Have You Experienced "Tool Sprawl" in Cybersecurity?

Published September 8, 2022

Christopher Gannatti, CFA
Global Head of Research

We know we have a diverse array of readers:

- Individual business owners
- Employees of large companies
- Employees of much smaller companies
- People who are retired or between jobs

Whatever your situation, how many different cybersecurity tools are you aware you interact with? A password manager? A single sign-on interface? A specialist tool focused on email? Another specialist tool focused on accessing cloud computing infrastructure?

The fact is, the more you learn about cybersecurity, the more you are awakened to a large number of providers, each specializing in different types of cybersecurity products. We saw the term "tool sprawl" used to describe the 2022 cybersecurity landscape—we thought it painted an informative picture.1

How Many Tools Are Customers Using?

Enterprise customers may be managing 60–80 tools, with those on the higher end of the spectrum possibly managing up to 140.2 Imagine dealing with all those tools in the course of normal business operation.

One reason the current environment is characterized by so many tools could relate to the progress of the chief information security officer (CISO) role. Ten years ago, the way a "good CISO" was defined largely had to do with buying and deploying tools. The CISO in 2022 is now evaluated based on outcomes rather than deploying tools, and is much more a top priority for a company's board.3

A survey done by Gartner found that 88% of boards of directors view cybersecurity as a business risk rather than a technology risk.4

Of course, the attack surface in 2022 has also massively expanded, and companies may frequently launch around new types of artificial intelligence and machine learning techniques, to use one example.5

Dealmaking Is Already Taking Off in 2022

Through August 18, 2022, private equity sponsors and their portfolio companies have backed 162 cybersecurity deals worldwide, valued at $34.9 billion. If this pace continues, it has the potential to surpass 2021's tally of $36.4 billion across 308 transactions.

One driver of this growth—valuations. In 2020 and much of 2021, the most newly public cybersecurity companies, many of which were focused on the cloud, experienced massive multiple expansion and therefore helped fuel valuations. The growth was strong, but the prices were not inexpensive in an environment where the cost of capital had been low for a long time.

With the rise of inflation and then the shift in policy of many central banks, going away from expansionary support of growth, many of these companies experienced dramatic multiple compression. This has helped private equity players focused on building consolidated product offerings to pick up interesting companies at much lower prices.

Thoma Bravo is one such player that has been quite active. Just in the identity space, Thoma has done deals to acquire Ping Identity for $2.8 billion and SailPoint for $6.9 billion.6

Consolidation is a big desire from customers—possibly a response to the tool sprawl that we mentioned earlier. There is a feeling in the market that there might already be too many companies, so it's not just about more innovation but also building integrated platforms so customers can go to one place and get more baskets of services.

Option3 is an example of a firm that has shifted from funding new firms to acquiring late-stage middle-market companies for buy-and-build strategies. They are planning to raise a $250 million buyout fund dedicated to a platform acquisition strategy.7

Private equity firms are attracted to cybersecurity companies for many reasons, but they have exhibited lower churn rates than other Software-as-a-Service (SaaS) businesses. They also have tended to generate high margins.8

What about the Slowing Economic Environment?

As with many things, historical comparisons can only take us so far. If we think about the state of cybersecurity in 2007–2009, encompassing the Great Recession, it was totally different. Cybersecurity budgets are much different in 2022 than they were in 2007 heading into that significant slowdown.9

One doesn't need to look too far to see quotes from industry leaders indicating that even if cybersecurity spending is impacted by a slower economic environment, it most likely wouldn't be impacted as much as other areas. There are many things that are regulatory requirements or viewed as 'table stakes' to the ongoing operation of companies, making them difficult to cut.

The Securities and Exchange Commission has explored a rule that would require disclosure of a "material cybersecurity incident" in a public filing. Disclosure would likely have to be made quite quickly after the event—possibly a response to certain types of attacks and breaches like SolarWinds, where months after the fact the scope of potential damage was growing and growing.10

Regulations aimed to combat cybersecurity threats are likely to have that impact.

Conclusion: A Megatrend for All Seasons?

Norges Bank Investment Management, the world's largest sovereign wealth fund at $1.2 trillion, recently indicated that cybersecurity is their biggest current concern, noting that it faces an average of three serious attacks each day. The fund sees roughly 100,000 attacks per year, and they classify about 1,000 of them as serious.11

Firms operating in the financial industry have been increasingly targeted, and firms operating in the Nordic region feel the proximity to Russia during the Ukraine conflict quite tangibly.

While many investment themes might be a bit discretionary or susceptible to delays in a slowing economic environment, we believe cybersecurity is not one of them. We may not know the exact companies or services that will grow the fastest, but backing away from focusing on security is generally not an option. For investors seeking to implement an investment strategy focused on the future of cybersecurity offerings, consider the WisdomTree Cybersecurity Fund.

1 Source: Kyle Alspach, "Thanks to the Economy, Cybersecurity Consolidation Is Coming. CISOs Are More than Ready," *Protocol*, 6/17/22.
2 Source: Alspach, 6/17/22.
3 Source: Alspach, 6/17/22.
4 Source: "Gartner Survey Finds 88% of Boards of Directors View Cybersecurity as a Business Risk," *Gartner*, Press Release, 11/18/21.
5 Source: Madeline Shi, "PE Dealmaking Thrives in Cybersecurity Sector," *Pitchbook*, 8/23/22.
6 Source: Shi, 8/23/22.
7 Source: Shi, 8/23/22.
8 Source: Shi, 8/23/22.
9 Source: Kyle Alspach, "Cybersecurity Spending Isn't Recession-Proof. But t's Pretty Close," *Protocol*, 6/6/22.
10 Source: Kyle Alspach, "'Game-changer': SEC Rules on Cyber Disclosure Would Boost Security Planning, Spending," *VentureBeat*, 3/10/22.
11 Source: Adrienne Klasa & Robin Wigglesworth," *Financial Times*, 8/22/22.

Christopher Gannatti is an employee of WisdomTree UK Limited, a European subsidiary of WisdomTree Asset Management, Inc.'s parent company, WisdomTree Investments, Inc.

As of September 7, 2022, WBCR held 0%, 0%, 7.14%, 0% and 0% of its weight in Thoma Bravo, Option3, Ping Identity, SailPoint and SolarWinds, respectively.

Important Risks Related to this Article

There are risks associated with investing, including the possible loss of principal. The Fund invests in cybersecurity companies, which generate a meaningful part of their revenue from security protocols that prevent intrusion and attacks to systems, networks, applications, computers, and mobile devices. Cybersecurity companies are particularly vulnerable to rapid changes in technology, rapid obsolescence of products and services, the loss of patent, copyright and trademark protections, government regulation and competition, both domestically and internationally. Cybersecurity company stocks, especially those that are internet-related, have experienced extreme price and volume fluctuations in the past that have often been unrelated to their operating performance. These companies may also be smaller and less experienced companies, with limited product or service lines, markets or financial resources and fewer experienced management or marketing personnel. The Fund invests in the securities included in, or representative of, its Index regardless of their investment merit and the Fund does not attempt to outperform its Index or take defensive positions in declining markets. The composition of the Index is heavily dependent on quantitative and qualitative information and data from one or more third parties, and the Index may not perform as intended. Please read the Fund's prospectus for specific details regarding the Fund's risk profile.

Statements concerning financial market trends are based on current market conditions, which will fluctuate. References to specific securities and their issuers are for illustrative purposes only and are not intended to be, and should not be interpreted as, recommendations to purchase or sell such securities.