The Hexagon Briefing: A Global Perspective from HSBC

Episode 8: Total Security and Fintech

July 14, 2021

Please refer to important disclosure at the end of this document.

Jose Rasco

Thank you for joining us today. Before we begin, you should be aware that relevant information relating to this podcast and the products and services we are about to discuss are available at the end of this recording and on our website at www.us.hsbc.com.

Welcome to the Hexagon Briefing: A Global Perspective from HSBC. Each episode, we'll bring you our insights on key financial topics. You can learn more about insights and research offered by HSBC on our website at www.us.hsbc.com.

I'm your host, Jose Rasco, and thanks for joining us today.

Today, we're going to cover the topic of total security with a focus on cybersecurity. And joining us is Prasant Chunduru, HSBC Commercial Bank's Head of Venture Debt. And he is here to discuss all of that with me today.

This podcast was recorded on July 14, 2021.

Thanks for joining me. And let's get going.

Before we talk to Prasant, let's start here. Let's talk about technology and tech diffusion. One of the key things that we need to focus on is how do we invest in technology or more importantly, how should we invest in technology? When you talk to your advisors about investing in technology, invariably you're going to come up with themes and topics and company names that you feel are relevant and that you feel have growth potential. And invariably those companies will be the ones producing the technology, so you can invest in technology through multiple markets. There is the angel market, there's the venture market, there's the mezzanine markets. And those are all sort of private markets. Then you get to the point where you even have public markets where you can invest in technology, right? And so we all know about these different markets in different stages of investing. But one of the things that I don't think gets enough play in terms of the media and makes enough noise because it is a key component is the concept, the two concepts, I should say, of diffusion and convergence.

So the first concept is, as you invest in technology and that technology grows from an idea to an actual product or service. It then becomes something that is usable by the market. And usually it will be one market that those innovators will be going after. Right? And whether it's education or health care or financials, they will have a focus for their product, usually in one vertical. Now, where it becomes interesting, whether it's in the public or private markets is that technology begins to diffuse or begin to spread

through the economy. And we see many examples of that. We saw it in the 90s when technologies were focused on B2B. And I can help a company do X, Y, Z and lower their cost of goods. And then that company realizes, well, I was focused on health care, but I can apply this to financials, I can apply it to education. I can even go into the manufacturing sector. And so we see the companies begin to take those technologies and diffuse them through different sectors of the economy.

Now, the second part of this, which is going to be really important, because if you want to get a grasp on what we're about to go through, you have to go and look at history. And after World War II, the U.S. invested in the Marshall Plan, where we invested a ton of money into Japan, into Europe and helping rebuild those economies. And therefore, those economies had the latest and greatest technology and the latest and greatest infrastructure. That is what we're doing now across the globe. We're rebuilding physical infrastructure and we are including the digital components to that infrastructure.

Now, where does that leave us? As we roll out 5G and as these technologies, whether it's block chain, whether it's AI, whether it's big data. Choose your poison, as they say. Whichever technology it is, as it begins to diffuse through the economy and it gets joined up with other technologies, that's where you'll see not just the sales of current products, but the new products that will be put together by putting together big data and AI or security products and big data. And you will see that, that convergence of these new technologies, that's where you're going to get another level of productivity and profitability, where companies are going to say this one input plus this one input is actually going to give me a return of 3 or 4 or 5. And that's where you get that exponential growth in productivity and in profitability.

And that's what we're looking for. So as we continue this new business cycle, as we continue this multi-year rollout of technology, do not get stuck in just investing in technology companies that make the technology. Look for the companies in health care, look for the companies in education and financials and in manufacturing, and travel that are going to use these technologies to best lift productivity and they're going to put them together to lift productivity and profitability and those are the companies you want to invest in, and those are the companies you want to do business with.

So remember those two phrases. It's not just about technology. It's about the diffusion of those technologies and the convergence of those new technologies to lift productivity and profitability. We're at the beginning of a multi-year rollout here, which is going to be exciting. It's going to change the way we do a lot of things in our world and the opportunities are out there. Certainly, there are going to be risks, but that's why we're here, to walk you through this and help you and bring experts to you who can help you sift through the information and find the most appropriate vehicles and investment opportunities.

So as we've discussed numerous times, clearly, we are at the beginning of a new business cycle. We are also at the beginning of a new multi-year rollout of emerging technologies, which are really going to set the world on its ear. We have productivity enhancing technologies that are coming out all over the place. It begins with 5G and the future is quite open ended and quite interesting. So one of the big things that we're looking at as we begin this new phase of a technological revolution with 5G and beyond is what are some of the opportunities for investors and for businesses to develop, not

only to expand the business you're in, but to develop new businesses. And one of the issues that has come up since the mid 1990s, right. It is not a new theme, the issue of security. And if you look at the Biden infrastructure plan, clearly, there is a real emphasis on building 3 components of infrastructure.

Number one is physical. Rebuilding roads and bridges and tunnels. Number two is digital, which he is very focused on 5G, closing the digital divide and expanding the use of technology in everyday businesses and products and services. And number three is the expansion of human infrastructure, or human capital, and a big part of that is still digital, which is closing that digital divide, getting the workforce up to the level it needs to be at to engage in this digital economy.

So let's focus on one opportunity and one potential risk. But as investors, we see it as both of those risks and opportunities are definitely opportunities for us as investors and as businesspeople. And that's the world of security. And we have a focus on total security where we try to incorporate the physical security issues that are going on, whether it's in health care or traditional defense or even the space race. Then you see the injection of technology more and more in these different focuses or these different areas of physical security. In addition, personal security, financial security, biodefense, food security, which, believe it or not, in China, I believe Australia and 2 or 3 other countries is part of the actual defense budget. So those are some of the things we want to focus on today. How does cyber security fit into the world of total security and what are some of the opportunities we see in this space?

So before we get started here, let's welcome Prasant Chunduru, who is HSBC Commercial Bank's head of venture debt, and he is here to discuss that with me today. So Prasant, as we look at the world of tech, this new tech revolution and the world of security, what are some of the risks and some of the opportunities that you see in this world?

Prasant Chunduru Jose, thank you for having me here. It's a pleasure to be here. I'll get to your question, but I really liked your introduction as well, you know, linking physical and digital security. I think that's really a great starting point, because historically, the approach to digital security has been very immersed in physical. You know, everyone has heard of firewalls. You know, something we've all grown up with and very familiar with. The whole concept of a firewall was that you could ring-fence a certain physical location, whether it's a headquarters or even your personal computer, and you trust whoever is there in front of that device or in that office. And that person who is in that location has access and people who are not in there do not have access. So it was the digital security very clearly came from a physical security aspect.

I think as we've talked about the tech trends of migration to cloud, that covid has really accelerated some of these trends. We know the physical perimeter doesn't exist as clearly anymore. People want to be remote. There are tons more devices being connected to the networks. And with that, there is an increased need for a different approach to digital security that is completely non dependent on perimeter or physical security. And I think that's the real challenge to, you know, part of your question on what the challenge is really unlinking this digital security from everything that's come before, which has been very physical security driven.

I think the opportunities are huge. Like one, it's hugely convenient, right? It's much needed because it's impossible to expect everyone going forward to

work from a single location or from a very secure location. It may be possible in certain sectors and certain institutions, but certainly not everywhere. And with that comes convenience and a lot of aspects of it. So I think the opportunities here are, are endless. It enables talent to be sourced from everywhere in the world versus being dependent on a single city or a single talent pool. It enables a lot more scaling. You know, once you have figured out this approach of digital security, you could trust many different companies, many different vendors, many different servers to bring you competition and things that you need versus, you know, having to build it yourself again, dependent on physical security. So I think that there are great challenges. But, you know, the reason why we are moving in this direction is because the benefits, if we can figure this out, far outweigh the challenges.

Jose Rasco And that is the good news that the benefits outweigh the risks. Right. So that's the definition of a growth market.

Now, one of the things that we've talked about is in terms of cyber security is personal cybersecurity, financial cybersecurity, the protection of digital records, especially when it comes to health care and things like that. What are some of the opportunities, or where do you see the world of fintech going in terms of the cybersecurity angles? And where do you see some pockets of growth that could be potential opportunities for us?

Prasant Chunduru That's an interesting question, Jose. I think, you know, I think in the last few years we've seen a ton of hacks. I think every month I get an email from some service or another account that I have an account with that tells me that there has been a hack and they do not yet know if my information is a part of the hack. And if so, these are the pieces of information that have been leaked to the public domain. Sometimes it's innocuous, maybe it's just a name and maybe a location or city or something. But in some cases it's a password that you use and that is maybe the same password that you use in other places. So you have to quickly act and reset that.

So I think the threats that have emerged over the past few years have completely changed how I personally would manage my personal security as well, especially with high value services, whether it's, you know, banking, access to accounts, digital assets that I or someone else may own. So I think it is a whole wholesale shift in the way security is managed by individuals. I think the basics of it are something that we all know. I think we are all advised to have two-factor authentication on the important services, whether it's logging into your bank account, whether it's logging into your work account in some cases. So I think two-factor authentication is not a silver bullet, but it's certainly a lot more secure than just a password. I think there are many ways of two-factor authentication that have emerged, things like YubiKey and NFC based authentication. There are apps around, I think Google authenticator that refresh every 30 seconds. Unless you're in possession of a device, you cannot really log into a service. So I think there is a ton of new services.

Password managers, for example, have emerged that you can make. You can have a lot more complex passwords that, you know, it's impossible to retain in just your head. To have very secure passwords that are not used between different services. So every one of your websites will have a single password that's very complex. So even if there is a hack, it's only that a single account that's exposed. So I think there has been an emergence of these services which have tried to make it convenient while also boosting the security. And

that's the real tradeoff here. Right? Like, it's easy to have a single password that kind of has your account across every single website, but it's also the one that's most vulnerable if you work to that.

Jose Rasco And so as we look at security, cybersecurity, everybody focuses on the software. Right. What are the new software programs that are taking them out? But there are hardware components to it as well as you just sort of alluded to. Right. And the technologies themselves will actually create a level of sophistication and authentication that should provide some level of security as well as that. Is that a fair statement, you think? And if it's true, is that true?

Prasant Chunduru Yeah, absolutely. I think at the end of the day, hardware is probably a component of your digital security as well. I think when banks were first moving away from passwords, I think it was a pretty common approach to send you a dongle that you have in your possession that you have to type in some number to get a code and then you enter it into a service. And so that was a very hardware based digital security. And certainly devices have gotten easier. Fingerprint scanners, iris scanners. So I think hardware is an integral part of digital security.

I think the other piece of it is the world is moving from device based security in the sense that if I'm on a laptop or not me, if whoever has access to my laptop has access to certain applications so that it has been the model that most institutions still operate on, individuals operate on. Now it's moving to a model where every time you access something, you have to prove your identity in a digital way. So it's something called zero trust information in that every single service that you're trying to access assumes that you need to. You are not you and you need to first prove yourself to be you before you can access that service. So I think there is certainly a big hardware component to it. But it’s that married with identity married with, authentication and access.

Jose Rasco And so the combination is going to create far more secure devices and products and services as we go forward.

Now, one of the complicating issues, right, has been the expansion in the IOT, the Internet of Things. This device to device communication. Is that something that you think is going to make security tougher, cybersecurity tougher, or is it something that, in fact, devices can actually communicate with themselves much more easily? And therefore, could it be much more transparent to the user?

Prasant Chunduru It's a great question again, Jose. I don't think we fully know, but I think one of it is this is a trend that we cannot reverse. There are going to be more devices tomorrow than today, and that's going to continue to be the case. The trend is towards more connected devices. So it is something that I guess every institution, every security organization government is grappling with on the IOT side. I mean, certainly like there are a ton more devices with different levels of commissions, different levels of compute. I think it's a very common hack to have a bunch of these devices, which are all Internet connected, to be taken over by a network and pointed at a certain asset and bring it down. These are called distributed denial of service attacks, didos. Which have surfaced many times to take down a website, for example. There have been services which have evolved to make that denial of service attack a lot less effective. So it's absolutely essential for the network security managers to

manage every single one of these devices, as a device that could be hacked. And if it is hacked, how do you isolate it and how do you shut it down?

So one of the areas that's emerged a lot recently is something called Endpoint Security, which was used even by the Democratic National Committee to investigate some of the hacks of emails and such. And this is very much around endpoints. And endpoints could be computers, could be laptops, could be phones, it could be IOT devices. What these services do is monitor what a regular profile of this device looks like. And if there are deviations in how it behaves, it immediately isolates it, alerts the network administrators and in some cases can take action and shut it down until someone brings it back on. So it's always this Red Queen race, where the threats emerge and then solutions emerge to manage those threats and the threats evolve and the solutions need to evolve.

Jose Rasco All right, so it seems like, as you said at the beginning, the opportunities are greater than the risks.

Prasant Chunduru I think Jose, one of the other areas that we should certainly address, and this has been in the news domain a lot, is supply chain attacks. What this means is obviously networks are made of different companies and different components, and it's all about finding the weakest link in that network and attacking it and taking over the network. There've been very big hacks of government agencies, private companies, which are through no fault of their own, except that they've used solutions from companies / technologies which have proved vulnerable. I think there has been a hack which has really prompted the Biden administration's response to cybersecurity. And things that you talked about earlier on at a Marshall Plan around cybersecurity has been really driven by these supply chain attacks, which are also partly linked up with the IOT that we were talking about.

Jose Rasco You talked about block chain a little bit. Can we explore block chain? Because I know a lot of people have looked at cryptocurrency and we certainly don't want to address that world. But in the world of block chain, it is a technology that seems to offer tremendous opportunity for the future and really disruptive technology in certain parts of the economy. Can you talk to us about some of the opportunities in Blockchain and then some of the if there are some risks or some of the things that we should keep an eye on when we talk about block chain and the use of cryptocurrency in general without getting specific on any one.

Prasant Chunduru Yeah, absolutely Jose. Blockchain is a fascinating technology that it's hard to believe. It's only about a decade, like 12 years old and it's really dominated the zeitgeist, at least in the last three to four years in financial markets elsewhere. And I think it's only in the last one or two years that we are seeing real applications beyond cryptocurrencies emerge, driven by blockchain. I think in the early part of this year there was a lot of boom in something called non fungible tokens, which are digital assets that are not really tokens, but could be. I think one of the pieces sold for excess of $50 million, which is just a digital representation of an art piece, and it confers ownership.

But going back to the core of what blockchain is. Blockchain is a way to establish trust through computation. So it is not that you trust a party or a set of users that you're interacting with. You're trusting the network, even though there may be many bad actors in the network. So, blockchain is essentially a way to establish that trust in an untrusted environment. Earlier

we talked about zero trust as the model going forward in that if you're participating in a network, you're interacting with other parties. The default model going forward is likely to be that everyone has to earn their trust. And you're trusting the network to demonstrate that to you. Blockchain enables that through intense competition, basically making it extremely onerous and extremely expensive for any party to hack into a network.

For example, the most common cryptocurrency, Bitcoin, the numbers vary, but it's expected to be in billions of dollars of cost to take down a potential Bitcoin network, if it's possible at all. And it's in the realm of states now to do so. So I think kind of breaking apart the security from the crypto-piece has been very interesting. And there are tons of applications of blockchain without the tokens across financial services. Digital assets aren't all of these different areas. And there are a ton of benefits to be had from that. It's a model. It's a future security model in a way to address some of the gaps that we discussed earlier around IOT and other tech domains that may emerge from this. Blockchain can be utilized as a security mechanism to prevent bad actors from gaining control or making it very expensive for bad actors to hack into networks.

At the same time, I think, you know, it's not a panacea. It has many challenges. It's still in pretty early stages as a technology. Not a day goes by where the carbon footprint of blockchain technology doesn't get discussed. I think the computational capacity of some of these blockchains succeeds in countries now. And concerns around carbon emissions are very real. And I think it's likely to stay because it's really creating competition for security. Do we have a better way of establishing security, which is not through computation? There are ideas being discussed around staking and such. We are likely to stay in this paradigm for at least a few years. So I think blockchain's use in certain - these use cases is limited at the moment, but the potential is huge.

Jose Rasco Well, so what we get from this is the technology revolution is here, right? It is going to expand exponentially. And we see that cyber security is here to stay and in fact, is going to continue to expand as it grows along with this technology revolution. And it's going to become more complex, hopefully more seamless for the user, but more complex and more difficult, therefore enabling things like financial security and health care security to continue to expand.

Prasant Chunduru Yeah, very, very well said, Jose. And I think you will see it in organizations as well. Previously, if there was ever a role of a Chief Security Officer, it would be kind of deeply embedded within IT. Now it's very common to see Chief Security Officers report to the CEO. So this is something that's being taken very seriously, is attracting investment and will continue to do so. And it's basically survival for companies, for individuals.

Jose Rasco So the opportunity to grow revenues is going to have to go hand in hand with your security efforts. And therefore, it's a very investable space and it's something that we will continue to look at. And hopefully Prasant, we can have you back in a couple of months and focus on some new issues in this space as it's something that you certainly know very well, my friend.

Prasant Chunduru Thank you, Jose

Jose Rasco

So thank you for joining us. And I hope you enjoyed the time. We certainly enjoyed listening to you.

So as we look at what we covered today, obviously the opportunities in this new technology rollout, this multi-year rollout are numerous, but so are the risks. So keep in mind that we have to continue to look at what the opportunities are versus the potential risks and figure out where the right investment opportunities are and where the right business opportunities are as things continue to roll out, get redeployed and opportunities continue to emerge in this new and emerging market. So let's keep talking about technology and how it's going to affect the economy and the financial markets, and it's going to be an exciting time.

So that is it for today, though. Thanks to Prasant for joining me and to you for listening. We'll see you next time on the Hexagon Briefing.