Deloitte.

That Makes Cents
Season 3: Episode 3
May 2022

Security in a cyber-everywhere world

Host: Bobby Stephens, principal, Deloitte Consulting LLP

Guests: Elias Oxendine, CISO, Yum! Brands
Vikram Rao, managing director, Risk & Financial Advisory, Deloitte & Touche LLP

Bobby Stephens: Hi, everybody. I'm Bobby Stephens and welcome or welcome back to That Makes Cents. This is, of course, the podcast where we break down consumer trends to explore their impact on businesses and on all of us. Today's episode is all about cybersecurity. You know, we find ourselves living in a cyber everywhere world where digital transformation continues to accelerate. It's pretty exciting, but it also increases risks.

What are the biggest challenges for an organization in managing cybersecurity? What steps are taken to navigate this increase in cybersecurity incidents? We'll take a look at that and more in this episode with the help of Elias Oxendine, the chief information security officer, or CISO, at Yum! Brands, and Vikram Rao, a managing director with me here at Deloitte, who focuses on cyber and strategic risk services. Thank you both for joining me here today.

Elias Oxendine: Thanks for having me.

Vikram Rao: Pleasure to be here, Bobby.

Bobby Stephens: Cool. So, to ground ourselves, I want to quickly start with some data that everybody can understand, specifically the key findings from Deloitte's future of cyber survey, where 41% of CIOs and CISOs we surveyed acknowledge that gaining visibility across the increasingly complex ecosystem is really the greatest challenge they face. That phrase in itself was a mouthful. So, we'll break that down into digestible pieces in this episode.

Vikram, maybe we'll start with you. Can you tell us what were the key themes from the report in this study? And, Elias, we'd love to get your take on those themes.

Vikram Rao: Sure, Bobby. It's a fascinating survey. We interviewed over 500 C-suite executives around the globe who are responsible for cybersecurity, and the survey really shines light on what are we really up against as cybersecurity professionals? So, three important themes I'll touch on, emerging technologies, the COVID pandemic, and people. So, we hear in the headlines about new cutting-edge technologies, like quantum computing, 5G, AI, and we don't fully understand the cybersecurity implications and risks they pose, and even existing technologies like cloud are rapidly evolving. And this creates a weird mashup of old technologies talking to new technologies with no traditional enterprise boundaries. And all of this makes it very complex to gain cyber visibility.

The COVID pandemic, that's the next theme we saw. We all know the COVID pandemic has accelerated the digital transformation efforts, and companies that didn't accelerate probably lost market share, so it needed to be done to survive. But this speed gives you less time to contemplate cyber risks. The technologies and processes that were cobbled together in the time of this crisis were supposed to be temporary solutions, but often, as we all know, it becomes a permanent solution. And it's like anything where, once a product and a service hits the market and cash is flowing in, nobody wants to revisit it or touch it and redesign security. It's quite disruptive at that stage.

And lastly, people. I mean, the entire corporate workforce has become remote. They want the ability to work from anywhere on any device. Customers are becoming more demanding with how companies treat their data. Regulators are doubling down on laws and regulations about data privacy. And lastly, hackers. I mean, they're getting more sophisticated by the day. And with these new emerging technologies, it has opened up a lot of new avenues for hackers to attack in this cyber battlefield.

Bobby Stephens: One thing that stuck out was still just the market and business kind of driving things first, and then a lot of other parts of a company having to react. Elias, you've been focused on the IT space for much of your career, and specifically security. How have these focus areas for you kind of evolved, compared to maybe what you were thinking about, say, five years ago? Would love to hear your expertise on this.

Elias Oxendine: Yeah, sure Bobby. Vikram was so spot on with the things that he was speaking to. I'm sitting here nodding my head very strongly on all those points. And so certainly, from the emerging technologies, as we look at things like AI, machine learning, et cetera, all these are great transformative innovations out there that propel the business forward. All those things are positive. Then what we do from a cyber perspective is make sure we secure those the best we can. But the challenge, as Vikram was alluding to, is just the mesh of the new and the old technology. But with all that innovation that comes from these emerging technologies, the hackers are also taking advantage of these exact same things. So, the use of AI and machine learning for us are great defenses, but the hackers are using them to their advantage as well to defeat those defenses. In terms of the pandemic, absolutely Yum! is not immune to this.

Certainly, when COVID hit, we were racing to get into the digital technology space more so than we have. And so we brought on new teams, new resources with the emphasis on technology to propel us forward. So, we brought on companies like Kvantum, TicTuk, all these things that helped us reach our consumers so that they could easily purchase our products. In terms of people, absolutely. Five years ago, would you have asked me how we'd be in the middle of a pandemic like this where everyone is remote and working anywhere from any device, any time. And I'm thinking there's no way, slim chance, maybe 10 years, not five years, but with the pandemic, it certainly has accelerated that.

But also to Vikram's point, the consumer is more focused on privacy now and their data. And what we've seen there is that change from not only is their data safe with us, but can they trust us with the data, because without that trust, there is no relationship, therefore, there is no sale that takes place.

Bobby Stephens: It's really interesting. You mentioned at Yum!, what you guys had to do during the pandemic, as people were still hungry. So, how are we getting into more delivery and third-party apps, and other ways to make it as convenient and safe as possible, that then of course opens up additional routes of collecting consumer data. And then the privacy aspect comes out. And I think probably across every industry companies were prioritizing digital over the last few years to remain competitive and get new products and services to market. And there was a really big emphasis on speed there.

That speed, though, kind of exposes organizations to new forms of risk. You guys have alluded to them a little bit when it comes to cyber. Vikram, maybe for our audience, can you paint kind of a high-level picture of what some of these popular digital transformations are? What are companies really focused on and kind of changing these days? And really further, how are they assessing the underlying cyber risks that come with these new things?

Vikram Rao: Yeah, sure, Bobby. There are some really bold transformations ahead. Let me give the audience a little bit of statistics on what are some of the top transformations. So, the number one was data analytics. That was the very first one, followed by movement to the cloud and ERP upgrades. Those were the top three priorities. The next one on the list was interesting and we haven't seen this in the past. The next one on the list was digitizing and modernizing factories, warehouses, manufacturing facilities, which traditionally have had really old archaic kind of technologies, so that was kind of fourth on the list. And then AI, cognitive computing, IOT, and connected devices, and then lastly, blockchain and crypto.

So, those were some of the digital transformations that companies are embarking on. And to your question about assessing and mitigating cyber risk, I mean, that requires a bit of a cultural shift. I would say, open lines of communication and seat at the table with the business leaders who are running these transformations. I think that's really important. Secondly, I would say integrated teams who can proactively assess cyber risk as the transformation is being designed, I think that's important, not after the fact. And lastly you need budget and leadership support and a mindset that cybersecurity is really an enabler, it's a differentiator for your business and not an impediment. Elias, I bet you deal with company culture on a daily basis so I'd love to hear your thoughts.

Elias Oxendine: Oh, tell me about it. In the places I've been and certainly in Yum! as well. So certainly yes, big cultural shifts are taking place here. I think first and foremost, with the digital transformation, with this transition, is that our business partners are starting to learn that in order for them to really be successful on this journey, is that they must involve cybersecurity earlier on in the process. And we're talking about things like a code development and infrastructure. And if you think about in the past, usually security is the roadblock. Security gets in at the very end of any type of a project and these kind of things. Well, with speed to market, you can't do that. So, certainly, they're breaking us forward in early into the process with a shift-left or day of security operations where we're involved upfront to make sure that we're not rolling any type of vulnerabilities or anything that can lead to a security incident once that particular product or solution goes to market.

Certainly, second thing, transition to the cloud. So, a lot of businesses are making that transition to minimize their physical footprint in the data center and then moving into the cloud. When people go to the cloud, a lot of times there's this mindset of, well, we'll put it in the cloud, we'll set it and we'll forget it. It's lift and shift. But at the same time, they need to understand, no, you're not done yet. We need to look at proper security configurations for those cloud interface environments, but also get tooling in place that makes sure that security compliance is being satisfied and met to make sure everything is secure and protected.

But then, Vikram, as you mentioned as well, too, we as cybersecurity, we want to be a good partner to the business. Therefore, we're working constantly to make sure that we are brought in early on projects and not at the end, because when you look at the number of breaches and incidents that are taking place today, we're all trying to be successful as a business and we need the consumer to do that. If the consumer does not have trust in what we're doing with the data and is secure, then we're not able to be successful from a business perspective.

Bobby Stephens: You guys hit on a lot here.

Elias Oxendine: Sorry, sorry.

Bobby Stephens: No, in a good way, and some pretty big things. So, things like moving your entire ERP and financial systems, changing the way your teams work together and when they get involved with big projects, engendering an important concept like trust that's kind of esoteric and actually making it kind of real within both an organization and to your end consumers and your customers. And so I do want to just extend on that consumer piece a little bit. As consumers, we really do expect personalized, targeted experiences, convenience, we kind of want everything from our food delivery, Yum! Brands, there you go, to travel, to health care to be frictionless, based on our needs.

But what we don't want is the sense of being followed or watched everywhere by marketers who want to feed us an endless diet of offers, solicitations, whatever. So, Vikram, we'll start with you. How are companies managing customer data differently? How are they connecting online and in-person experiences while also protecting privacy, and what does that natural tension look like?

Vikram Rao: Il'll say companies have come a long way in managing the customer data better. And if I look at the survey we did, over 90% of the chief marketing officers stated that they feel their organizations did a pretty good job balancing the data with customer trust. Now that paints a rosy picture and I personally feel the growth is somewhere in the middle, but more progress needs to be made, but they've definitely come a long way. But the regulatory environment is definitely forcing companies to get better organized with data. But the regulations, they have their own limitations. Privacy regulations are a patchwork of state, federal, global laws. Sometimes the requirements are conflicting, so it's a bit of a challenge to comply.

But I think companies need to really think about, if they really want to get customer trust, shouldn't they be really going above and beyond the basic compliance? I mean, the new generation of customers, they're passionate about many things, like climate change, socioeconomic issues. I mean, they're certainly a lot more passionate than I was when I was young. So, this new generation is not going to hesitate to boycott a brand if they don't think they're good stewards of their data. So, I mean, this whole concept of data privacy by design, that's really important.

And a lot of it is around educating your employees, thinking about, do I really need this information from my customer? And if I don't really need it then I shouldn't be replicating this data all over the place in the enterprise and I have to put the right safeguards. And lastly, be transparent with their customers about privacy.

Elias Oxendine: And I would say, what do you mean when you were young, man? You and I are still young. What are you talking about?

Bobby Stephens: You stole my joke.

Elias Oxendine: I was going to say, we're still young; we're still in the game.

Vikram Rao: Yeah.

Elias Oxendine: And so certainly, from my perspective what I've seen, once again, Vikram is spot on. For us here at Yum! and I assume, I expect other global companies do this as well too, but certainly what we do here from a Yum! perspective is that you've got these local, regional regulations that come up all the time. And what we've done is we have structured our data privacy team by regions, in which that particular team is responsible for what comes out of that region, making sure they know all the ins and outs, all the details, and then they drive our compliance to that.

So, that's been something we've had in place now for like the last 12 to 18 months. It's working very well for us, but these new privacy regulations, they come out all the time. So, we really try and make sure we're in front of that as best as possible, still some work to do there.

The other piece is, once again, it's that consumer engagement and trust. I don't want to sound like a broken record here repeating myself, but trust is so important. Trust is almost like a new currency today, in that we must make sure that we continue to build that trust and we maintain that with the consumer. And so, a lot of ways companies can go about with this trust is, there are things, requirements out there like data subject request, where the consumer can ask, "Well, what information do you have on me? How are you using it?"

But I think to Vikram's point, to even take it a step further, in our side, we're offering up consent and preference management. So, this is really giving that consumer, so, Bobby, the thing you were talking about here, how do you contact me? How do you engage with me? We're setting up a new tool that we have in our environment, our space, that we capture their consent and then we also capture their preference on how they want us to engage with them. So, once again, trying to build that level of trust and going a little further with them downfield.

Bobby Stephens: I love that and you kind of hit on two things that were a bit internal-facing, one is how you've organized your teams within regions just so you can be "ear-to-the-ground," so to speak, in those regions. And then the consumer preference center—important. With that said, obviously cybersecurity investments are a prime focus of investment for you, given your role and broader organizations today. To both of you, but maybe let's start with you, Elias. What are some of the more important methods and tools that you're deploying, in addition to what you just mentioned, to guide your cybersecurity investments and to track potentially the return on those investments?

Elias Oxendine: So, the focus for me is, it is strategic and then it's tactical/operational. From a strategic standpoint, most companies, and I've done this in my past, everywhere that I've been, is that we conduct these periodic security programs.

So, this is where you bring in, and you can either do this yourself or you can bring in a third party to do this for you, but they essentially come in and they assess the program on a capability maturity scale, the scale of going one to five. One being very initial, five means you figured it out, congratulations, go write a book, sell it, and make some money on what you're doing with your program. So, we would typically take this maturity assessment and we use pretty much this framework.

And I would share with you that once you take this assessment and you present it up to your board of directors or audit committee, this is something they're familiar with and they know, and once they see this, they know what it is, they get excited, they get locked in. So, certainly the program maturity assessment is one way you can do that. From a tactical, operational standpoint, we look at cybersecurity risk metrics, kind of KPIs or KRIs, that sort of thing. And the thought process is, with any type of investment to address and fix a KPI is that that risk, that metric itself will improve and get better. But that's how we know, if it does get better, then we know that investment is paying off dividends.

Vikram Rao: What Elias just said aligns well with what we've seen in the survey. More than 40% of the respondents said they use maturity assessments, cybersecurity assessments to guide their investment decisions. The next 35% said they use risk quantification tools, which includes some of the things that Elias just touched on, like KPIs and KRIs and what are your cybersecurity metrics and which metrics are the most important.

But I will say, this ROI question in the cyber field is not an easy one. I mean, it's much harder to translate cyber risk into dollars and cents, but there are some interesting tools in the market we're seeing for risk quantification space and just metrics and using some real data to convert that into dollars and looking at certain scenarios for risk. So, we're seeing some movement in the market there.

Bobby Stephens: So, with that, what do you find to be the most challenging aspect of the job, if maybe getting the funding for it isn't the hardest thing right now? What is the hardest part of the job, or what is the most challenging aspect of the job?

Elias Oxendine: I'll jump in here. I think, certainly three things, you see how I bucket things in threes.

The first two we've already kind of spoken to. So that digital transformation, just really keeping current and keeping pace, to support the business on that journey. Culture, we've spoken to this one as well. Also, to where we really gotta shift working in security, as we're the friendly security guys. We're not bad parts of the business. So, that's another thing for us. But what's really hitting and we haven't touched on this and just briefly is finding and retaining that cybersecurity talent.

The market is, particularly for cybersecurity professionals, hot right now. And whereas typically in the past, I would try to find local talent, but since COVID has hit everything's remote, so I'm not just competing locally now, I'm competing on a national level and sometimes on a global level trying to find talent, but then once I have it, I gotta work to make sure I retain it as well.

Vikram Rao: Our survey was very similar. Digital transformations, hybrid IT, dealing with all of that were some of the biggest challenges. Talent was definitely on the top list for executives from a challenge standpoint. And in the culture, I mean, this definitely makes it even worse if the culture is rigid and not adapting to the current time. And cyber hygiene, that was also one other thing we saw because in large organizations with a lot going on and a lot of the breaches we see are not because of sophisticated attacks, but because of just basic cyber hygiene issues. So, that's definitely another challenging area.

To your question, Bobby, you talked about the funding. The funding has definitely become much easier over time. But I think what is becoming difficult is explaining to the CFOs and other executives, how is that, to my earlier point about how do you take that funding and how do you show the progress that this funding has reduced the overall risk and how does that translate to return? I think that's definitely a little bit of a subjective discussion.

Bobby Stephens: The risk and the scary factor only probably lasts for so long. And in certain areas we've got to show a measurable return also, which I think is fair. But that's good to know. And it's really interesting to hear you guys come at it from both, Elias, the hands-on experience perspective and then, Vikram, the broader view of the market and the survey and the data. It's a really, really nice back and forth. So, why don't we do a final question here. And for those who've listened before know that my final questions are either fun or a little open ended. And this one we'll keep it open-ended, not that cybersecurity isn't fun. So, I don't want to give that impression whatsoever.

Let's look forward-looking. So, the cybersecurity landscape, we've just talked about it. I mean, even in the last year, it's been very dynamic. So, how do you see it evolving over the next five years? What's one or two things that our listeners could take away as almost a prediction from you? We won't hold you to it, but I'd love to hear from each of you. Maybe, Vikram, you go first and, Elias, you follow up.

Vikram Rao: So, to look at how the cyber landscape is changing, you have to really look at how the technology landscape is changing. Some of the technology trends we are seeing are data sharing is becoming easier. I mean, COVID has made some of that easier because shared data was used for medical advancements, things like that. So, that trend we're seeing significant innovations in IT automations and cloud vendors is next. Blockchain is going to be ready for business and then an explosion of internet-connected devices. So, those are the technology trends.

Cyber is going to go hand-in-hand with all of those technology trends. And we will have to assess cyber risks as we go and adapt, and go from there. I do think we are going to see more use of AI in cyber. Both on the defensive side and unfortunately on the offensive side as well, meaning the bad guys. And then hopefully we'll see more cyber board governance, elevation of the CISOs role, etc. That's my take. Elias?

Elias Oxendine: I will add, I think certainly the technology view is the right perspective to look at it. And, Vikram, as you mentioned, we're going to see more of that and more AI and more machine learning. Today there's still a human in the loop to a certain extent. And eventually I think the technology will get to where it's tech versus tech. So, eventually I think the human will be out of the loop. Certainly elevation of the CISO into board positions. We've already seen some of that coming out from the SCC announcement I think last week about, similar to SOC, they want to see the same thing happen from a cyber perspective. And then, Bobby, since you put it out there, being a little froggy, I guess, with the metaverse. That's what's happening, what's going on now. We're still kind of waiting to see with this one. And I think given the use of the cryptocurrency and NFTs, and as businesses actually, well, some are already doing this, purchasing space in the metaverse to actually conduct business to where someone can go in with an avatar, order, and then have it physically show up at your house. So, still waiting to see how this plays out. I think there might be some new cyberattacks that are different than what we've seen in conventional ways. But watching that one closely and see what happens and what develops there. So, stay tuned, I guess.

Bobby Stephens: You left us on a perfect note. That is exactly the sort of question that I love to leave the listeners with. And lots to look forward to in the space, even if there are quite a few things we should also be looking out for, which I think is an interesting kind of thing, that when you're looking at cybersecurity and the advancement of technology and how to keep that safe and secure, you're kind of always striking that balance. So, with that, I really want to thank you both for your time. I want to thank you for coming on the show and really breaking down what is a pretty complex topic, frankly, for our listeners. But it's something that impacts them every, probably, second, or at least every minute, even if they don't realize it. So, I really appreciate it.

Vikram Rao: Thank you for having me, Bobby. This was fun.

Elias Oxendine: Thanks for the opportunity.

Bobby Stephens: Thanks. So, for those listeners who are interested in learning a bit more about the report that Vikram discussed today, you can search for *Deloitte 2021 Future of Cyber Survey*. Also, you can connect with Elias, Vikram, or myself on LinkedIn for more. Thank you guys for listening and catch you next time on That Makes Cents.

Learn more

Visit the That Makes Cents library:
www.deloitte.com/us/that-makes-cents

Join the conversation on Twitter
@DeloitteCB

This podcast contains general information only and Deloitte is not, by means of this podcast, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This podcast is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this podcast.