LaSalle Street: Financial Markets Insights
The Podcast of the Financial Markets Group
at the Federal Reserve Bank of Chicago
Podcast 7 Transcript

Alessandro Cocco: Welcome, this is *LaSalle Street*, the podcast of the Financial Markets Group at the Federal Reserve Bank of Chicago. In this podcast, we explore systemic stability through the lens of financial markets. In today's episode, Ketan Patel explores a key risk affecting systemic stability: cyber and technology risk. Ketan, over to you.

Ketan Patel: If you were to ask a chief risk officer what their top ten risks are, you're very likely to hear cyber risk among them. Cyber risk is not new, but it *is* getting additional scrutiny—particularly in the past few months, given some of the recent events that have transpired.

Hi, I'm Ketan Patel; I'm a policy advisor at the Federal Reserve of Chicago. On this week's episode of *LaSalle Street*, we sit down with chief information security officers from Vanguard and Nubank to discuss cyber risk.

We get to learn some basic terminology and some background, but then also get their perspectives on risks at play and how they guard against them. We also discuss issues around vendor risk and look back at lessons learned from the Covid pandemic.

As a reminder to our audience, the views expressed on this episode do not necessarily reflect those of the Federal Reserve System or the Federal Reserve Bank of Chicago.

I'm privileged to introduce our speakers for this episode. Joining me from São Paulo, Brazil, is David Currie. He is chief information security officer for Nubank. And joining me from Malvern, Pennsylvania, is Alonzo Ellis. He is chief information security officer for Vanguard.

Welcome, gentlemen. Glad to have you both on *LaSalle Street*.

David Currie: Thanks, Ketan. It's, uh, great to be here today, and it's great to also meet Alonzo—looking forward to the discussion.

Alonzo Ellis: Likewise. Thanks for having us on, Ketan.

Ketan Patel: Uh, let's start the discussion with some basic terminology around cyber risk and resilience. I mean, people hear terms, are not quite sure what they mean all the time—terms such as DDoS, ransomware, malware, others.

David, if I could just start with you, maybe you could kick off—give us some background and some of the key terminology that's out there and being used, particularly around cyber risk?

David?

David Currie: Yeah, sure, Ketan. Let me try to demystify some of the security terms and jargon. Let's start with perhaps who we're defending against. So let me clarify kind of what an attacker could be to help give a bit of context.

So an attacker could be an individual hacker that's motivated by personal interest or, or someone who wants to build kind of a reputation for themselves in the hacker community. The main—there are many types of hackers who operate on this basis, uh, just out of curiosity or, you know, to engage in responsible disclosure programs in some cases as well.

We work with many hackers who are reporting security vulnerabilities through kind of the appropriate channels to us to help us improve security.

A hacker could also be someone who's linked to a hacktivist group, um, so you might hear the term *hacktivist groups*. They're motivated, motivated primarily by social issues, like attacking companies who they believe are unjust.

I had some firsthand experience, uh, with hacktivist groups in Hong Kong in my previous role during the Hong Kong civil unrest—both in 2014 and 2019.

A hacker could also be someone who's linked to organized crime groups, uh, and, and are purely motivated by profit, uh, and work as part of a collective.

And then lastly, I think, a hacker could be, also could be someone who's linked to government—a nation-state that's well-resourced and equipped with tools and techniques that are not commonly available; and they're generally very persistent.

So I think it's very important to know who we're up against when we're building cyber defenses. Attackers have lots of different tricks and techniques at their disposal.

I'm not going to go into all of them, but I think there's a lot of material that's on the internet—for free—if, uh, you'd like to research. But I think it's worth exploring a couple of key terms, uh, that most companies, uh, are dealing with and, and you hear it kind of talked about.

So as, Ketan, as you mentioned, uh, DDoS—uh, dis-, distributed denial of service attacks. These attacks are designed to dis-, disrupt or take off-line internet-facing services—generally by flooding them with requests to overwhelm.

It's like stuffing a letterbox full of junk mail until it's full and then the mailman can't deliver your actual letters. It's a cheap kind of attack to run, but generally very effective.

Aside from that, malware—or viruses—is code written with the intent to cause harm. It's either directly delivered to you, or you're sent a link to click on, that takes you to a website to run the malware to infect your device.

Malware can create a way into your PC or into your network or steal passwords, uh, to take over accounts.

Ransomware is something—it's fairly topical at the moment, due to the, uh, Colonial Pipeline incident, very recently, and is rapidly growing as a threat vector. It's proving to be a really profitable threat. Uh, ransomware is, is a form of malware that's designed to encrypt your device or data. And the only way to get your data back is to pay the attackers—generally in cryptocurrency.

One of the other terms you'll hear a lot is phishing. Phishing is typically an email or some kind of message that contains a link, uh, or malware designed to, to kind of trick you into clicking on it. Uh, phishing emails can often be hard—really hard—to spot, actually. So I think training is essential to, to be able to pick up fake messages.
And lastly, something that's not new—uh, social engineering—generally is an attack where hackers try to impersonate you, uh, by calling a help desk or to reset your password or take over your account—or in some cases, and I've had experience with this as well, where they'll call your suppliers and try and get your information, uh, in terms of pretending to be you to, to kind of commit corporate espionage. So I think, um, social engineering is another one to be aware of.

As I said, there's many types of cybersecurity threats. Uh, but I think they're some of the common terms that we'll hear. And hopefully that kind of demystifies a little bit when you hear these things.

Ketan Patel: Thanks for that, David.

If I could just kind of stick with a couple of points you just brought up, and if we just look at the past few months, I mean, we've heard warnings from the White House around nation-state threat actors, which you just mentioned and explained a little bit about.

But then, on the other hand, in May, we had the attack on the Colonial Pipeline, which supports much of the mid-Atlantic and parts of the South in terms of energy. And then recently JBS caught headlines, and it seems like these attacks are proliferating.

And given some of the headlines, I'd like to get Alonzo's take on this, on what he's seeing, and is there some trends we should be aware of? I mean, what's your take on some of the nation-state threat actors that we've seen and maybe are on our horizon that we should be aware of?

Alonzo?

Alonzo Ellis: Yeah. Oh, thanks for the question, Ketan. This, this is definitely a, a growing concern, uh, in the scope and complexity of cyberattacks, you know, against U.S. critical infrastructure. In recent, you know, in recent months, you mentioned, you know, Colonial, their CEO, Joe, Joe Blount, mentioned this in his testimony to the, uh, to Senate Homeland Security and Governmental Affairs Committee on, on, uh, June 8th.

And it basically comes down to this, you know—the fact is that while it's certainly true that in Colonial's case, you know, their network was breached due to a lack of multifactor authentication on an internet facing network endpoint—which could have been mitigated with a better defense-in-depth controls framework—the broader issue here is that, is the need for closer public–private partnership and information sharing on cybersecurity, readiness, and incident response to really mitigate these threats from these events' threat actors, which are increasingly active.

And whether those, those actors originate from nation-states directly or from a proxy for a nation-state, on behalf of a nation-state, or from independent, well-funded cybercriminal organizations, the threat is real, and we're seeing the impact of these attacks on vulnerable networks.

And look, our critical infrastructure and resource suppliers, you know, we tend to see that they're, uh, are mostly understaffed and underfunded when it comes to cybersecurity, talent, and technology. And so the threat actors have known about this for a long time. And as a result, it's clear that they've begun to ramp up their, you know, their attack efforts.

And while on the surface, most of these threat actors basically are seeing this asymmetric opportunity to attack underprepared entities that have a higher probability of *paying* a ransom—since they can't afford to have their operations interrupted for even a short duration—so they're taking advantage of that.

So whether it's a fuel distribution system, as we saw with Colonial, or a municipal water supply system, as we saw with the, uh, the water treatment, wastewater treatment plant in Oldsmar, Florida, or JBS food supplier, that the cyber mitigation's maturity, coupled with the nature of their operations, really makes them prone to the attack.

Now, given the role of these entities—that these entities play in our supply chains—the risk is not just a matter of economic loss, but also one of national security. And that causes us to consider, you know, these threat actors in a different context.

And so said another way, it's becoming more difficult to distinguish a cybercriminal organization from a nation-state threat actor, as their motives appear to overlap—or at least are beginning to appear to overlap.

So with each successive attack, there's a trail of evidence pointing to the tr-, to the traditional cybercriminal activity, such as an extortion request; but it's also coupled with an attack designed to cripple the operations, with impacts that reverberate throughout, you know, the U.S. in this case, but can certainly be more global as well.

And so when you look at these attacks from this perspective, it clarifies the need for a closer public–private partnership to really address these threats. So, that's, that's something that we, that we're seeing the broader, as far as broader, implications here.

Ketan Patel: Maybe we could just stick with one of the points that both of you alluded to. Uh, David, a bit more explicitly, we talked about ransomwares and payments to keep operations going—and crypto's been lin-, linked to this. I'm wondering if you guys have any thoughts into—is there going to be increased scrutiny around the, the crypto market?

I know it's an adjacent topic to cyber risk, but it seems to be ever-linking, given the criminals are using, using crypto payments—particularly Bitcoin—in some of the other recent events.

I wonder if either of you wanted to comment on that.

David Currie: Yeah. Look, um, Ketan, I think it's a really interesting kind of a—it's a really interesting question. Um, we, we definitely see the proliferation of ransomware attacks happening at the moment and, you know, the, the kind of foundations of some of these—and specifically the payments—is around cryptocurrency.

So I think, you know, we're definitely conscious of this. And I think this is going to be something that, um, you, we need to figure out—whether it be through regulatory measures or other measures—on how we kind of deal with this.

I, I'd be interested to kind of dig into this a little bit more. I think ransomware is something, a particular topic where we're kind of focused on—both ransomware, but also other types of extortion attacks where, you know, are less public attacks—where we're seeing demands, you know, across industry for payment to be made through cryptocurrencies. So I think i-, in that kind of vein, it's definitely going to be something that, you know, continues to play a greater kind of role. And the other aspect is—that we're conscious of as well—is the integration of cryptocurrencies in terms of mainstream banking. You know, making it a lot easier to cash out of customers' accounts and therefore, um, making a-, an interesting kind of fraud, uh, opportunity for attackers to kind of pursue.

Ketan Patel: Thanks, David, that is very insightful.

Alonzo, I just want to see if you want to comment on this. If not, we can move on to the next topic.

Alonzo Ellis: Yeah, the, the—I'll add that, you know, there's a heightened level of complexity when it comes to the use of cryptocurrency, uh, or, you know, tokens, coins, uh, in these, uh, crypto assets and the, as a-, as a payment mechanism for these types of attacks. And that has to do with, of course, the anonymity, as well as the challenges as it relates to tracking, you know, an attacker across multiple geographical boundaries.

Uh, and so many countries have agreements in place. If you think about the traditional financial markets where, you know, you can—you control accounts, or freeze accounts, and that system has been, you know, uh, set up from a financial crimes perspective, uh, and operates pretty well. But when you bring cryptocurrency into the picture, those sort of agreements have *not* been hammered out across, you know, different regulatory regimes. And so it makes it difficult to actually execute an order, for example, to freeze an account—uh, a crypto account—whereas it would be much easier to do so if it was a traditional banking account.

So you think, you know, the difficulty with which it is—takes to track the, you know, the attackers', uh, funds—as well as the ability to actually do something about it once you're able to *find* the wallet—makes it all a little more difficult. And so, of course, you know, the attackers see that as an asymmetric opportunity to take advantage of, and, and that, that's what they're doing.

Ketan Patel: Okay, I'd like to now probe on your guys' views on the resilience between financial and nonfinancial firms, keeping in mind some of the attacks we just discussed seem more focused on the nonfinancial sector. And then also the fact that the financial firms over the past two decades have invested quite heavily in their cyber risk controls.

I'm especially curious on your take, David, and I'll start with you—given Nubank is a dig-, digital bank and it also has international presence—how those nuances are playing out from that vantage as well.

David?

David Currie: Yeah, Ketan, it's a, it's a great question. Um, I think traditionally hackers were like bank robbers, right? So, uh, they robbed banks because that's where the money is. Uh, but that's kind of changing. Financial institutions, as you mentioned, have been significantly investing in cybersecurity over the past ten, 15, even 20 years. And I think they now have fairly effective defenses.

Cybersecurity is also a board-level risk, uh, it's got high levels of focus constantly. So I think it's getting harder to rob banks—not impossible, but, but getting harder. So I think it's, it's kind of only natural for attackers to turn to softer targets or industry sectors where the investment hasn't been, uh, as substantial over the, over the past decade or so.

So I think there are kind of other ways that, you know, other critical suppliers or, or supply chain partners that can be monetized now, that hadn't been looked at in the past.

So I think ransomware attacks really, uh, are fueling this in some respects—so I think the success that the, uh, extortionists are having with ransomware attacks. Uh, and also in some cases, you know, of late, there's been a lot of talk about insurance companies and the underwriting the risk and the role that's playing in this type of attack as well.

So I think there's, there's new incentives for attackers to go after nonfinancial firms, um, institutions, where they, they previously haven't had s-, a lot of success.

Kind of switching to Nubank, in terms of, in terms of *our* focus, I think that Nubank, you know, is not immune to, to hackers' attentions. Uh, you know, we're, we're the world's largest privately owned digital bank. Uh, we've got 40 million customers, and we're growing rapidly. So with each new customer, you know, the target now back-, continues to get bigger.

All the types of attacks that I mentioned earlier in, in, in this talk are relevant in the context of Nubank, but I think we have some interesting opportunities in how we deal with that in being a, being a virtual bank.

So Nubank was born in the cloud. So we have some interesting opportunities to deal with, uh, security threats by building our own tailored solutions to the threats; and also, you know, that means that we can adapt really quickly as well.

So I think as the threat evolves, we're, we're not generally in a vendor-dependency cycle, where we need to, you know, wait for a vendor to kind of improve their security with something that we can act upon. So, it's been an interesting dynamic to kind of Nubank.

As well as that, Nubank's continued to make—and *will* continue to make—significant investments into cybersecurity, uh, as our reputation scales. So essentially, this is going to be, obviously, essential to our customer-centric journey.

But I think in terms of the question about the switch of focus from financial institutions to nonfinancial, um, I think there's some, some obvious incentives now for attackers, uh, to go after probably the weakest link in the chain.

Ketan Patel: Thanks, David. I think we'll, we'll touch upon, uh, vendors a little later in the discussion, but I'm glad you brought that up. And I really liked the quote from Willie Sutton—for those of you who aren't familiar on, uh, when they asked him why he robbed banks, he said, "That's where the money is."

Uh, but getting back seriously, um, Alonzo, I'd, I'd be interested in your thoughts on this. And particularly since you, you currently work for a buy-side firm, but you previously worked for a sell-side firm, which w-, had more traditional physical branches, so you may have a different view on this.

And I'd like your take in terms of resilience in the financial markets relative to these differences on nonfinancial firms as well, given your experience.

Alonzo?

Alonzo Ellis: Yes. And tha-, thanks for the question. Um, you know, so you know, I th-, so the firm I'm at now—Vanguard—uh, you know, is a 46-year-old asset, you know, asset manager buy-side firm, as you mentioned. We are the custodians of 7-, little over 7 trillion and, um, in other people's money and client assets and information that we have to protect.

Given our, given the age of our firm, we have to sort of live in three worlds, as I share with our board, right? We have the, you know, we consider that the most modernized environment, which is the cloud environment. Then we have the open systems. And then finally we have a mainframe environment. And we have to protect all environments at, well—so we have to maintain parity with our security posture across all environments. And so that, that makes the job particularly complex.

Um, and then as you called out, I previously worked for a firm that also had the physical infrastructure, a very large physical infrastructure—footprint—as well.

And so, one of the benefits as you spend years in, in, in working in th-, the cybersecurity space with-, within financial services is, you have to be very adaptive in your thinking, you have to be very agile in your thinking. Um, it's not enough for, you know, you to just leverage a particular vendor solution off the shelf or, you know, a consulting-, consultant-crafted solution. You have to really make sure that you have engineers and architects who have really good knowledge of the tradecraft, and they have to—associated capabilities to develop countermeasures that may not have existed in the marketplace. That's really the only way you're going to survive.

And so it's not by accident that, you know, most large, uh, financial firms have figured this out, because as you stated, hackers have long had an interest in breaching financial firms, um—particularly for the assets, but also for the information—because, you know, even the information on clients, um—you know, social security numbers, tax IDs, additional financial information—can be used, uh, for them to obtain credit, for example, at a firm. So it's not just about stealing the assets, but it's also about the information protection.

Also, if you think about it from a nation-state perspective, there are firms that, you know, have been designated as significantly [systemically] important financial institutions—SIFIs—so they have, uh, an added risk of exposure to a major cyber threat, where it could potentially have a negative impact on the financial markets writ large.

So, because of all, you know, all of, all of these risks, you know, financial services firms had many years and, and—to think about this—it's been a board-level issue for, for many years—and they've made the proper investments to, to, um, defend against what we would consider, you know, the traditional type of attacks that, that you would hear about in the news, but they've also developed unique capabilities to deal with, um, APTs.

So that's the good news. The bad news is that, um, you know, the threat landscape continues to evolve. And so they have to keep pace, or actually stay ahead, of the threat actors. And that's no easy task. On top of that, most financial institutions work with, with several third parties—enterprise critical vendors and suppliers—that they deal with. And so that opens up an avenue for, you know, potential threat if those supply chains are not, not locked down—or those suppliers are not at the same level or parity with, with the controls that the financial institution has in place.

So it's a complicated model, complicated ecosystem, to, to maintain a proper defense-in-depth risk posture, but, you know, as it's, I would say for most major financials, they have figured out a way to get pretty, to get to what I would consider pretty good, solid defense-in-depth risk—defense-in-depth model.

Now, when you go beyond that market, and you look at, uh, areas such as health care, or large research and development organizations, uh, universities, et cetera—they have not quite gotten up to the level of where you'd see most of your top-tier financial institutions, um, at, as it pertains to cyber defenses.

And it's simply because they haven't had a, necessarily had the need to, until recently, to exercise and flex those muscles and to really sort of make it a board-level issue, which would bring about the appropriate level of sustained investments in cyber defenses.

That's happening now—you see it in health care; you're starting to see it more in retail, since the Target attack. But, uh, it's something that's relatively new, whereas for most financial institutions, this has been something that has been a board-level or CEO-level, um, issue since, you know, th-, the mid '90s, mid to late '90s.

Ketan Patel: Thanks, Alonzo. I want to follow up on one of the themes there. You said "defense," and being a risk manager, I always think of, like, stress tests. And from what I understand, around cyber risk, best practices of the stress tests is often called a "penetration test," where you have these red teams—as they're commonly referred to—attacking your systems, and you have blue teams playing defense.

Can you give us some insight how this works and what the best practices really are?

Alonzo?

Alonzo Ellis: Sure, absolutely.

So, uh, a penetration test is a, is really a hands-on way to assess the efficacy of an organization-stated cyber risk posture.

Red teams are typically, you know, either internal, uh, an internal team or they're hired cyber specialists who utilize real world attack techniques to achieve a predefined objective on target environments.

Uh, and so we use the term “capture the flag” exercises, uh—or the phrase “capture the flag” exercises—which, uh, simply means that their goal is to find a way to compromise a network endpoint, a platform database, or application, or user—or some combination thereof—to, uh, to test the strength of the firm’s cyber defenses.
We also leverage them in what are known as cyber range exercises, where their purpose is to emulate an advanced persistent threat actor, uh, to see if we can detect and isolate and eradicate the threat.

So the approach from a, a red team’s perspective is, is, is quite different than leveraging, let’s say, an automated tool for vulnerability scanning or a static analysis security s-, testing tool for u-, for source code.

In most cases they’re leveraging their knowledge of the tradecraft to develop attacks that are specifically designed to evade the defenses that have been set up by the company in a way that’s very custom built for that environment.

Uh, so think of their attack design as being the equivalent of a virus that was designed specifically with your DNA in mind. It knows everything about you, and it triggered—only triggers when it comes in contact with you.

And so, you know, there are automated breach and attack simulation tools that help automate some of their work, but it’s still to this day, mostly manually done, given the expertise and knowledge of the tradecraft needed—necessary—to develop something that’s specific to one company’s environment.

Now, the output of their work is intended to give, you know, the CSO and even the board basically a reliable validation of the potential effectiveness of an attack, should one occur against that environment.

Uh, and what they do is they work in conjunction with the blue team—better known as the security operation center, or the SOC—and the purpose of that collaboration is to really help them identify, um, not only the efficacy of their detection and response capabilities, but they also want to help them understand the implications of the existing vulnerabilities that may appear—that they may have in the network and their backlog, uh, and how they can—and how those vulnerabilities can be exploited by attackers to achieve the objectives such as, you know, a pr-, privileged escalation attack or data theft or some sort of asset misappropriation.

And so the—having a red team really, or pen testers, really unlocks value for firms, in that it helps companies to address not only the backlog of vulnerabilities, but, um, to do that in a way that, um, it’s much more risk-based, uh, so that they can prioritize, you know, what is—what are the most important and critical few things to focus on as it, as it pertains to preventative controls and risk mitigation in the event that, um, you know, they a-, they are hacked.

Ketan Patel:
Thanks for that, Alonzo.

I’d like to now move on and kind of revisit some of the events that happened in 2020. And on *LaSalle Street*, we’ve covered some of the financial market events in some previous episodes, but now I’d kinda like to get to more of the operations and get your guys’ view from a cyber lens.

Uh, the pandemic basically brought about two tail events happening at once. We had a financial market stress event happening as well as a pandemic, which basically thrust us to remote working and creates its own unique challenges.
And what we're seeing increasingly is that remote working has gone from BCP to more BAU. So I'd like to hear your guys' thoughts and how you guys think the Covid impact of your firms and some of the changes around cyber risk.

I'll start with David on this topic and then s-, then ask Alonzo for his views.

David?

David Currie: Yeah, thanks, Ketan.

Um, I think, uh, to make a bold statement that, you know, everyone probably agrees with, that Covid's changed everything, uh, and I don't think we're going to go back to, uh, the way that we operated pre-Covid, um, in the future.

So, you know, a-, as an industry, we've had to react, to what really is an unprecedented event that hopefully we won't see again in our lifetimes.

Across the industry, uh, as a result of Covid, we're seeing, uh, some interesting, kind of, spikes in certain attacks—um, specifically things like social engineering, uh, attacks, uh, where there's been an increase in efforts to try and, uh, take over, you know, either staff members' accounts or, or directly through customers, or phishing attacks.

The one thing that, you know, I think the hacker community picked up on very quickly is that we're all spending, you know, increased ye-, amounts of hours in front of our screens, uh, on video conferences, uh, for much, much longer periods. And that's resulting in less time between meetings to, to actually kind of get the job done.

So I think th-, they're taking advantage of that, and the fact that we have less time to focus on responding to emails, responding to messages—everyone's, uh, acting, uh, with a lot more urgency in some cases. Um, so I think, you know, the likelihood of you clicking through on something you probably wouldn't have in haste now is kind of increased.

So I think there's a, there's a much higher focus, uh, needed on user training. And, and that's been one of the, the kind of key focus areas for us—uh, simulating phishing attacks, uh, periodically across all staff, trying to sharpen their awareness, to the threat that, you know, that they're being targeted with now.

And also conducting kind of more targeted phishing attacks—uh, looking at those who have sensitive roles, you know, key engineers, key, uh, management team members, even board members, that have access to, you know, highly sensitive information or, or increased privileges that could cause damage if their accounts were compromised.

As I mentioned before, Nubank was born in the cloud, so this has given us, uh, an interesting starting position when we've reacted to Covid. Um, we took a decision to protect all of our staff and go fully remote, uh, at the beginning of the Covid, uh, pandemic very rapidly.

The design of, of Nubank's cloud-based productivity tooling and our, our systems has meant that it was reasonably easy to mobilize everyone, and do it quickly without impacting business operations. So I think in reality, we, we kind of went fully remote almost overnight.

Um, the cyber risk profile for Nubank, however, i-, didn't change *that* dramatically, which was, which was kind of interesting.

Aside from the kind of increased threats that I mentioned—as far, uh, uh, as far as adopting video conference culture, everything, you know, everything else that we were, were currently doing inside the office, uh, we found that it was something that we could mobilize a workforce, um, and, and kind of do remotely.

So there wasn't too much of a-, an interruption in that sense, but we're still learning, um, we're still on picking, you know, attacks—we're still seeing, you know, increases or kind of anomalies in, in kind of, uh, you know, different types of attack vectors that we're still learning from.

I think honestly, we're going to continue to operate in a fully remote mode for, for the foreseeable future, at least anyway. And everyone's kind of adapting to this. Um, but you know, we're obviously very sensitive to, you know, the needs of staff members. So, you know, we, we realize everyone's home environment is different—not everyone has, you know, an environment that's conducive to, you know—as the office would be—to, to carrying out the job.

So in some cases we need to make allowances, uh, you know, in terms of home office setups—you know, enabling access to certain things, uh, in terms of printing and certain things connecting to, you know, a laptop that we probably wouldn't do in the office.

So we've had to kind of react to that and really think through kind of our, our approach to, you know, how we tighten up security on our endpoints, but at the same time, you know, allow flexibility of our workforce to, to be able to get the job done.

Ketan Patel: Thanks for your insights on the, the Covid-related impact on your firm, David.

Alonzo, I'd like to hear from you, similar, similar points: What do you think worked well? Any lessons learned from either your vantage at Vanguard or the broader industry?

Alonzo?

Alonzo Ellis: Thanks. Uh, you know, the key lesson here is that, you know, when you're in business continuity crisis response mode, things do not stay static, right? You have to adjust your network and application service adjunct authentication, EDR, threat hunting, vulnerability management, you know, and incident response playbooks to be *very* dynamic.

Uh, and so this is something that we know well, right? We, we do internal tabletop simulations and cyber range exercises—we've been doing that regularly for years.

What was different for us with Covid was the duration of the event, right? So most crises are resolved, you know, in, within hours or within a matter of days, not years, right?

And so given the expected duration of the response, we had to really rethink our approach to technology, to employees, uh, how we manage the workforce and supplier crisis response, um, which led to really a, a, a number of innovation, i-, i-, innovative changes. Um, so I'll share a few.

So on the technology front, we refined our security monitoring capabilities to account for increased network, um, increased work from, from remote locations. Um, we added additional detection and blocking patterns for Covid-related phishing campaigns, and we ramped up our security awareness training to ensure that our employees remained vigilant for the duration of the pandemic and beyond.

Uh, we increased the frequency of endpoint patching, limited off-VPN network access, enhanced privileged session monitoring, and beefed up VPN and VDI access capacity.

On the employee front, we were concerned with the fact that many of our new and even long-tenured employees were shifting to working from home literally for the first time. They were at risk of not having the right focus on security.

And so, you know, as they become more, became more complacent to working from home, we felt that they'd be more susceptible to lowering, *lowering* their guard and really exposing themselves to social engineering or spear-phishing attacks as a result.

And so to help address th-, *that* risk, we developed, uh, behavioral anomaly checks based on job profiles, so that in the event of a sophisticated threat actor or even an insider—um, they, you know, if they did something to attempt to compromise an endpoint or business process—we could detect it, contain it, and remediate the threat.

Also, while we knew the vaccines were on the way, early on, we had no idea of exactly *when* they would be available, and we clearly didn't know, beyond that, when we'd reach herd immunity, uh, and be able to return to, to, to office. So, uh, Covid contagion was added to our in-, insider threat response plan. It wasn't there initially, right? Uh, I don't think anyone had that in-, initially in their insider threat response plan.

And so, what we kept—what that meant for the security organization is that we kept some members of our, uh, security operation center on site and some at home in an A/B rotation pattern, so that we would remain resilient in the event of a Covid-19 contagion risk within our own SOC.

So, we also worked with our partners and, and our general counsel and HR departments to conduct a privacy impact assessment, which we use as an input to our rapid design and implementation of a firm-wide contact tracing and incident response program.

And finally, uh, we thought about the supply chain and the critical threat to, uh, having to, uh, a lack of access of, of, of the supplies that we need for critical technology and security purposes. And so to address *that* threat, what we did was we accelerated the purchasing, the purchase of planned, um, IT-spends for critical security hardware to forestall anticipated supply chain delivery issues.

And we were lucky that we did that, because that in fact happened. But we were, we were, um, well positioned because we had spares and, um, you know, as needed to address any equipment failures, et cetera.

Uh, and so for us, you know, the, the main key to success was that throughout the pandemic response, um, was really to avoid distractions and to focus on the critical few things that mattered most for our technical, cyber, and business resiliency purposes.

Ketan Patel: Thanks for that. Now I'd like to pivot to vendor risks.

We touched upon this a bit earlier. Uh, the topic of interest is not new, either. Um, industrial firms have grappled with this in terms of vendor controls with their supply chain for decades, and we've even seen recent headlines around semiconductors and how that's impacting some of the supply chains.

But looking at this from a cyber lens—which seems to be in, in increasing use of how vendor risk is looked at—and looking at the empirical case of the SolarWinds incident in 2020, where a third party's, a third party's vendor code made it feasible for hackers to access of *thousands* of accounts—including government accounts—I'd like to hear from both of you on how you think the vendor risk interplays with the cyber and if there's some new things you guys are looking at, or do you think the threat profiles increase?

I'll start with Alonzo, first take, and then ask David.

Alonzo?

Alonzo Ellis: Sure. You know, so as we talk about this method of attack—the supply chain attack—we ostensibly are talking about one of the oldest-known attack methods, right? The, the Trojan horse.

Uh, and so it's really sort of a simple—uh, uh, sorry, a modern, uh, version, or digital version—of the Trojan horse attack when you think about, uh, this threat.

And so in that case, you know, it's, uh, you know, the, in the case of SolarWinds, it was, you know, obviously a very popular and trusted network management tool that was compromised, and malicious code was hidden in the body of a legitimate software update. Um, and that let, allowed hackers to leverage that access to monitor communications, actual trade data, and disrupt operations, uh, for their targets.

Now, the thing that's important to, to know is that this, this threat isn't, isn't particularly ne-, new in terms of th-, the threat that, you know, a supplier could, could be attacked and that could lead to sort of a downstream impact. And, you know, many companies should have—I know in the financial services space, um, you know, they have some defenses around that. So, for example, segmenting portions of their network; um, doing deep-dive security assessments for enterprise critical suppliers who have direct connectivity to their environments; um, adding additional monitoring for, you know, those connections; working with those suppliers to ensure that those suppliers have the adequate protections in *their* environment—in fact, including that in contract agreements as well.

So it's not something that's, you know, I would say, is something brand new, but what's, what *is* interesting about it is that, historically, um, attackers would tend to go after, you know, the, directly after the large institutions, whether it be, you know, a financial, you know, institution or like a, a, a research facility—they would go directly *after* them.

Now, I think, you know, the fact that they're able to leverage these suppliers in, in, in, in different ways for surveillance or for, you know, direct attack across, uh, an aggregated list of, of targets is, is on the rise. Uh, not that it's, uh, it's not new, but it's certainly on the rise.

And so, one of the things that *we* discovered when, for example, the SolarWinds attack happened, we were able to get situational awareness quite quickly, uh, within our environment to determine whether or not, you know, the software was ever in use and, and if it was active in, in our environment. And I know for us, you know, the case—the answer in both cases was no.

It didn't take us too long to figure that out. Whereas with some of our suppliers, when we put the question to them, it took them longer.

And so, you know, one of the things that we took, uh, from that experience as an input, as when we did our post-incident review, was that, you know, we would make a commitment to open up, um, sort of more of our—what we call our governance processes and methodologies around, you know, tracking, for example, your CMDB, um, in a more effective way so that you *know* what assets are in your environments—what's talking on the wire. You have a good connection with your enterprise supplier management team so you know what contracts are being signed and you actually have, you know, a, an approval process that involves a cybersecurity organization, so that you know, if there's going to be a vendor that is providing critical software that touches your network, whether it has access to sensitive data, or both—um, that the security team always knows about the status of that vendor and, and their technology that's in the environment. And they should be able to get situational awareness pretty quickly.

So some of the, some of the, you know, lessons that *we've* learned and built into *our* maturity model: We've made a concerted focus to educate suppliers that have had some difficulty in getting—and in *responding* to us—to help them get to a better spot.

In addition to that, we've had a conversation with a limited set of peers and suppliers about essentially setting up a mechanism for us to, on the fly, set up a communications, um, sort of real-time sort of communications hub, um, whereas we, as we deal with something that we would consider a, you know, a business continuity incident, that we can bring them into the, into the ecosystem. And so they essentially become part of the response where we can talk in real time, get situate-, situational awareness across the board, and then move on. And so some firms may be un-, you know, may not be impacted; other firms may have limited impact and may be resolving an issue—uh, in which case, we will continue to track that as part of an incident response, even though it may be external to us, uh, until the matter is resolved.

Uh, and so that's something—that's an enhancement that, um, that we've added, and we've historically had a semblance of this for things that we would consider traditional business issues like pricing—being able to price data, being, uh, price, uh, the funds; being able to make sure we have access to market data feeds that with reliable information; and the ability for us to connect with custodial banks and to move money.

We've always had the ability to be resilient with it from a supplier perspective there, uh, to bring them into any sort of incident response there. Uh, we've expanded that to include things like the, the SolarWinds-style of attack with, uh, with suppliers that have those types of connections—network connections—and, and data connections to us.

Ketan Patel: Alonzo, if I could just ask a follow-up question: When it comes to software patches, which, whether it's the desktop or your phone, there seems to be a trade-off—that the patches often have security updates, which are meant to protect you, but, as you just alluded to, you're never sure what's behind the code.

So, are you, is this standard practice to test this in a, test the patches in a, uh, test environment before deploying it? Or how's that balance struck? Is it risk based? Just, I'd like to probe a bit on that and hear how you guys handle that.

Alonzo?

Alonzo Ellis: Sure, sure. So, when it comes to patching and patch hygiene, uh, part of our framework includes testing any new patches that we receive—and in a secure sandbox that's segmented and away from our production environment.

And so that way it allows us to not only do a security posture check, but it also allows us to do a resiliency check and to do all the appropriate regression testing to make sure that something hasn't broken, um, fr-, with posted application of the patch.

And so, um, that is, that's something that, a standard that we've had in place for several years, uh, and it's, and it's, um, it's, it's basically created a lo-, um, tremendous dividends for us because, you, we haven't, while we haven't seen a lot of risk on the security side, um, what we do see from time to time is, you know, you, you apply a patch and then, um, you lose connectivity to an upstream system or there's a data corruption issue that you have to address. Um, so just doing all of that in an isolated environment provides benefit from that perspective. But also obviously from a cyber perspective, you know, we can apply the patch, do a security posture check, uh, and then do, um, we actually profile, sort of fingerprint every running workload, the running workloads that we have in our environment so that we know how these applications should perform, and if they are doing something that, um, doesn't comport to our expectations of how this app should perform.

So if it's doing something on the network, or if it's trying to ping out to, you know, uh, an endpoint that it shouldn't be, then we'll take the appropriate measures to investigate it—including, you know, going back to the vendor, getting an understanding of, you know, did they have something that they missed in the release notes, or is there something that *they* weren't aware of that we, we may have discovered, uh, from a cyber perspective that they need to go and remediate.

Ketan Patel: Thanks for that, Alonzo.

David, I'd like to hear your views on third-party risk management in terms of cyber risk and how you look at it. Can you give us some of your insights?

David?

David Currie: Yeah, Ketan, just building on top of, uh, Alonzo's kind of, uh, comments there—which were, which are kind of, um, you know, really kind of reflective of how we feel as well—I think—let me set the scene a little bit in terms of Brazil.

So at the beginning of 2021, we saw two major events: a data breach, which involved approximately 220 million personal data records of Brazilian citizens, and then, uh, shortly after we saw in another data breach, of approximately a hundred million personal data records combined across two major telcos.

So this kind of creates a really interesting, uh, security challenge for all companies operating here that the personal data used to authenticate customers to, to register them for services is now being exposed.

So, um, in terms of vendor risk—thinking about third-party risk—um, this is something that really keeps you awake at night, and is one of the pillars of, of our security strategy.

Beyond kind of having effective due diligence and security built into contracts—which, you know, we've always done and traditionally kind of relied upon—we're taking more of a continuous approach to security assurance around our suppliers and partners.

So what we look to do is risk-profile and continuously monitor what our vendors', uh, security risks are—and by that, I mean, our security assurance team actively works with the suppliers. And to, to kind of support that, we're doing continuous vulnerability scanning, uh, of all of our suppliers, uh, for the bank.

And in addition to that, we're continually doing, uh, due diligence assessments. So, uh, beyond the, the kind of the initial contract, as we set up and operate with our suppliers, we're coming back to them, uh, and we're working with them to get insights in terms of how their controls are performing, uh, how they're meeting their compliance obligations, um.

You know, in the context of Nubank, we obviously have heavy dependencies on some, uh, big clouds—uh, infrastructure providers and software providers—but there's also some very unique, uh, vendors, uh, that we operate with in the domestic market within Brazil, that in some cases have monopolies over some of the services, and we don't have many options, uh, but to deal with them.

So we have to work very closely with them, um, in some cases having to educate them on their risk. And we've had some, some varying degrees of success—specifically, when we are able to kind of point out, uh, vulnerabilities in their public-facing infrastructure and allow, they've allowed us then to kind of come in and invite us in to, to kind of help work through those problems.

So I think we're trying to take a more hands-on continuous approach to managing the risk around our key suppliers. But we're aware for, for kind of all the efforts, uh, the best efforts that we're making around contro-, uh, you know, supply management, um, day to day, we're not in control of the suppliers' operations.

And so I think, you know, we're, we're kind of taking this view now that this is, uh, really a partnership approach to, to working with our critical suppliers, uh, and trying to help them manage down risk.

You know we've seen, in a lot of cases, that they don't have the same level of investment as what we would have at Nubank. Uh, and so therefore, the control expectations that we have, we need to figure out how to manage that and manage down the risk.

So I think vendor risk is something that we're not going to get rid of. Uh, for all the—again, all the best efforts, uh, that we have—and we do a lot of homegrown, uh, investment in building and technology—

we're still dependent, you know, on critical suppliers as part of the, the supply chain and part of the, the financial ecosystem in Brazil in order to operate.

And so I think this is something that is going to be a, a consistent risk that we continue to need to make focus on. But what's promising is, we're starting to see more opportunities and more, uh, service providers entering into the market to allow us to proactively and continuously manage the risk.

Ketan Patel: Thanks, David. It's interesting that both of you are talking about partnerships with the vendors, so it seems like more of a cooperative and collaborative model, which, which makes sense.

I think this has been a great session, but I'd like to close, um, with hearing your guys' thoughts and insights on what's top of mind, particularly around your cyber and, and tech dashboards. What, what do you guys focus on? I'll start with you, David, and then turn to Alonzo.

David?

David Currie: Yeah, Ketan, I think, you know, there's, there's probably three key points that's going to be, you know, a key focus in terms of industry trends or risks around, uh, cyber or kind of tech dashboards.

Um, specifically I'm, I'm kind of focused on—um, we, we talked a lot about cyber extortion, uh, whether it be ransomware or, uh, in some cases, *ransoms*, which, uh, uh, are less kind of public, but equally kind of worrying, in terms of attacks.

This is something that, uh, is going to continue to rise and evolve. I think the sophistication of some of the ransomware will get better. I think we're seeing ransomware now as a service. So it's, it's much easier for, uh, organized crime, uh, and criminal elements to take advantage of ransomware as a way to exploit and monetize, uh, cyber risk.

We talked about remote first, you know, this is going to be something, uh, that is going to be present in our lives, and we're going to have to continue to rethink how we're operating.

Uh, Alonzo made some, uh, awesome points about how their SOC is, you know, continually monitoring, uh, looking for, uh, anomalies that, you know, that may not have been present, you know, outside of kind of Covid. So I think we're, we're considering these same things as, uh, persistent, uh, that we're going to be dealing with.

And the other, the other aspect is, you know, looking really at our staffing needs—looking at the endpoint that, you know, whether it be a MacBook or, or a mobile phone or, or kind of, you know, a device that we need to put in the hands to, to empower people to be able to work remotely and cater for, you know, their varying kind of needs, as well as achieving good levels of security.

So I think you're looking at, uh, you know, more innovative ways how we can deal with security and making, you know, an appropriate balance, rather than trade-off, uh, giving more flexibility to kind of, uh, all their staff members.

And one of the other, the other kind of trends, uh, or kind of focus areas really around my strategy anyway, is going to be, uh, automating and, and creating more data-driven kind of instant responses.

Um, we made heavy investments, uh, into automation and orchestration in terms of security; and now we're looking to complement that with, uh, the mountains of data we're sitting on to then, you know, essentially build a self-driven security model where we can react to events like data loss, you know, or, or predict where we're going to have data loss events and start to react faster, contain those, uh, and prevent, uh, the risk before it really becomes, uh, an exposure, uh, for, for the bank.

So I think, you know, they're the, the three key points where we're continually focusing on, I think, for the immediate future anyway.

Ketan Patel: Thanks. Uh, Alonzo, I'll give you the final word on this in terms of trends or risks that you think we should be aware of on the cyber and tech front.

Alonzo Ellis: Thanks. Well, you know, it's—in terms of, you know, top three things, um. One is, you know, obviously this ever-present, or evergreen risk around r-, ransomware and similar types of, types of threats, threats, um.

You know, it's only, we're only going to see an, you know, an increase in sophistication and, and, um, in number of, of these types of attacks across various industries. Uh, and so, you, the real challenges for—from a cross-industry perspective—uh, and I would say it would also, um, include, you know, the public or the governments, um, moral governments in this, in this, uh, response capability is duly needed, right?

We need, we need to make sure that, um, there's a good public–private partnership, so there's good information-sharing on what the latest and, and, and greatest threat factors are, uh, as well as, you know, the proper defenses to, to shore up those risks. So that's, that's sort of one sort of ever-, evergreen thing that's always top of mind.

The second is, as we think about the ability for us to automate the incident response, um, that is something that, um, should be top of mind as well, because even with the best defenses in place, you're always gonna run the risk at, at some point, someone who will figure out what the zero day or, uh, you know, just, uh, a re-, a really focused advanced persistent threat actor, nation-state, um, they're going to figure out how to get a toehold in, in, in your environment or in the environment that was of a major supplier.

Uh, and so then the conversation shifts to, well, what can you do to really minimize the impact of that attack. Uh, and so the ability to leverage more automation, so, you know, I'd say, go from run books to, you know, to scripts and ultimately to intelligent bots, right? Where you can leverage predictive analytics through machine learning and, and A.I., um, which leads to, uh, technology, you know—in the case of cloud, cloud fleet technology—that would allow you to provide immediate response across, uh, a number of threats that may be hit-, hitting you simultaneously.

So you, you, you could have threat actors who have figured out a way to worm into your environment, and then all of a sudden hit you with a DDoS, a ransomware, and an insider threat simultaneously.

And so as you think about the needs, they're going to evolve, um, from a cybersecurity perspective; they're going to evolve to *have* to incorporate, you know, automation and orchestration as just a core component—a foundational component—of detection, uh, and, and incident response.

And lastly, it's the talent. In fact, I maybe should have put that first, because it's, it's always the talent, right?

And so, you know, there's a, there's a dearth of talent when it comes to, uh, cybersecurity—deep cybersecurity expertise; uh, and there's a war for talent to, you know, get access to, you know, those, those individuals.

So, you know, there should be a real concerted effort, and it's something that's always top of mind for me wherever I, my team, can add value by helping to upskill individuals who may have, um, adjacent skill sets—and basically incentivize them to maybe take on a, a, a role first in cyber, which may lead to a broader career path. That is something that, you know, is *very* important for us—we think, you know, we, we hear that our peers have, you know, uh, at least somewha-, somewhat of a focus on this as well.

And so the talent, you know, the, the talent focus is also something that I, I would say is top of mind for us and, and, um, you know, we, we include that as part of our key investment criteria to ensure that we will always have the talent to deal with these evolving threats, you know, as they, as they come.

Ketan Patel: I'd like to thank you both for joining *LaSalle Street* and sharing your experiences and insights; it's certain to have informed all of our listeners on this episode. Thanks, David. Thanks, Alonzo.

Alonzo Ellis: Thank you.

David Currie: Thanks, Ketan. Thanks, Alonzo.