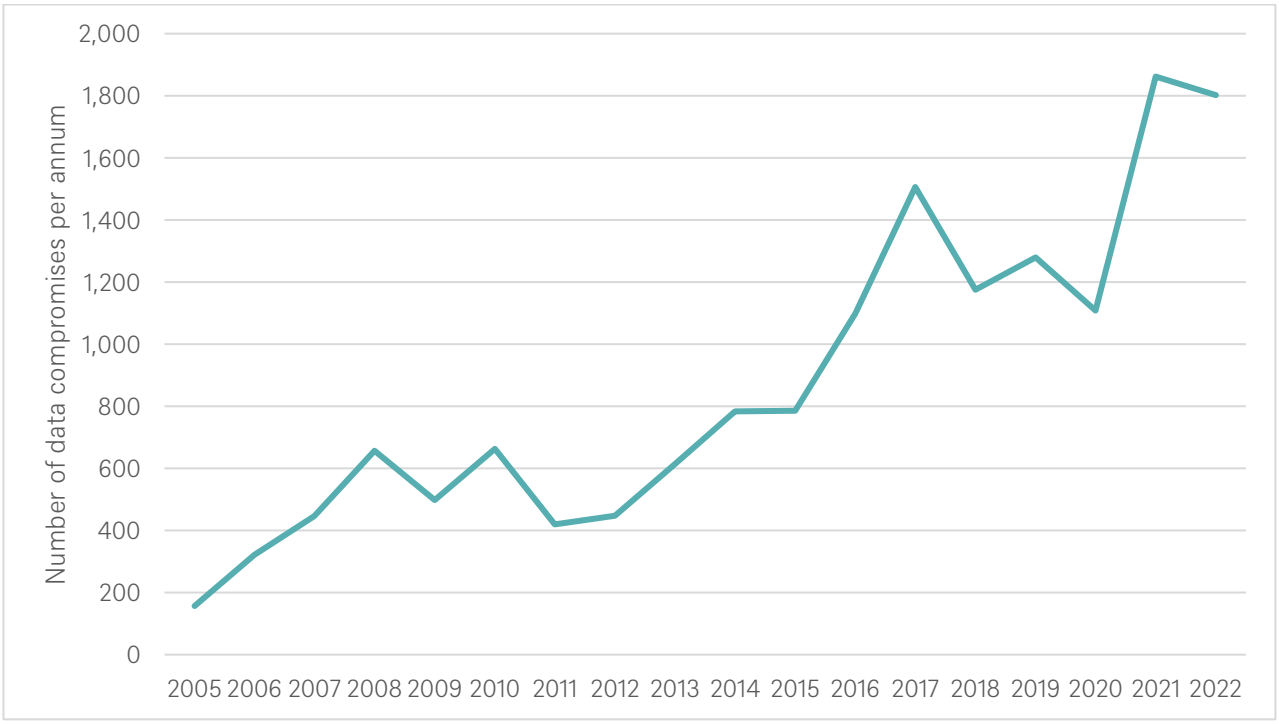
Our view is that thematic investing can play a role for investors if they have conviction that a specific segment of economic activity has the potential to outgrow the broader economy, or if the revenues, profits, and, ultimately, share prices of the global companies involved can do the same. Of course, to make such a prediction about cybersecurity providers is a daunting challenge, but we re-emphasize the three points from this note that at least make that viable:

- As ever more activity shifts into the digital world, the scope of the threat from cyber-crime and digital attacks is growing fast. This is well recognized by governments, supra-nationals, think tanks, companies, and individuals.
- There is a gulf today between the economic cost of cyber-crime, and the amount that is being spent on solutions. Market saturation appears a long way off.
- The insidious innovation that cyber-criminals demonstrate suggests that solutions will also need to evolve. That ought to mean that companies involved in creating these solutions will likely remain relevant for as long as cyber criminals can remain ingenious. And, that, we hope, can be good news for the companies and their investors, and bad news for the criminals.

[2] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers#/

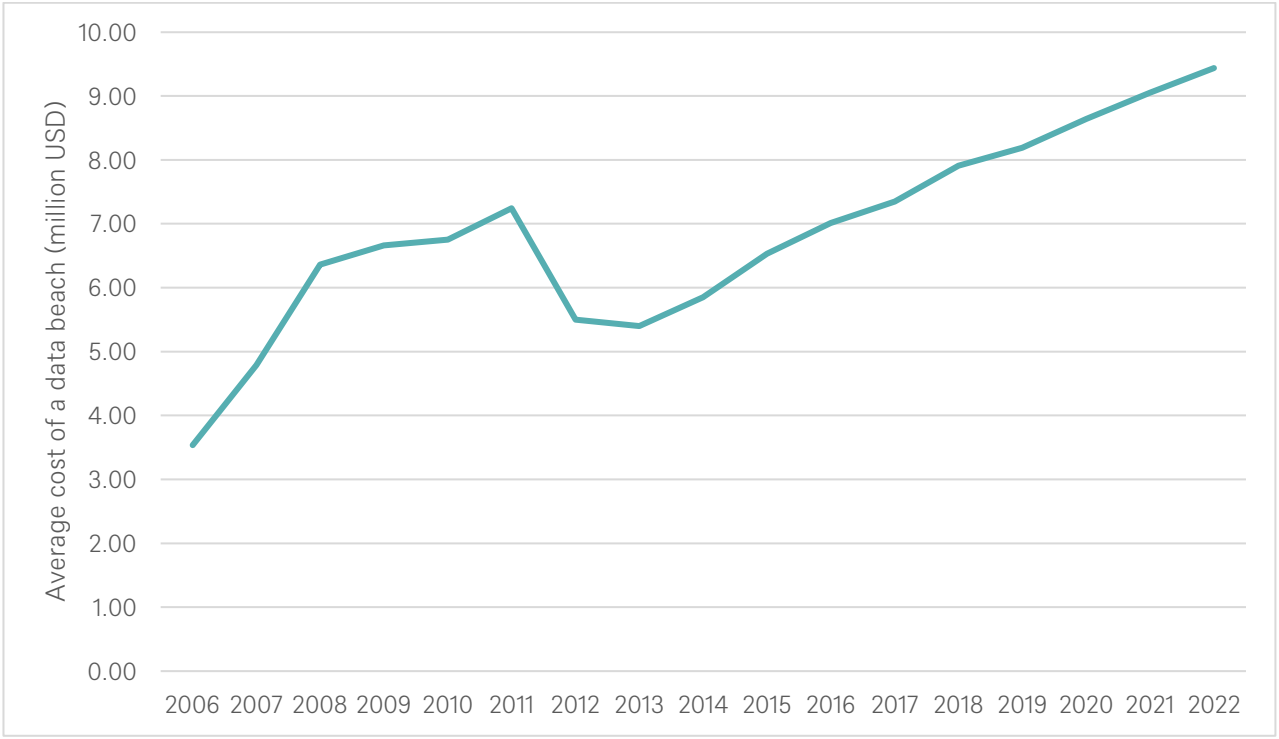
[3] https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

Figure One: Annual number of data compromises in the U.S. from 2005 to 2022



Source: Statista as of January 2023.

Figure Two: Annual cost of a data breach in the U.S. from 2006 to 2022



Source: Statista as of January 2023

DWS Distributors, Inc.
222 South Riverside Plaza Chicago, IL 60606-5808
www.dws.com service@dws.com
Tel (800) 621-1148