MERGERS & ACQUISITIONS

SEPTEMBER 25, 2022

Technology Stalwart Goes All in on Cybersecurity

RICH BLAKE

Already investing heavily on the growth prospects for cybersecurity – because the threats keep coming and the stakes are ever-higher – Thoma Bravo announced in early August it was all-in on Ping Identity, a leading provider of identity access management services to enterprises worldwide. Ping's mission statement is to protect a company's employees as well as its customers and suppliers to ensure every digital interaction is safe and seamless. It's a bustling space that is not without competition but is being buoyed by digital transformations and the move to the cloud. We interviewed Thoma Bravo's Chip Virnig below.

Chip Virnig

"Ping Identity is well-positioned to capitalize on opportunities in this area," says Chip Virnig, a partner at Thoma Bravo. Virnig went on to say that the market in which Ping competes represents one of the highest growth categories of the broader $170 billion cybersecurity industry.

The Ping take-private deal, valued at $2.8 billion, is expected to close by the end of the year. It follows several high-profile Thoma Bravo acquisitions in recent years, including the acquisitions of Sophos (next gen endpoint and network security), Proofpoint (email security category killer) and Sailpoint Technologies (identity governance and administration).

"We're talking about a $170 billion annual spend by corporations on a sector that has 35-plus sub sectors," Virnig said in a phone interview on the day that the Ping deal was announced. "Yes, we're betting big. It's a massive industry that is not going anywhere. All the issues of a decade ago are all still relevant today. But there are new issues such as operating in a multi-cloud environment, the Internet of Things, remote work and ransomware. So yeah, it's endless."

Virnig, a Brown University graduate, cut his teeth as a multi-industry analyst in the investment banking division at Merrill Lynch. He decamped for Thoma Bravo in the summer of 2008. That was just weeks before Merrill collapsed during the global financial crisis and was absorbed into Bank of America. Among the first big deals Virnig worked on at Thoma Bravo was the firm's $2.4 billion acquisition of mainframe giant Compuware in 2014. In 2019, Thoma Bravo spun out Dynatrace from Compuware in a successful IPO and subsequently sold Compuware to BMC Software, a KKR-owned holistic-IT-solutions-focused company.

Over the last 14 years, Thoma Bravo has emerged as one of the most active investors in cybersecurity and they don't seem to be slowing down.

Virnig took time out to speak with Mergers & Acquisitions. They discussed some of the emerging trends in cybersecurity, including aspects that have him brimming with optimism about the sector – and some things keeping him up at night.

If you were a CISO, building a big corporation's cybersecurity from scratch, what would it look like?

Virnig: No one builds these things from scratch but hypothetically you would start with protecting your network and your endpoints via next-gen endpoint and next-gen firewall. Those two categories sort of gave birth to the cybersecurity market 30-plus years ago and remains the largest category of cyber spend to this day. From there you would then need to go into a myriad of subcategories including, but not limited to, managing identities, securing applications, encrypting data, enforcing public cloud posture and protecting email/digital communication channels. I mean, conceivably, you would need at least 35-plus vendors to cover today's current threat landscape. It is not uncommon for large enterprises to deploy 50 unique cybersecurity solutions in a given year. 'Oh, sorry we got hacked, I was just trying to consolidate our relationships' is not something the CISO can say to the board. This is an area where best of breed matters and you can't make any excuses such as trying to save money. Sadly, when companies face major breaches, the CISO often gets fired.

Do you see some consolidation, eventually?

Virnig: Our thesis is that this is going to remain heavily siloed for the foreseeable future. You will certainly have some large category killers that dominate a market and some adjacencies, but you will not see any vendors successfully serve as a "one-stop shop" for all things cyber. That thesis has failed multiple times over the past decade and the stakes are now higher than ever.

How does the move to the cloud impact cybersecurity?

Virnig: Large complex enterprises have built policies and protocols specific to the needs of their heterogeneous on prem infrastructures for the better part of 50 years. These same companies are also in the early innings in their journey to the cloud, but the issue is how do these companies enforce the same policies and protocols that have protected their [on-premises] infrastructure for decades into their newer and faster growing cloud infrastructures? This gets even more complicated for large enterprises which are deploying a multi-cloud strategy and balancing this with their existing on prem infrastructure. There is nothing scarier from a security perspective than maintaining best-in-class cybersecurity for a hybrid-plus multi-cloud environment, unfortunately none of this is seamless. Machine learning and AI will have a role to play, taking threat assessments and allowing teams to be more proactive in detection, but this is a monstrosity of a to-do list. The shift to the cloud is here to stay and makes IT hugely more efficient, but let me tell you it's increasing the threat landscape significantly for the cybersecurity industry. There's no magic bullet.

It sounds as if cybersecurity threats are growing alongside the complexities of trying to combat them, and that the bad guys know this ... what chances do the good guys even have to prevail?

Virnig: Companies know that they'll never be able to prevent cyber breaches 100 percent of the time. They'd settle for 95 percent. The real issue is, if you do get hacked, how soon can your team figure out that it happened? And then, how long before there is a response, to mitigate the situation? When you read about a hack, and often companies don't make this public for weeks, by that time the culprit is long gone. These guys are too good. The damage is already done. What's really scary is that the underground industry for selling personal data has gotten so large that it's now motivating smart programmers to build their own malware to sell to cybercriminal organizations. So now you have incredibly talented software engineers effectively becoming "digital arms dealers." So it's not if you get hacked, it's when, which is why cybersecurity is now firmly embedded in corporate budgets.

Knowing what you know about this sector, and the many rising threats, what are your worst-case scenarios?

No shortage of them. Given everything is this world is a "connected" device, nothing is off limits. We've all read stories about hackers showing they can take control over everything from a car to a pacemaker. We've seen actual hackers compromise gas pipelines and national grids. I don't want to paint a doomsday scenario, but without effective cybersecurity we could be living in a James Cameron movie. "Judgment Day" isn't that much of a stretch. We are seeing a big increase in nation-state attacks year-after-year. Most recently, the entire cyber industry saw a huge uptick in targeted campaigns by Russia during the early phase of the war. It's everything you could imagine and, unfortunately, stuff we can't yet even fathom.

Besides Cloud Security and Identity, what are some other subsectors to watch?

One thing that has become very clear since the pandemic is no matter what best-in-class cybersecurity solutions you have in place, you are only as strong as your weakest link. People-centric security solutions can never be overlooked, and this goes beyond identity access management. We have been very bullish on the e-mail security market for the last five years with our investment in Barracuda Networks and most recently Proofpoint. During the pandemic, the number one cause of ransomware was targeted spearfishing attacks via e-mail. E-mail security has been around for a long time but is more important than ever. All it takes to completely undermine a world-class CISO's best of breed cybersecurity infrastructure is one employee clicking one bad link in an e-mail. Another category we are big believers in would be dev sec ops. The thesis there is that as every company is becoming a software company, their digital footprint is increasingly exposed to attack.

Hackers can now break into a bank by finding a vulnerability in the code underlying a bank's website. That wasn't as much of a risk 15 years ago.