Exchanges at Goldman Sachs

Cybersecurity Deals Surge Amid Rising Attacks

Marco Poletti, Head of Cybersecurity Investment Banking, Investment Banking Division, Goldman Sachs

David Campbell, Managing Director in Growth Equity, Goldman Sachs Asset Management

Allison Nathan, Host, Goldman Sachs Research

Recorded: June 8th, 2022

Allison Nathan: The scale and sophistication of cyber-attacks are rising exponentially, but so are the levels of investment, innovation, and corporate activity in the space.

David Campbell: There was over $30 billion invested in cybersecurity companies last year, so it is a very well-funded space from the investment perspective.

Allison Nathan: I'm Allison Nathan, and this is Exchanges at Goldman Sachs.

Amid heightened geopolitical tensions and slowing economic growth, the world is bracing for a surge in cyber-attacks, so what are companies and investors doing to prepare? To help us understand the key issues, I'm sitting

down with David Campbell, who invests in growth equity companies, many of which are cybersecurity startups, for our asset management division, and Marco Poletti from our investment banking division, who's been involved in recent M&A deals in the space. David, Marco, welcome to the program.

David Campbell: Thank you.

Marco Poletti: Thank you.

Allison Nathan: So every day it seems like we're hearing of yet another cyber-attack that is wreaking havoc in some way on society, so just give us a sense of the scope of these attacks today and how the cybersecurity market has evolved. David, maybe you can start us off.

David Campbell: Yeah, with economic, social infrastructure and government value moving into our computer systems, we expect that the cyber-attacks are going to be a permanent part of our ongoing computer life. So how has it evolved? It's moved from an annoyance to now where it's really an organized business. I think a recent McKinsey study estimated that the amount of cyber-

related losses will move from 6 trillion last year to over 10 trillion in 2025. Now, that's over 20% CAGR, and that the spend to try and defend against these attacks is going to rise to over $100 billion in 2025. So I think that cybersecurity is going to be a core part of our ongoing online presence.

Allison Nathan: And we're not only expecting to see the number of attacks increasing, but how is the environment changing in terms of the overall surface area that's vulnerable to these attacks, given all the shifts we're seeing today in terms of moves to the cloud, the digital transformation, the fact that people are just working remotely more?

David Campbell: Yeah, the attack surface has expanded dramatically. You know, we've moved from the data center to a very diversified set of end points and computing platforms. You've got mobile. You've got Web, cloud, SAAS, IoT, and OT, so attacks are happening from all points where you touch a computer system these days. This has made it easier for cyber criminals as they now have more places where they can enter the system and infiltrate into the computer systems, and it's made it much,

much harder for the cybersecurity professionals who are trying to defend all these points because they're no longer in one place. They're very diversified, and they often don't control large parts of those systems so they now need to defend.

Marco Poletti: Yeah, I agree with David. I would say, look, you have more data to protect. There's more ways to access that data, so that results in data attacks being more vulnerable. And by the way, that's true for consumers, you know? We live more and more of our lives in a digital world. We have more data saved in the cloud, and that just makes it riskier for us.

Allison Nathan: And so we've also had geopolitical developments this year. Russia's invasion of Ukraine. Rising geopolitical tensions in other parts. So has that raised the risk of further attacks? Or are there drivers as well behind this rise in attacks and in more places?

Marco Poletti: That's a really interesting question because, if you look at where most of the attacks are coming from today, it's really not from nation-states. It's from organized crime. And when you're looking at the war

in Ukraine, we haven't really seen nation-state-driven cyber-attacks come out of Ukraine to the rest of the Western world yet. It's interesting, I was in Israel meeting with a number of my clients a month ago, and the general view was that that cyber war at the nation-state level hasn't really happened yet. And look, we obviously don't know where the Ukraine War is going to head into and the further developments that we may say, but there is a scenario where Russia uses cyber warfare as a way to fend off the sanctions and any potential escalation. And frankly, I think that's the reason why there's been guidance from governments all across the Western world to have essentially all companies in a, quote/unquote, shields-up mentality because it may come.

David Campbell: I would add onto that it's quite interesting, when you look at nation-states, they've developed a lot of cyber weapons. They don't want to use them because, once you use them, you expose them and then you start to build the fences for them. So they use them fairly sparingly. But one of the interesting things in the Ukraine attack was how the group Conti, one of the cyber-criminal groups, helped Russia to attack the Ukraine, scraping texts and infiltrating information. The

interesting thing is that Conti was estimated to have $180 million of revenue last year on $6 million of expenses. I mean, if we could build a business like that, we'd be doing very well.

However, they also have the advantage that they do something like this, and it hurts their business model because now people don't want to pay their ransomware. And so they just rebrand overnight, and so they're splintering into multiple rebranded groups who are now coming back into the market. Same tools, same people, different name.

Allison Nathan: Interesting. But if we take a step back and talking about these trends in terms of increased attacks, greater sophistication, are the tools in general keeping up with this onslaught?

David Campbell: Look, I would say that, as you look at any conflict zone, there is a constant evolution of both the attacks and the defenses, and the defenses are evolving. The challenge is, as it's always said, the attackers only have to get through once and succeed once; the defenders have to succeed 100% of the time. And that's a

very uneven playing field. I think the other challenge we have is with the black market and so much money now in cyber-attacks that the criminals have an increasingly sophisticated tool set that's evolving much quicker.

So some of the changes that we've seen in the market is that we are starting to see AI and ML technology leak into the cyber defense space to try and keep ahead of the attacks that we don't know. And then more of a support infrastructure we're starting to see things like software supply chain security tools starting to come in that are helping downstream users of these technologies to be safer.

Allison Nathan: And Marco, do you have thoughts in terms of areas of innovation that you're seeing to defend against these attacks?

Marco Poletti: Yeah, definitely. And I would say it's a very dynamic environment today where I truly think we have entered into a new wave of innovation for cybersecurity. And I would say that a couple of themes that I would mention, one is around cloud security. We were talking about that earlier. More and more data is being moved to the cloud. More and more workloads are

being moved to the cloud. And so because of that new wave of computing, we just need new ways to secure that. And so there are a lot of startups today that are trying to address the problem of cloud security.

And the second theme I would mention is really just around bringing more protection into the software development life cycle because, if you think about it, everything being built on software, the easiest way to secure that software is actually to bring real-time runtime protection of that software as it's being built. And so I would say those two areas are probably one where we're seeing a lot of investments, a lot of innovation, and a lot of venture capital focus. And David, I'd be curious to get your perspective on those, too.

David Campbell: Yeah, of course. And it's quite interesting because, as we've seen more and more sophistication come into the tools, it's still the best defense that a company can still bring to its environments is education. So we have seen a rise in various companies that are focused on helping to upskill end users, helping to upskill the security professional, and helping to upskill developers. And then on the other side of it, the other

innovations we're seeing the simplification of the cybersecurity stack. As the number of places where you can be attacked and the type of attacks you can have, that's brought a lot of complexity into the defense. And so companies who are starting to simplify that security stack make it easier for businesses to provide a comprehensive security platform for their environment is the other place I think we're seeing some real innovation. And I think that will continue over the next few years.

Marco Poletti: I agree with you. I think that last thing is extremely important. If you think about it, just in the US, there's something close to 2,000 security vendors. At RSA, which is the largest cybersecurity conference in the world, which is happening this week in San Francisco, there's something like 300 new vendors. And so companies and customers of cybersecurity really need help in simplifying their security stack to actually really be able to have a security [UNINTEL] that works.

Allison Nathan: And that level of innovation is also leading to a surge in cybersecurity M&A deals. And Marco, you've worked on a number of these deals. From your perspective in investment banking, what does deal activity

look like? And do you expect the pace of transactions to continue? Where do we go from here?

Marco Poletti: Yeah, and maybe to put that in numbers, we saw about $70 billion of M&A volume for cybersecurity in 2021, and that number was four times what we saw in 2020. And the short answer to your question is I would expect that that level to stay at a relatively high mark for the foreseeable future. And there's really two main reasons for that. The first one, when you think about security for large corporates, security has really become a horizontal priority that is frankly a requirement in order to do everything else their business does. And because of that importance of security for companies, that has made large plat providers really being more focused on the space. And I would expect them to continue growing inorganically to really acquire more protection mechanisms that they can then offer to their own customers.

And on the other side, you have financial sponsors which have become very active in cybersecurity. The reason for that is I think the financial model and the business model for cybersecurity companies is extremely resilient and

extremely durable, which are obviously two characteristics that financial sponsors tend to like, and so that's the reason why idea also think that, from that universe of financial investors, we'll see them doing more in cybersecurity.

Allison Nathan: Well, let's talk a couple of minutes about the investment landscape. David, you invest in cyber startups within asset management. How do you think about investing in cybersecurity? What's your strategy?

David Campbell: Yeah, well, look, there was over $30 billion invested in cybersecurity companies last year, so it is a very well-funded space from the investment perspective. And the challenge is there are literally thousands of businesses out there. The way we approach it is we're looking for things that have some longevity because typically valuations are quite high even in very early stages of these businesses. So we're looking for companies that we think either address a very new space in a novel and defensible way or things that could grow into being part of the security platform and in and of themselves a platform.

We try to avoid better mousetraps. And it's not because better mousetraps aren't good, and then there's some really valid technology developed there. But it's very hard to grow them into a large business over time because, soon enough, with such a dynamic environment, you'll need an even better mousetrap in the future. So that's a tough place to be.

We have focused a lot on AI and ML. We've looked at that space. I think there's some really interesting technologies coming out of that. We've looked at technologies and companies that help simplify that cybersecurity stack, particularly for the low end of the market where it's just overwhelming. You can't hire cyber professionals. There's a lack of them. And you can't really keep up with the complexity of the environment. So I think that's really important.

And then the other place which we discussed earlier on is we look at new areas of the attack surface. Certainly SAAS I think has become an incredibly important space, and we've been looking at a number of businesses in that space. And then you look at things like the collaboration

environment. We've seen workflows move out of email into collaboration environments, and collaboration environments are far more dispersed so they're very difficult to defend. And so these are some of the spaces where we've been focusing on.

Allison Nathan: But if you think about the investment environment more broadly, it's obviously quite challenging across the markets, and cyber is one of those areas where people are still quite excited about so competition's intense, valuations are high. So it's a challenging investment environment, correct?

David Campbell: It is. We looked at hundreds of businesses last year, and I think we made two, maybe three investments that you could call cybersecurity related. So it's a really tough environment. It is very competitive. You tend to have to focus on things that you really believe have some longevity and defensibility to them.

Allison Nathan: Right. And in general, has that changed the way you're thinking about investing or changed your criteria at all in this pretty challenging environment?

David Campbell: Yeah, absolutely. I mean, one of the things you have to do, when a company becomes obvious as a new pillar in the cybersecurity world, its valuation becomes out of reach, and it's a great company but a very difficult investment. I think that has forced us to move much earlier in the investing landscape. So we're typically coming in, even in Series B, we're typically much later stage of the businesses, but now we're coming in at very low levels of revenue but with a proven team, proven technology, and aligned with parts of the market where we feel there's a strong thesis for success.

So when looking at cybersecurity, we are more thematically driven and we tend to go earlier in the company's life cycle. So themes that we're focused on fall into two main categories. The first one is new security requirements that are driven by changes in the ecosystem. And these are things like cloud and SAAS, identity management, and authorization, application security, DevSecOps. We also look at data security and privacy, and we are focused on the attack surface management.

The other category is application of new technology into solving fundamental problems. And these are things like

using AI and ML to solve existing security problems better. Or things like full stack managed security service providers or MSSPs.

Marco Poletti: Yeah, unfortunately for David, I have to agree based on all the discussions I'm having with my own clients and our clients in investment banking where I do think security remains an area where a lot of VC firms, growth investors really want to find a way of investing given all of the tailwinds we talked about earlier. And especially in a world where we're seeing a ton of innovation, I also think that a lot of investors are thinking through, “Well, what is truly going to become a platform and can be a really large critical part of the cybersecurity ecosystem in a few years compared to new technologies that are extremely valuable but may be more of a feature that over time gets attached to a bigger platform?”

Allison Nathan: And given how much devastation cyber-attacks can inflict, the other area of focus of course is regulation in the space. Regulations in particular really designed to strengthen the financial market's reliance to resilience to online attacks. So where does that regulation stand at this point? And what could be the implications?

David Campbell: Yeah, look, I think we're seeing governments start to turn a lot of focus towards cybersecurity, and I'll use it in a more general sense here that RSA, one of the key themes in the regulatory space, has been around privacy. And we're seeing these new regulations like GDPR and CCPA come out, which not only are very broad but they're also very deep and specific in terms of protecting personal information and how companies have a responsibility to protect individuals.

And then on the other side of it, we're starting to see the government involved. Certainly within the government, they've adopted the NIST framework, and they're using that as sort of a basis of where they're driving all of their different operating departments to drive their cybersecurity. I think we'll see that start to come into certainly critical industries and industries that are fundamental to the security of the country. So you'll see that moving into manufacturing and utilities, and you'll certainly see it come into spaces like financial services where real impact can be brought against the country if they're to be compromised.

Marco Poletti: And I would add to that, which I completely agree with, I would also add some of the more -- as you were thinking about this specifically for financial markets, you probably saw some new requirements the SEC brought in for companies to essentially report and disclose security incidents. And I think all of those themes, with what David talked about also, participate to the fact that security has become way more complex than before to operate. Regulation is changing constantly. You need to constantly evolve, and that goes back to one of the themes that we've both talked about a lot, which is simplification and really helping companies actually run the security, which is a really important theme right now that we're seeing a lot of investment behind. And I think frankly regulation and evolution of regulation is an important factor in that overall thesis.

David Campbell: And the only add-on to that I would put in is this is starting to affect every scale of business right down to small businesses. And to try and make that manageable, particularly in the backdrop and of lack of cybersecurity professionals in the market, we're starting to see MSSPs start to play a bigger role in helping businesses of all scales to address the cybersecurity problem. And I

think the MSSP will be important on an ongoing basis. Even companies with very sophisticated cybersecurity programs will lean on MSSPs to do certain parts of their cyber defense.

Allison Nathan: Marco, David, I know we didn't get to everything. There's a lot to discuss in the cybersecurity space, but thank you so much for coming on and sharing some of your insights with us today.

David Campbell: Likewise, Allison. Thank you.

Marco Poletti: Thank you.

Allison Nathan: Thanks so much for joining us this Wednesday, June 8th, 2022, for another episode of Exchanges at Goldman Sachs.

But before we go, I'd like to share news about an exciting new project we've been busy with. Every week on Exchanges, I sit down with top Goldman Sachs leaders and thinkers to discuss how the most press macroeconomic issues are moving economies and markets. But have you ever wondered how other top investors are navigating

today's market headwinds?

In our new special series, Exchanges at Goldman Sachs Great Investors, Alison Mass, our chairman of the investment banking division, and Katie Koch, our chief investment officer of public equity in our asset management division, will be speaking with some of the world's most respected investors about their investment strategies and views on markets and global economies. Catch this limited run series on the Exchanges feed now.

If you enjoyed this show, we hope you follow on your platform of choice and tune in next week for another episode. Make sure to like, share, and leave a comment on Apple Podcasts, Spotify, Stitcher, Google, or wherever you listen to your podcasts.