Research @ Citi Podcast, Episode 18: Cybersecurity — New Risks, Expanding Threats

Recorded: November 26, 2024

Published: December 11, 2024

Host: Lucy Baldwin, Head of Research, Citi

Guest: Fatima Boolani, Co-Head of U.S. Software Research, Citi

Transcript:

Lucy Baldwin (00:01)

Welcome to the Research @ Citi podcast. I'm Lucy Baldwin, Global Head of Research at Citi. In each podcast episode, we bring you our thought-leading views and analysis across asset classes, sectors, and economies from around the globe.

I'm delighted to be joined today by Fatima Boolani, who is our co-head of our software franchise in the U.S. here at Citi. Fatima, welcome to the Podcast.

Fatima Boolani (00:28)

Thank you very much. I'm delighted to be here.

Lucy Baldwin (00:30)

Really excited to talk to you today because I know one of your areas of expertise has become the “cyber problem,” for want of a better phrase. Maybe you could just set the scene a little bit in terms of cyber and the evolution from a historical perspective. Is this a totally new thing in your career, or actually, has this cyber threat always been there in different ways?

Fatima Boolani (00:51)

Yeah, I think that's a great place to start. So, you know cybersecurity threats have had a renaissance of sorts in the better part of the last decade, and I'd say even through the global pandemic, a lot of cybersecurity risks and concerns were laid bare by way of organizations having to materially change the way they were working and operating. And so while this issue of cybersecurity is not a novel one, it's gained a significant amount of prominence in the course of the last decade, largely as a result of these very, very big picture themes, and the confluence of these big picture themes that we all talk about within the context of enterprise software, right, like cloud adoption, work from home, work from anywhere, and this rise of the Internet of things and the internet connectivity of devices.

Lucy Baldwin (01:42)

And maybe just to dig into that in a little bit more detail, Fatima, when you think about the spending in this space, give us a sense as to how that has evolved in the last few years in terms of investments into cyber.

Fatima Boolani (01:55)

The sort of renaissance of the cyber problem has gone hand in hand with a lot more budgetary attention and much, much greater levels of strategic priority. Now, we've been covering the space for about 15 years, and there has been no better time to be a cybersecurity company because there is so much of an effort and so much of an executive board level, fiduciary level focus on ensuring that you have your cyber house on high priority

and on lockdown, right? And so what I mean by that is roughly ten, 15 years ago, cybersecurity typically tended to be tactical type of investments. But with the onslaught of rising regulations, with the onslaught of very mainstream *Wall Street Journal*-esque front page news on brazen breaches from malicious actors and adversaries, you know, the whole notion of cybersecurity has taken on this increased importance, and that's pulled in a lot of budgetary attention. And so, we're fortunate enough to run our CIO surveys every single quarter and speaking to the top decision makers and very large organizations as to how they're adjudicating and portioning out their budgets— and Lucy, I have to tell you the number one budget priority is cybersecurity, bar none, and that's been the case over a very longitudinal period of time, right, so there's absolutely been consistency there. And this whole concept of budgetary growth and this idea of budgetary growth for cyber has volleyed somewhere in between mid to high single digits of growth, pretty consistently for the better part of the last couple of years, which is an outgrowth relative to overall IT budgets. I know we've been in sort of a budgetary malaise, if you will, for overall IT spend, but cybersecurity has actually been pretty insulated, if you will. And outgrowing the total wallet by a factor of two to three because the risk profile and the attack surface of a lot of these organizations is just too large and too risky to want to cut back. That's kind of the lay of the land in terms of the priorities have actually matched the budgetary allocation as well within the IT wallet.

Lucy Baldwin (04:14)

I mean, Fatima, if I'm not misunderstood, the big meta things that you guys, I guess, will be grappling with in the team include things like use of cloud, work from home, Internet of things, and obviously a huge need to innovate, or, if you like, out-innovate the bad actors in those sorts of space. Can you tell us a little bit more about some of those meta things and what you're seeing?

Fatima Boolani (04:34)

Absolutely. You know, I want to go back to this concept of attack surface. Twenty years ago, the world was simpler. IT was simpler on a relative basis anyway, right? You had a moat around your castle by virtue of what your IT department is, you're just protecting your castle, which is your entire IT footprint from the Internet. Fast forward to today, there are a compounding number of variables and vectors that are metastasizing your risk across those three vectors you called out. So when you're adopting public cloud, you're effectively renting someone else's computing resources. So you don't have the degree of visibility and the ownership that you had in the yesteryears and in the before times. And so that brings another facet of risk and introduces another facet of risk that requires an architectural shift as you think about cybersecurity and risk management. You layer on the fact that, you know, in 2024 and beyond we can sit in a Starbucks, open up our laptop and get some work done, right? And that's not a connection or Internet connection that is coming out of a corporate network. And so how does an organization actually wrap its arms around the risk that is inevitably introduced from that type of day-to-day productivity and working interaction? So again, adding to this notion of metastasized attack surface. And lastly, I think probably most importantly, this whole notion of the Internet of things and the connectivity of devices that you wouldn't traditionally think of as computing devices, right? You know, robots on a manufacturing floor, or your critical grid systems in a nuclear plant, or a water treatment facility. I mean, these are all pieces of infrastructure that historically never touched the Internet but are touching the Internet now and will continue to do so as large swaths of the economy modernize to everybody is digitizing, right, no matter if you're an old economy sector or a new economy sector. Really a lot of these factors are playing into this attack surface notion, and organizations just have to rethink, and have had to rethink, their strategy

around which vendors and which capabilities are going to be able to safeguard from external incursions into the organization because the footprint is so large.

Lucy Baldwin (06:53)

You know, you're painting a really clear picture, Fatima, about this diverse attack vectors that we're seeing, right? And how should we think about the nation-state actors in this space, Fatima? You know, obviously huge changes in the last few years, geopolitically, perhaps a blurring of lines between traditional and cyber warfare. What do you see going on there, and how is that, I guess, shaping spend and investment, too?

Fatima Boolani (07:19)

Yeah, I think it's such an important observation as it relates to — in periods of foreign policy upheaval and/or geopolitical tensions — we have seen the ebbing and flowing of very large, well-financed, very, very motivated nation-states who are compelled to want to take a cyber warfare oriented approach. Some of the more damning examples are the attacks on the water grid and the utility systems and nuclear power plants. You know, but there's other considerations as well that I think are very impressionable to memory: the Sunburst attack in late 2021, early ‘22, as perpetrated by a foreign body, you know, made its breaches into the highest levels of the federal government and cabinet agencies. So while that's not quite an Internet of things–type cyberattack process, it certainly gives you a flavor of how pernicious nation-state activity can be, when tensions are high amongst nations, right? So I think it really boils down to sort of the willingness, the financing, and the motivation for some of these adversarial nations to kind of do a lot of these malicious things. And they can be downright scary.

Lucy Baldwin (08:49)

And I guess since COVID, you know, all of us have become much more aware of supply chains and supply chain vulnerabilities. When you kind of think about that fusing together, I guess, of the cloud and network security, what is the most key area, I guess, of your cybersecurity architecture, if you're a CEO or a board and you're trying to think through supply chain vulnerabilities as well as part of that?

Fatima Boolani (09:14)

Yeah, you know, one of the things I mentioned earlier was just around— organizations, for lack of a better term, *outsource* a lot of their IT from the standpoint of hey, we're not going to build these data centers. We're going to leverage very large public hyperscalers and public cloud providers to run our computing environments. Because if I'm an industrials company, if I'm a manufacturing company, my core competence and my forte isn't to actually run the best-in-class IT environment, it's to provide the best industrial products. It's to provide the best agricultural products and widgets if I'm kind of in that space, right? It's not to run the best and shining A+ IT department. And so what challenge that brings on — and this actually doubles back to the Sunburst attack — this whole concept of supply chain and supply chain oriented attacks. And functionally and fundamentally, it's, hey, if I'm not owning the full process of how I'm building my IT environment, how I'm building my applications, my new modern next-generation applications with the whizbang technology, well, I'd better be darn sure I know what's going in those application environments. So having the wherewithal and the foresight to have the sort of ingredients lists of what developers are doing, how IT is moving, and understanding that if you're going to be building these applications in an infrastructure that you don't own with tools and capabilities that you don't fully own, you ought to know what's actually going in the pie, so to speak. So this whole concept of supply

chain is going to become that much more important because it is absolutely beholden to organizations' ability to move very nimbly as it relates to using IT as a strategic advantage, right? So all of that to say is, the more organizations are ceding to third party providers to enable their flexibility and agility from an IT standpoint, you are introducing more risk into the organization because you're moving fast and breaking things, as they say in the business, and that necessarily comes with the risk from the standpoint of okay, I need to understand what components, new components I'm introducing into the organization, and I ought to sanction that these are fine and they won't actually create more risk.

Lucy Baldwin (11:29)

And Fatima, can you just bring to life a couple more examples of how this manifests and how this looks across industries and where you see some of the big differences? I mean, I know when you and I've spoken before, we've talked about some of the issues in areas like, I don't know, Internet-connected insulin pumps getting hijacked, which is obviously very scary, so in the healthcare space, in Internet-connected security systems, heating ventilation systems, just bring to life a few things for us in terms of some of these vulnerabilities that we're seeing across the system where obviously attacks can I guess amplify very quickly in a 5G era where you've got this unprecedented connectivity.

Fatima Boolani (12:10)

Yeah, you know, the whole notion around bringing devices in what I like to refer to as "non-carpeted areas of IT" — so exactly what you talked about, right? — manufacturing floors and facilities, power plants, Internet-connected security systems, healthcare devices that, even from a consumer level, a lot of these personal health devices are manageable through an app through your phone, right? And if it's manageable through an app through your phone, well, guess what — if it gets into the wrong hands, that could wreak havoc. And so just from that standpoint, the real challenge is twofold. You have these devices that don't look and smell and feel like normal IT devices that are coming online and touching the broader network — and by the way, they have an entirely different dialect. I won't say language, but an entirely different dialect as it relates to how you protect these systems because they're very different. But the end game is the same. I mean, you want to make sure you have visibility into how these atypical computing and IT devices are behaving, because if you don't, you can't solve for what you can't see. And in many cases, a lot of bad actors can actually use these atypically connected devices to move onto the traditional network, which is where the prize is. So that's why that trend has become so much more important because you're getting a fusing of these discrete environments, which can be a mechanism and a conduit for a lot of bad actors to actually get into the meat of the organization, where a lot of the data and important information worthwhile exfiltrating is. So this fusion is very important to watch. And I think the last point I'd add to add gravity to this observation is in the next decade, we're going to have a multiplicity of these interconnected devices coming online. So that's going to be orders of magnitude greater than what we are going to see on the traditional IT side. So it's absolutely worthwhile and merits watching.

Lucy Baldwin (14:14)

And I guess AI only adds fuel to that fire in the sense that you've probably got the use of AI to perpetuate attacks, and I guess you've also got, offsetting that to some degree, the use of AI to defend against those attacks. And then I suppose, you know, there's like a— perhaps a third vector, which is thinking about protecting data and the outputs that AI itself generates. Is that how we think about AI in the space?

Fatima Boolani (14:42)

That is absolutely our mental model and framing of how the entire concept of AI and machine learning is going to impact the space. From a good guy to an adversary standpoint, both are going to need to be powered by AI. Using AI to build and create more attacks is going to make it just economically so much more attractive for bad actors to keep perpetrating attack. So actually using AI for a nefarious advantage in increasing attack activity. On the flip side, the good guys and the companies who are defending your organization and all the commercial tooling that's there to safeguard your organization, well, they'll have to keep up with AI too because the barrage of these attacks in terms of volume, intensity, sophistication are going to have to be met with AI because you can't come to a sword fight with a butter knife, right? And so it's AI versus AI from a combat and a defense standpoint. So that's absolutely right, number one, and we're seeing a lot of commercial organizations within the cybersecurity universe talk about the infusion of the AI technology and related capabilities into their platforms to increase efficacy, increase speed to response, increase time to clean up a breach, for instance, right? So most certainly, I think that's the most important part of that trifecta. That translates into the second piece around hey, we need to use AI to defend against AI offense, right? And the third piece, I think, is more of the blue ocean conversation around, hey, what more open-ended risks does the use of AI create in an organization, right, and this can be in the form of unforced errors, leakage of information that shouldn't be in the wrong hands. And that is certainly going to be a big topic of debate as it relates to how much AI, and generative AI in particular, is going to democratize access to data and output that you actually don't want as democratized. So there's a governance element to it, which I think is going to definitely be an industry talking point.

Lucy Baldwin (16:59)

And given that sort of big blue ocean point, Fatima, I know you guys wrote a fabulous report last year, thinking about the cybersecurity problem. And in it, you spent a lot of time thinking about the talent shortages that were very evident in the sector at that point in time. Has that story changed much in the last 12 months?

Fatima Boolani (17:18)

I tell you it's almost exacerbated. Concepts that we just fleshed out as it relates to, hey, AI is just going to create more volumes of attacks, more intensity of attacks, and you just can't have a human engage and process and analyze the voluminous nature of these attacks that are bound to become even more sizable in nature, right? And so translating that down into an industry or in an industry level where you already have a dearth of talent and just a shortage of human labor supply to even tackle what we have today. That only is going to exacerbate the problem in our opinion. And so, you know, that's where AI comes in on the defense side. There is going to be an absolute parabolic rise in the type of information that's going to come in, and you need an analytical partner with the analytical horse power of AI to kind of help you to the finish line, right? So while I don't think generative AI or AI solution and capabilities are going to help narrow that 4 million person global, you know, skills deficit that we do have to fill, which is pretty remarkable, it certainly helps chip away at the problem in maybe more automated way.

Lucy Baldwin (18:44)

Well, and presumably the regulatory and the compliance challenges, reporting standards, et cetera, that sit around this space, seem to be going in one direction only. So I can imagine that only adds support to budgets needing to go up. Maybe just to close this out, what would you say are the main factors that people should think about when they're looking at the

private companies versus the public companies, the raising of capital in the space, over the next three to five years, where do you see most of the change happening and where do you see most of the focus for the VC firms operating in the space?

Fatima Boolani (19:23)

Yeah, you know, this has been such an incredibly evergreen fertile market for innovation, for VC funding, for organizational attention. Because as we take a step back, I think it's remarkable to appreciate the feedback loop here, right? There is an ongoing and actually very rapid innovation cycle in cybersecurity, which is both a gift and a curse. And so for those reasons, we're going to continue to see a lot of vibrancy in the space all the way from early stage VC and fundraising, to solving kind of the next big problem that's around the corner, to scaling a lot of these companies in a very institutionalized way. So we're going to continue to kind of see that trend in this virtuous cycle continue. And Lucy, cybersecurity is a $170 billion market today. It's going to grow low teens over the next five years. It's going to be close to $250 billion in size. So there's going to consistently be an impetus for budget and wallet share disruption. But from the standpoint of, hey, which specific subcategories we think are going to get the spotlight, we're going to be in a phase of continued IT and architectural modernization over the next couple of years, right, and with cloud and public cloud adoption, especially as motivated by the demands for generative AI and the appetite to want to have more generative AI infused and within IT, well, that's going to continue to keep a focus on how do I secure my assets in a cloud environment, right? So we continue to think cloud is going to see— and cloud security, frankly, is going to see continued focus, which by the way, is going to introduce other blind spots, right, that will need innovation and then funding and budgetary allocation. Cloud would probably be the first and rather one of the more prominent areas. And then relatedly, just with respect to the security operation center [SOC], which is effectively the NASA control room of what's happening in an organization from a cyberattack and cyberdefense perspective, we expect there's going to be a fair bit of modernization from the technology infrastructure within that realm of an organization, right? So this “modernization of the SOC” theme is something that we're very keen on, just as it relates to how much data and telemetry is being generated, all the signals coming in from different parts of the organization, larger parts of the organization. So just better performant, faster, more modern technology to manage a lot of that data to analyze security risks much better. And then, you know, naturally, the last related piece is the labor force productivity gains that can be had with AI. So a lot of the $250 billion market spend that I alluded to, I mean, substantively half of that is services oriented. So we absolutely see this theme of the “software-ification,” if you will, of that spend to just derive better outcomes and better security outcomes and mean time to resolutions, and mean time to detections for breaches. So we absolutely think that's going to be a huge part of the investment case, if you will, for the cyber industry, for both buyers and financial backers.

Lucy Baldwin (22:55)

Fatima, wow, what a fantastic whistlestop tour of how the sector is evolving. Clearly, it's going to be a space that everybody listening is going to hear more and more about in the coming years given so many of the complexities that you've described today, and obviously, it's going to be an area where you need global collaboration. Thank you for taking the time to speak with us today. It's been a great conversation.

Fatima Boolani (23:15)

My absolute pleasure. This is a space that's very close to my heart.

Lucy Baldwin (23:19)

Thanks for joining today's episode of Research @ Citi. We at Citi Research provide the highest-quality products, services and content covering all major asset classes and economies around the world. If you enjoyed this podcast, you can follow us for regular episodes. And feel free to share, like, leave a comment, and subscribe. See you next time.

[Disclaimer] (23:44)