Julius Bär

Think Tank Podcast: Crime goes online – let's talk about cybersecurity

TRANSCRIPT

Nisha Pillai (NP): Welcome to Julius Baer's Think Tank podcast. In this series, we will be walking you through the mega trends of the future, bringing you closer to our network of thought leaders. They will be capturing the world's big changes and putting them in context for us. I'm Nisha Pillai, former BBC world news presenter and your moderator today.

What happens if our Internet connections were to go down? And our activity trackers' information suddenly go missing? Data breaches are a juicy business for cyber aggressors, and while we worry about physical and personal security, cybersecurity is just as important.

Alexander Ruchti, Julius Baer's next generation research analyst and Esteban Polidura, Head of Americas Advisory & Products are our guests today to give us the view on how to fight and be prepared for this invisible threat.

Alexander, as we know digitalisation has been steadily growing for the past decades, but it's really exploded since the start of the pandemic, in early 2020, hasn't it? So how do you analyse and evaluate the risks in cyber space at the moment, Alex?

Alexander Ruchti (AR): When we look at the risk in cyber space, we look at it from two different angles, from two dimensions. So first, it's just the threat landscape itself. So are there more data exfiltration happening, are cloud outages a bigger thing, is financial theft the bigger problem, malware, what's is happening in those ends, and then we look at the industries themselves. So how are they positioned for those fields. If you're a bank, then financial theft is a very big, big problem for you, but if you're a social media company, you don't care that much about it. On the other hand, if you are a cloud provider, and cloud outages become a bigger risk, then that's fundamentally a threat for your business. So then on that side, it really depends not just on how the threats landscape develops], but also on how the companies themselves are exposed to different fields of cyber security risk.

NP: So are you seeing in some industries much higher levels of preparedness, awareness, much more work going on to combat these cyber risks than in others.

AR: Well, some of the biggest spenders are in the healthcare space and in the financial services sector, because if you're a bank and you lose your client's funds, you can pretty much close your shop. And in the healthcare space as well, if your preliminary data gets stolen, if you lose big confidential client data, there your business is much more at risk. So we see those industries are much more willing to spend big dollar tickets on preparing for cyber risks.

NP: Right. So the beneficiaries of that big dollar spending then will be the companies that have developed the programs to combat it, right? Are there opportunities for investors and investing in those kind of companies?

AR: The big beneficiaries are the companies that provide true value-add services. So the ones that offer big scalable solutions for data prevention. One thing we often look in the next generation reports and our studies is: do we feel that cyber security is a growing field? Is it going to be more important, do we think that big companies are going to achieve bigger revenues? And there the answer is pretty clear. We are very, very likely to see high growth numbers in the future. Everything points towards that we see higher aggressors' sophistications, so attacks are getting much more sophisticated. We also see that just the way we shifted to more work from home, which means more

connections, which then means more attack vectors. So we need to be more prepared for that. But we also see a bigger regulatory push. So regulators such as the EU, are much more willing to actually fine companies if they're not compliant with data security protocols and are getting hacked. The European Union just published today the new information that we are now seeing hundreds of millions of fines having actually being implemented to companies that have not safeguarded the data as well.

So from all those different industry angles we see big growth for the cyber security space. But it is often important to ask: are the companies then able to transform that growth into sustainable earnings and sustainable free cash flow? Because if the companies are just growing but they're not making any money by doing so, then it's not going to be beneficial for shareholders in the long run. And our overall assessment on that is that we're rather constructive. We are not bullish, because the valuations of many of the stocks in the sector are more on the demanding side, but we definitely see constructive potential in many firms in the field.

NP: Right. So you have a pretty nuanced view on investing in this area, Alex, by the sounds of it. Despite the massive amount of spending that's going on to try and combat cyber-crime, the attacks just keep coming, right? And I saw in your recent Julius Baer's market outlook, you have matching worries of an infrastructure outage. How probable are these kind of attacks?

AR: Well, cybersecurity attacks, they happen all the time. We don't have the 2020 data right now from the FBI, but it's very likely that the amount of cyber-attack related complaints are going to be more than 500,000, and that's just for last year. And it's an impressive number by itself, but at the same time it's an increase of more than 50% versus two years prior to that. So we see a big increase and that happens across the field, across the spectrum. There have been a number of infrastructure attacks, successful infrastructure attacks, and I am very confident that we're going to see some in the future. Now we can distinguish between large-scale infrastructure attacks and more small-scale infrastructure attacks. So, the very big large-scale infrastructure attacks where we're considering an outage of the Internet or entire countries being shut off the power grid, we believe the likelihood of that happening is very, very low. But at the same time, there are many instances of infrastructure attack on a small scale. One of the examples that often comes up is in last autumn we had the hospital of Dusseldorf which was being hacked and they suffer the ransomware attack. And so their IT systems didn't work and then what happened next is one woman was close to being delivered to that hospital through an ambulance but because their IT system didn't work, they had to transfer her to a different hospital, and because of the longer ride time she unfortunately died. And so we think that those kinds of smaller infrastructure attacks that can sometimes come at the cost of human lives also we're going to see that in the future. That's something as well.

NP: It can have tragic consequences, by the sounds of it. I know you've modelled some scenarios for possible global scale Internet attacks. Are those also very unlikely to happen? What did your modelling suggest?

AR: Very unlikely. On those scales, you have so many different safeguarding mechanisms and backup systems that we see that a global outage of the Internet in multiple countries or the shutdown of a power grid or something like that to be so small that it almost becomes negligible.

NP: So when we discuss this area, cyber security, cyber-crimes, cyber-attacks, the stories are horrific really. The losses entailed can be enormous, including loss of life. Step back for a minute for me, Alex, and tell me why do you think this is an attractive area, an attractive next generation theme for investors?

AR: So, we believe that it's attractive because it isn't just growth by itself, but it is growth that is adding value. And only when an industry is actually adding value from medium to long term that industry will be able to generating superior returns for shareholders. If you look back to the 20th century, you're searching for growth stories, you're searching for technological advancements, you're searching for things that changed society. One thing you might end up with is the commercial airline industry. There are a few technological changes that have impacted us that much, that have been that peak of growth fibres. And if you look at them through a purely financial lens, through a shareholder lens, the airline industry has been a value destroyed for decades. And we can completely take out anything Covid-19 related. In the decades prior to Covid-19, the airline industry has, on the biggest part of its history, not been able to generate returns on invested capital that is above its cost of capital. And so for us, it's always important to not only look which segment, which industry do we believe is going to be bigger in the future, it's actually a growth story. But then ask ourselves the question, well is that growth going to translate into actual financial returns or not? And there we see some of the cyber security players while we have a stronger conviction that they will be actually able to transform that growth into businesses that have competitive advantages versus others that provide necessary services that clients are willing to pay for and are therefore attractive in the long run. Even though some segments of the markets already are trading at not cheap valuations at the moment.

NP: Ok Alex, sitting in front of you as a time-pressed investor. Summarise your position on why you think that investing in cybersecurity is an attractive proposition.

AR: There are a number of supporting factors for the cybersecurity investment landscape. From the company driven pull factors: to protect himself from business disruption, financial losses, reputational risks, to then the regulatory driven push factors, by mandating security standards and threatening with fines if the standards are not met. And on that backdrop, we have a constructive view overall of the industry and see decent growth potential in it.

NP: Very interesting indeed. I learned a lot. Alexander Ruchti, thank you so much for joining us on Think Tank.

AR: Thank you very much, Nisha.

NP: And now let's turn our focus to the Americas. Joining is Esteban Polidura, Head of Americas Advisory and Products for Julius Baer. Welcome, Esteban.

Esteban Polidura (EP): Thank you very much. A pleasure being here.

NP: We have all heard about the series cyber-attacks that the US government has suffered recently. But is the US prepared to confront these threats?

EP: Indeed, malicious hacking from domestic or foreign enemies remains a constant threat to the Americas. Just last month, the US issued an emergency warning after discovering that hackers hijacked software used by multiple federal agencies to gain entry to their secure IT systems. Columbia University estimates that malicious cyber activity costs the global economy some USD 600 billion annually and the US economy upwards of USD 175 billion a year. The US is the top victim of cyberattacks in part because it is so dependent on the Internet, which makes it more vulnerable.

The risk is however not only for the government, but especially for companies. According to CNBC, cyberattacks now cost businesses of all sizes USD 200,000 on average, with 43%t of them aimed at small companies.

Beyond the immediate financial impact of the hack, there are other costs that continue to drain a company's finances and that should be discussed. Hidden consequences pointed out by Deloitte include insurance premium increases, higher cost of debt, lost value of customer relationships, devaluation of trade name and loss of intellectual property, among other..

NP: Yes, so the impact is clearly very widespread and can be extremely onerous. What about the US's neighbouring countries? What's the situation in Latin America?

EP: Ransomware and malware attacks have also proliferated in Latin America. Fortinet estimates that jus in 2019, the region suffered more than 85 billion attempts to attack. And these only increased amid the coronavirus pandemic. Data from Statista shows that Brazil had the biggest share of users attacked by ransomware in Latin America last year, with nearly 47% of users infected. Mexico ranked second, with approximately 23% of users attacked, followed by Colombia, with over 8%. Moreover, during a 2020 survey, approximately 65% of responding IT managers in Brazil stated that the organization they worked for had suffered ransomware attacks, while in both Mexico and Colombia, 44% said their organization had hit by this type of attack.
Multiple channels are being used. About 72% of cyberattacks attributed to Latin America came from a mobile device, while 28% were registered as originating from a desktop.

NP: So why is Latin American being targeted in this way? What's your analysis?

EP: Sure. There are three key reasons for why Latin America is being targeted. First, it has seen a major increase in internet access over recent years, a trend that only accelerates. Approximately 67% of the people living in Latin America had access to the internet in 2020, up from a 36% internet penetration rate recorded in 2011. But the World Economic Forum notes that in countries that are considered "well-connected", internet penetration in rural areas still only reaches 40-50% of the population whereas in poorly-connected countries, that number drops to an average of 10%. This only signals ample room for penetration to increase. Second, financial technology (fintech) is being embraced in the region more and more. The Bank for International Settlements (BIS) highlights that in the 2017-19 period, fintech investment in the region rose more than 100% with Brazil dominating the landscape with major deals in digital banks and payment services firms. And third, cybersecurity investments are still suboptimal and poorly coordinated defence mechanisms are scarce. The region's cybersecurity market was valued at USD 13 billion in 2019 with the bulk of investments concentrated in only two countries, Brazil and Mexico.

NP: So Brazil and Mexico seem to be particularly vulnerable, right? What's that about?

EP: Sure, Brazil has been a cybercrime hotbed over recent years. A couple of months ago, the Brazilian Superior Court of Justice was hit by a major cyberattack that brought its operations to a standstill for several days. It has been regarded as the most severe cyberattack ever orchestrated against a public sector institution in the country. Aerospace group Embraer was also targeted by a cyberattack that impacted the company's operations. Two years earlier, a large botnet was discovered to be hijacking traffic meant for Brazilian banks. And the 2016 Rio Olympic Games were targeted by sustained, sophisticated cyberattacks.

In the last few years, Mexico has also been affected by a number of high-profile malware attacks. In 2020, for example, Mexico's economy ministry detected a cyberattack on some of its servers. It was the second high-profile hit on the Mexican government after hackers demanded USD 5 million in Bitcoin from national oil company Pemex in 2019, forcing it to shut down computers nationwide. And in 2018, malware affected several banking institutions, particularly the electronic payment system used across the board. Clearly both Brazil and Mexico offered opportunities for this kind of cyber attacks.

But also across the region, you can find similar stories. In Chile for example, registered 5,000 phishing attacks a day in 2020, according to La Tercera (*Chilean newspaper*). One of the main focuses of cybercriminals is attacks on people, where identities are kidnapped and private data, as well as bank accounts, are stolen. But the financial sector is a target too. Last year, Chilean bank Banco Estado closed all of its branches in response to a ransomware attack.

NP: So here we are, early 2021, still in the thick of the Covid pandemic, what has been the impact of the pandemic on cyber-crime, Esteban?

EP: Surely the ongoing Covid-19 pandemic has prompted cybercriminals to innovate and devise new modus operandi to exploit the situation and to target new groups of victims. According to Kaspersky, 2021 will be another challenging year for Latin America from the point of view of the diversity and complexity of attacks. More ransomware and malware will be developed regionally. There will be an increase and diversification of attacks directed at financial systems by local criminal groups. Android operating systems and communication platforms such as WhatsApp will be increasingly used to conduct attacks. Sophisticated techniques related to artificial intelligence will be used to orchestrate disinformation campaigns or propagate malicious code. And a large number of corporations will seek to buy cyber-insurance to protect their businesses.

NP: And we've also seen cryptocurrencies picking up again. With all-time highs in bitcoin and others. So what kind of risks face investors in this base?

EP: Indeed. The risks will only increase as cryptocurrency-mining malware present cybercriminals with an alternative to ransomware. The global market value of cryptocurrencies has surpassed USD 1 trillion amid a volatile rally in Bitcoin to record levels. Speculative retail buyers are among the reasons for the surge. But several sources show that some of the biggest backers of the recent surge in crypto currencies are also institutional investors. I think this is very, very interesting.

NP: Um, very interesting. I wouldn't have expected that. And Latin America, is Latin American particularly vulnerable to cryptocurrency-type of cyber-attacks?

EP: Indeed, it is. And unfortunately it is. The depreciation of local currencies and low interest-rate environment prompts many investors to seek refuge in Bitcoin and peers. And uncertain political environments seems to have the same effect. Argentines, for example, have now begun using cryptocurrencies as an alternative to the peso, with the number of people using Bitcoin exceeding one million in recent months. The heavy flow of remittances to the region is also a catalyst of cryptocurrency use. Mexico-based cryptocurrency exchange and financial services platform Bitso is already processing USD 1 billion in remittances for its customers. So clearly Latin America will continue to be vulnerable to cryptocurrency-related cyber-attacks..

NP: Esteban, a fascinating set of insights there into the cyber-attack in Latin America and across the Americas. Thank you so much for joining us on Think Tank.

EP: My pleasure. Thank you.

NP: Clearly digitalisation is not only transforming the way we consume data but also how we live, work, and interact with each other. If you have any question or you would like to find out more, why not get in touch with your Julius Baer representative? Thank you for listening to this Think Tank podcast on cyber-security, the risks and opportunities. And you can follow the Think Tank series on Spotify. That's all for now. From me, Nisha Pillai, good-bye.