Beyond: A KPMG Cyber Podcast

Series 1: Destination Digital ID

Episode 4: From today to tomorrow

Imraan Bashir

[excerpt from future section]

This is a dynamic space that is evolving, even the standards are evolving, but that doesn't mean we need to sit and wait for all these things to settle.

Katie Bolla

[excerpt from future segment]

The consumers, we can look forward to a convenient, a seamless, a personalized, and a much more secure future.

Marc Chaput

[excerpt from future segment]

Rome wasn't built in one day. So it's going to be an iterative process. It's not too late to start.

Narrator

An ancient Chinese proverb reads: "A journey of a thousand miles begins with a single step." From finding the courage to take it, to making sure that it is a step in the right direction, we're closing out our Digital ID discussion with a focus on action.

[SFX – Theme music swells]

Hartaj Nijjar

This is Beyond – A podcast exploring cyber security and business today, tomorrow and beyond.

I'm Hartaj Nijjar, Leader of KPMG Canada's National Cyber Security Practice.

Journey with me into the world of cyber security to understand the vital role it'll play in protecting our future.

[SFX – Theme music fades]

Narrator

And I am your host, Tamara Stanners. Today we are bringing our exploration of digital identity to a close.

At this point, we've made an audio voyage into the future. You, our listener, should by now be familiar with what digital identity is, how it stands to change many facets of our current identity verification processes and what it might take to protect this newly formed system. Now, as our journey nears its end, we return back to the present.

In this episode, you'll have a chance to hear (once again) from each of our speakers, as they impart a few key takeaways for Canadian citizens, governments and businesses.

For, if there's one message our listeners should walk away with, it's that no one group will be able to bring digital identity to life on their own. It'll require a close and collaborative effort between citizens, governments **and** businesses.

With that, let's address the first of these three stakeholder groups – Canadian citizens. What can each of us do today to protect our identities?

Erik Berg

It's critical for consumers to first understand where their data is.

Narrator

We're hearing again from Erik Berg, KPMG's Technology Risk Specialist

Erik Berg

Different mobile devices, laptops, both physical (hard copy) and digital information that's scattered all over the place. It's critical to understand where that information is and what type of security controls you have over that information. You wouldn't be leaving your passport in an open mailbox outside your house. Same with digital information. It should have security on it. It should have encryption on it.

Second, be very diligent in how much you provide, uh, as far as personal information to third parties, um, they may not need it. It should be on a need-to-know basis, based upon a specific business and functional need. Unfortunately we sometimes see, uh, third parties asking for more information than they actually need and consumers happily giving over that information, which may not be necessary. So I think awareness on, on both sides is pretty critical.

Narrator

While citizens might still have a while to wait before a Pan-Canadian digital identity eco-system spans the country, we **can** do our part to protect our identities today. Be vigilant, aware and cautious. Not just for our own protection, but **also** that of our loved ones.

Yassir Bellout

We usually forget that in our word, young people, our kids also have access to internet. And one of the things that people (I'm a father myself, I have three kids.) and one of the things that we should do start doing more and more is watch out for our young, our kids. Uh, not only practice the good hygiene in using the internet and around digital IDs, but also teaching it to our kids. Better solutions are coming. I have no doubt around that, but meanwhile, protect identities, protect data of younger people is very important.

Narrator

Younger generations are digital natives. The bulk of their education, social lives and pastimes are on the digital plane, so developing a skillset around how and when to safely share personally identifiable information online is a must.

Dramatization 4.1 – Gone phishing

FADE IN:

SFX - Gaming arena. Tournament taking place. A father and son have arrived to their seats. Dad is watching while the son is on the tablet.

DAD

Alright Sam, what are we watching here?

SON

Just the greatest gaming tournament ever Dad - the League of Lords Mid-season Invitational. Those guys over there are the players and you see what they're doing on the big screen, right?

DAD (IGNORING HIS QUESTION)

It's so dark in here…where is the hot dog vendor?

(checks his pockets)

Ah darn, I forgot my cash.

SON (EMBARRASSED)

Dad. Come on. It's not 1904. You order everything from your phone now.

(switching topics)

Can I have your credit card?

DAD

Can you ask more politely please? And what for?

SON

May I please have your credit card?

Kurt just sent me a DM to download this new game. He says it's like really sick. You go around capturing kingdoms and earning jeweled armour.

He's already on Level 4 and I have to get it before he's untouchable.

DAD

Let me see that message for a second.

SFX – Passes phone

Okay, first off, this seems a little fishy to me. I mean, look at all these grammatical errors. And look, he even spelled your name wrong. Aaand, don't you think it's strange that Kurt is asking for credit card information directly?

Why don't you text him, huh? And ask him if he actually sent you that message.

SON

Ah come on Dad!

DAD

No "ah come on Dad". Either you write the message or no credit card.

SON (BEGRUDGINGLY)

Fine.

SFX – Typing on phone. Message send sound. Receive sound.

SON (SURPRISED)

Huh

DAD

So? Was I right?

SON (BEGRUDGINGLY)

Yaaaa… Kurt's never even heard of this game.

[FADE OUT]

Narrator

Just because someone asks for information doesn't mean they have a right to see it. We all need to stay vigilant and constantly ask the right questions **before** allowing anyone, whether in person or online, to access our personal information.

And while we do the hard work today to protect our identities, we do have a very bright future to look forward to.

Katie Bolla

With the implementation of digital ID, the shift of power and control is toward us - the consumers. We can look forward to a convenient, a seamless, a personalized, and a much more secure future. We can now determine who when and why someone or an organization or bring and might access or use our personal information with this empowerment. We can feel more safe and confident with the security of who we are in our identity.

Narrator

It's no surprise that on the road to a Pan-Canadian Digital Identity ecosystem, governments - the foundational issuers of identity – will play a vital role.

Marc Chaput

Building up that new digital identity and infrastructure will require effort from public and private sector. Uh, so these actors need to work together in order to deliver a strong digital identity framework.

Narrator

We're hearing once again from Marc Chaput, KPMG's Identity & Access Management Specialist

Marc Chaput

I think our country is a little bit late. It's not too late, but some other countries are far in front of us with this regard. So we need our public sector government to start working on the standard, the governance, all that is required, as a rule - compliance laws legislation that needs to be put in place.

And then we have the private sector who will be helping in building the actual infrastructure, which will be supporting that new digital identities. So there's many industries, who will be required to be at the table of that collaboration.

So of course it will take some time. Rome wasn't built in one day. So it's going to be an iterative process us. It's not too late to start, so let's get started and build that exciting and new identity paradigm.

Narrator

Where Marc encourages swift action, Sylvia Kingsmill, KPMG's Global Cyber Privacy Lead, whom we heard from in Episode 3, urges for legislative reform.

Sylvia Kingsmill

One call to action is legislative reform. We still have a long way to go to ensure that at the requirements that are needed to ensure the customer experience, the privacy protections, are there -- the trust, you know, the data minimization, all the things that are required to, in effect, make digital identity a reality for the government it starts with reform, legal reform. We still don't have a legislative framework, the rules of engagement for private business and enterprise across Canada, and for federally regulated entities through federal privacy law. We do have a provincial legislative framework that enables some of this to happen through bill 64 in Quebec, but the other provinces are still in consultations with the government with respect to how their respective laws are going to look and feel like. So in order for us to give citizens, businesses, and everyone who will be relying on ID in the near future, if we're gonna play this game, we need some rules. We need some rules of engagement. And that hasn't yet happened in a harmonized way across Canada.

Narrator

In this team effort of building a digital identity framework, businesses must also keep privacy at the forefront.

Sylvia Kingsmill

Think about it with a privacy first mindset.

Narrator

That's Sylvia again, speaking to Canadian business.

Sylvia Kingsmill

It's a cultural change. It's adopting privacy thinking. It's about looking at the emerging technology before launching into the marketplace, thinking about what the privacy and security default setting should be, so that we can get the trusted ID out there in an effective way. And since we don't have a harmonized legal framework to work with, I think it's on us to look to market solutions, industry standards and best practices to get ahead of the legislative curve and get outta the gate a lot faster. Cause it might be some while yet before we see any legislative change. So we don't wanna wait for laws to dictate the future of a new digital landscape. We wanna start adopting best practices and getting out there about a bit faster.

Narrator

There is a real sense of urgency for taking the right first steps forward, which is no surprise given the potential benefits of digital IDs.

Speaking of first steps, if you're a Canadian business executive listening to this episode today, what should you do to if you want to reap the benefits of the first mover advantage in the digital ID space?

Imraan Bashir, KPMG's Digital Identity Lead, shares.

Imraan Bashir

Understand your customers before you even embark on your digital identity journey. What are your customers' pain points? What are your use cases for interacting with them? How can identity even help solve the problems? There are some cases in business today where identity doesn't come up. A lot of transactions are anonymous in nature. Maybe it doesn't need digital identity, and that's fine. Priority number one needs to be to identify those cases where digital identity is needed in your business, where today you are accepting some sort of manual or analog proof of identity, or you are doing some sort of manual check in the background that could be made more efficient, more robust, and more trustworthy.

Another important element of a digital identity implementation is also to understand your place in the ecosystem. Are you an identity provider? Are you an identity consumer? Are you both understanding where you play in this Pan-Canadian ecosystem that we kind of dream of here of trusted sources, issuing trusted identity to relying parties or people that rely on this information. There is possibly a place where you play a role in multiple areas, so better understanding your organization's role in this ecosystem is important. And then understanding what standards you would need to follow, what rules framework you need to abide by in order to play in this ecosystem and be allowed to continue in this ecosystem as well.

Narrator

It's about seeing true value and use cases beyond the hype, but balancing this analysis with timely action.

Imraan Bashir
I encourage organizations to take a culture of experimentation in this space as well. This is a dynamic space that is evolving, even the standards are evolving, but that doesn't mean we need to sit and wait for all these things to settle. I worry about waiting too long and losing interest from the customer base and risk businesses becoming irrelevant, because we didn't change fast enough.

Narrator
One of the key challenges with any digital transformation is making sure that speed to market doesn't compromise security. And, as this is a podcast about how we can protect a digitally-enabled future, we'd be remiss not to point out the importance of staying ahead of the threat landscape.

Dramatization 3.2 – The ethical hacker

FADE IN:

SFX - Zoom meeting launch. An ethical hacker is meeting with a Chef Risk Officer to discuss a recent penetration test.

CONSTANCE
Good afternoon Ria.

RIA
Hey Constance.

CONSTANCE
How are you doing today?

RIA
Solid. Three coffees in. Have been running pen tests all morning, so feeling pretty productive for a Monday.

CONSTANCE
Great to hear.

Alright, we need to talk about that traffic check and the application gateway today.

But before we get to that, can you please share the results of the penetration test you conducted? Hoping …

SFX - sound of web interference

RIA
Uh Constance, you cut out for a second there.

CONSTANCE (CONFIDENTLY)
Oh sorry, I was just saying that I am hoping for good news today.

I know the round of tests we ran at the beginning of the year were all very solid, so this is just a formality. Regardless, how'd we do?

RIA (RELUCTANTLY)
Well… um… actually, this round I found a way into your data repository through a pinhole in the firewall.

CONSTANCE (SHOCKED)
Really? But we just patched a bunch of holes and completed the optimization exercise just last fiscal.

RIA
I know, but the threat landscape is constantly evolving. It doesn't take time for a coffee break.

(pause)

CONSTANCE (CONTEMPLATING)
Right…

(pause)

RIA
Listen Constance, you and your team are already ahead of the game just by dedicating the amount of time and resources that you have to strengthening your defenses.

But, coming from somebody who does this for a living, trust me when I say that these exercises can't be a once-a-year thing.

Attackers won't rest and we can't either.

CONSTANCE (ASSURED)
Right. I'll have our team look into this and assemble a task force tomorrow.

RIA (SUGGESTING)
Or maybe this afternoon?

CONSTANCE (CONFIRMING)
Or maybe this afternoon.

[FADE OUT]

Narrator
Remember: Cybercrime is easy. Protection is hard.

Attacks will always be a possibility and no matter how sophisticated your defenses, a false sense of immunity will only spell disaster.

If we are to keep our technology-enabled future safe and bring the full promise of digital identity to life, then we'll need to build security into the foundations of our identity systems and be proactive in maintaining strong defenses today, tomorrow and beyond.

I have been your host, Tamara Stanners. Thank you for choosing to take this journey with us and we hope you'll join us again in October 2022 for our next future-focused series. Until then, take care.