accenture

HOW WAR IN UKRAINE AFFECTS SECURITY AND BANKING

VIDEO TRANSCRIPT

Michael Abbot: So everyone, thank you and welcome Michael Abbott. I lead our global banking practice here at Accenture. And I want to talk to you a little bit about what we're seeing in the banking sector more broadly outside of the cyber components, but in particular around banking and what's happening from the from the Ukrainian Russian invasion.

Here. So a couple of things here. 11 big takeaway is to look at is that if you look at the impact this has had to the banking system, itself or to the banks themselves in terms of safety and soundness, when we look at it, what we see is we see that the banking impact is actually very moderate. So it's a it's if you look at any of the individual banks that might be affected, most of them tend to be in Europe at the moment, even if they wipe out all of their investments in Russia at the moment or any relation to the side of that, what you'll see agency that generally they're looking at less than or about 1% of their Tier one equity capital. And what I mean by the 1% is 100 basis points off of call it, you know, anywhere between a typical of 12 or 14%. So maybe a seven to 10% net reduction in tier one capital, even if they take and they write off the entire investments on that side.

So the most important thing I've found to take away from this is that this has this has had an incredibly negative impact on the Russian banking system. But on the Western banking system, the actual impact has been relatively muted and relatively light at this point in time and anticipate it to probably remain that way. As many of you are aware of, there was a shift, there was a shut down in Swift by many of the Russian banks.

And what happens in that sense is that you do it's like having a friend that you don't like. You end up shutting that person off from the ecosystem, but everybody else can still work together inside of that. And as long as that still holds what you'll find, you'll find there'll be continued to be incredible pressure on the Russian banks and on the Russian side of the equation.

But it does business on that side. But for the rest of the banking system, it will be it will be relatively unaffected. And we do believe over time that the impact will be incredibly severe. I mean, Russia was able to do capital controls to be able to work through this for the first several months. They're already now starting to see the effects of that.

And you see that certainly if you if you watch the news, you see the effects on supply chain, the inventories, food supply, and also, frankly, as they do let those capital controls go, I think you will see also a readjustment. You will see a readjustment, the currency and the two sides of the Russian equation from that point of view.

So it will be incredibly severe on the Russian banks, but it will be relatively not so severe on the European banks. And when you look at that, even take it to a broader step and you look at what's occurring globally, what you find is the impact to the US banks and to many of the Asian banks will also be relatively minimal at this point in time from direct exposure to Russian banks.

This obviously sets aside any of the potential cyber scenarios that we might discuss and

other components that we'll talk about in a few minutes here. What we are seeing though, and you're already seen as we've seen it in our own world, is we've seen almost a 50% rise in the last several in the last four to five weeks of inbound and AML KYC for the work that we do with various banks around the world, just in terms of raw volume coming in and so you're going to continue to see that rise, I believe in AML, KYC and also suspicious activity reports.

And looking at that, especially as increasingly number of oligarchs are added to West. And you have to there's a lot of work that has to be done, obviously, around drilling down to each of those components. But you're also going to see, we believe that extending to regulatory oversight and you're going to see it extended the regulatory side, what we've seen in the AML, KYC world start to bleed into the cryptocurrency world.

Now, so far, cryptocurrency has actually been there's been two sides of this equation on cryptocurrency. One side is that Ukraine itself has actually legalized it as tender, and that's allowed an enormous amount of donations to be able to make it into Ukraine and be able to be used for both humanitarian efforts and also for military efforts. The flip side of that is there is a large worry, although not proven yet, that the Russian oligarchs have handled have hidden a significant amount of money in the cryptocurrency markets.

If you had seen that, you would have seen, I think, a very different scenario over the last several months. But nevertheless, we do believe that there's going to be regulatory oversight will very decidedly creep into the cryptocurrency world. And you've already seen it with the shutdown of various exchanges and being able to let Russian citizens get into those exchanges.

But obviously that does not stop it from moving anywhere across the world. So I think we will. That's an area to continue to look out. And that said, on a positive note, and aside from obviously the longer-term oil prices, what we've seen around the world is there is excess consumer savings coming out of the pandemic. So if you look at post COVID and almost every world around every country around the world, you've seen somewhere between about 15 to 20% of the bare minimum, upwards of 50% excess savings in consumers consumer bank accounts.

So that combined with a combination of low unemployment, we believe will act as a buffer to buffer to buffer to losses that the banks will face in that front. So in many ways what the banks are looking at here is probably the last point on this page and the most critical one, which is what will be the longer term impact, both of the increases in oil prices and frankly potentially also the, you know, the decrease in availability of food supply that may come, it will drive further inflation into the system.

So from that perspective, what we do anticipate is we anticipate you will see a rising rate environment. It could be quite substantial over the next several months, especially to kind of tamp down that inflation. And the question will be is how does that happen on a global basis? It's pretty clear that if you look at both the both the UK and Australia, you look at how much more they're farther ahead the rest of the world, you could argue that falling behind that is probably the US Federal Reserve has been falling behind that will be the ECB on that front.

So how that plays out we think is going to be the most the biggest impact the banks and then longer term it'll be the impact ultimately of a recession or unemployment that will drive the losses. But as we see it right now, the actual loss rate in the banking industry is relatively contained from the direct exposure. It's also contained because you have excess savings, low unemployment.

They should be able to buffer through the near term oil crisis, at least for the next several quarters. And then what you're looking at is depending on where all this plays out over the next six months or so, will determine ultimately whether or not the banks see losses coming out of this. Probably most likely in 20, 23 and probably not until the middle of 20, 23.

So with that, I'm going to turn it over to Valerie. So thank you.

Valerie Abend: Thank you, Mike. Hi, everyone. I'm Valerie Abend. I lead our global financial services security practice for Accenture. I really appreciate the opportunity to join with all of you today. And thank you to Nelly and to Mike for laying the groundwork as I talk through the various cyber threats specifically to the banking system. As we see it, we've laid out six major themes and the potential impacts from those themes.

And I'll talk you through them here today. And then leave you at a high level with some countermeasures. As I hand it over to my colleague, Dave Daley, to talk through more specifics about what you can do to actually manage your risk against these six themes and these impacts. So starting with the first theme, I think the biggest concern we have is really that there would be a shift and we've been seeing this shift kind of happen over time, but that that would get accelerated around what we call multi-pronged multi-dimensional attacks to financial institutions, as well as to critical financial market infrastructures, specifically in retaliation to the sanctions and these are not only focused on ransomware or pseudo ransomware, as Nellie was talking about, but availability style attacks, cyber fraud, all different types of of attacks extending to not only an individual entity, but actually targeting the entire value chain from creation of the transaction all the way through clearing and settlement of that transaction to really cause problems in the financial system. So the second area that we are concerned around is around third party or supply chain attacks, particularly impacting essential software as a service or platform as a service that are focused on supporting core banking and critical aspects of the financial system.

There could be potentially even in those software development teams for the SAS and PAZ providers, specifically Russian development teams. And that exposure does raise risk profiles for those third parties to the banking system. The third area that we're highlighting is particularly around cyber fraud and whether that be a rise in business email compromised, which we have absolutely seen, but also the creation of synthetic identity fraud and not escalating as threat actors, particularly in the criminal underground, seek new ways to avoid the sanctions.

The fourth theme that we're concerned about is the flourishing insider threat or insider risk, particularly as we've seen remote work persist. And we know that that's going to persist. That hybrid approach to work up to the workforce management in our banking system, we are super concerned that employees will unwittingly be exposing their access to Russian threat actors. The fifth theme is around extortion style attacks, advancing their destructive capabilities.

So going beyond just locking data, but actually changing data, potentially destroying and wiping critical data sets as an approach for undermining the financial system. And then our sixth and final theme is around hacktivist seeking out banks that are perceived to not be doing enough to disassociate with Russia and Russian oligarchs. And the concern that they will actually aggressively target banks.

The potential impacts obviously could be significant. You're talking about financial loss from large scale to service disruptions, potential undermining of data integrity, which raises not only the concern around the critical transactions, but actual counterparty risk, and then ultimately impacting your reputation as an institution and undermining the confidence in the institution or the financial market infrastructure. And then finally, we are concerned about, as Mike Abbott mentioned, the regulatory pressures, the fines, the growing number of incident reporting requirements or the complex regulatory oversight regimes.

And we expect that to increase over the next not just months, but over the next year. So moving on to the next slide, just a high level view of some of the countermeasures that you can take. We are specifically focused on the actions you can take now and in the future to harden your systems and to remediate quickly, to be able to identify where you have gaps and to close those

gaps and put in compensating controls, as I mentioned, around the identity issues, particularly as it relates to both insiders as well as to your customers, we're really focused on identity and access management.

We've seen that particularly in the announcements made by some of the government agencies and Nellie mentioned, see, so for example, I mentioned the concern around supply chain, so that governance over third party is really important and being able to demonstrate to the regulators how you're actually managing risk in a very well documented approach. The fourth countermeasure is incident response and crisis management we know that the time to prepare is never when you're having an incident.

And we really need to broaden out the crisis management approach to include third parties, to include counterparties and to make sure you're doing enough in that incident response and crisis management practice. And then finally, around recovery and resilience that ability to demonstrate that you can maintain integrity in your operations no matter what happens and being able to remain resilient and recover quickly your critical functions.

So with that, I thank you for your time today.

Copyright © 2022 Accenture
All rights reserved.
Accenture and its logo
are registered trademarks
of Accenture.