



Beyond: A KPMG Cyber Podcast

Series 1: Destination Digital ID

Episode 3: Down to business



Imraan Bashir

[excerpt from future section]

Digital identity is gonna be one of those things that become a difference maker for businesses.

Sylvia Kingsmill

[excerpt from future section]

For business owners, it's about giving their customers an optimal, seamless experience. They want happy customers. It's also about increased assurance.

Narrator

Somewhere at the crossroads of what's right and what's profitable, Canadian businesses will gain a new view into the promise of digital identity.

[SFX – Theme music swells]

Hartaj Nijjar

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

My name is Hartaj Nijjar, and I'm the National Cyber Security Leader at KPMG in Canada.

Let's travel into the realm of cyber security, uncover what the future may hold and how we can work together to protect it.

[SFX – Theme music crescendos and fades]

Narrator

And I'm your host, Tamara Stanners. Over the last two episodes, we've discussed the important role that identities play in the everyday lives of Canadians and have highlighted how the emergence of digital identity systems might effect citizens.

But, what will the shift to Digital ID mean for businesses? That's what we'll explore in this episode.

With the increased digitization of public and private sector services and rising expectations from customers, organizations all over the world now have access to more user data than ever before. And as privacy concerns and regulatory scrutiny grow,

the importance of knowing and understanding your data is paramount.

In the interest of learning what types of data requires protection, let's consider two key use-cases for identity data within a typical business.

Marc Chaput

There is two key ways that businesses are using ID data currently.

Narrator

That's Marc Chaput, KPMG's Identity and Access Management Specialist

Marc Chaput

The first use case is any organization involved in a business to customer relationship, have to manage information about their customer in order to do business with them.

And the second very important use case is to manage the employees of an organization. The workforce management is very important. There's many business process, which involve dealing with data of your employees.

Narrator

Regardless of the type of identity data collected, it's important to collect the data ethically and store it securely.

Imagine that you are shopping online and you stumble upon a fantastic new online store that sells, say, floral arrangements. With your cousin's baby shower coming up, you choose the perfect bouquet and begin to complete your order. You provide your payment information, name, address and email. Seems harmless enough. But now what? Where does all that personal data go? Where is it stored? Who has access to it? And how well protected is it?

Businesses have an important responsibility in keeping their client's data safe.

Sylvia Kingsmill

On the customer side, there's huge exposures with respect

to the overcollection and then subsequent use of personal information.

Narrator

You're hearing from Sylvia Kingsmill, KPMG's Global Cyber Privacy Leader

Sylvia Kingsmill

So the issue there becomes, you know, who's got access to what, and under what permission the general rule under privacy legislation you're allowed to collect customer data with informed consent that's transparent and visible to the end user. So the end user understands the purpose for which you're collecting their information.

The risk there is if it's not stored and protected with adequate security safeguards, there could be a risk of a data breach. So that's really the challenge of managing customer IDs. You can do a lot with the identifiable information in terms of misuse, unethical use of information. And so it really is important for organizations to protect the information that they, they collect.

Narrator

The term to note here is "overcollection". Not only is data overcollection unsafe, it's also a hassle. Users are put into a position where they need to re-share the same data over and over again with different institutions. This results in sensitive information being stored in a number of different places, which then requires additional cyber security investments to protect. It also introduces privacy risks that potentially expose individuals to unnecessary profiling and tracking.

Building strong relationships with your customers means earning and keeping their **trust** – something the advent of Digital ID stands to strengthen.

Sylvia Kingsmill

For business owners, it's about giving their customers an optimal, seamless experience. They want happy customers. It's also about increased assurance. Businesses will have trust that they're getting authentic information and it minimizes their risk exposures. So, in effect, they don't have to worry about the cost and the consequence of having a breach on their hands. So it's, in fact, not just easier for their end customer, it's also easier on them to have a more secure digital ID, because current solutions like scanning your driver's license, for example, and sending it by email are really inconvenient on both sides, and also really insecure.

Customers will feel empowered, right? Because they can share data when needed, they can revoke their consent. And, um, on the same side of the organization, the data custodian, the collection of information is not only compliant with their privacy obligations and law, but they are doing the right thing for their customers.

Narrator

Loyal customers, trusted transactions, and significant cost reductions.

Think about it, when all identification can be linked back to a trusted source, rather than being dependent on multiple standalone solutions, it'll allow businesses to rid themselves of the responsibility to constantly verify their customer's identities, which means more free time and resources to focus on making their business thrive.

Plus, jumping on Digital ID implementation **early** can lead to a significant competitive advantage, as Imraan Bashir shares.

We heard from Imraan back in Episode 1.

Imraan Bashir

Digital identity is gonna be one of those things that become a difference maker for businesses. If you are a business that offers instant and more seamless access to your services, because you accept digital identities versus a business that is expecting their customers to either wait on hold or wait for a code in the mail, or to go visit their bricks and mortar store at the earliest convenience. I tell you that the former is gonna win out 100% of the time in the digital future.

Narrator

As Marc Chaput shared earlier in the episode, in addition to customer data, another key type of identity information businesses leverage is that of their employees – a process that comes with a set of unique considerations.

Marc Chaput

There is couple of challenges related to managing employee data.

Narrator

That's Marc again.

March Chaput

So the first one is, uh, when an organization want to hire new talent -there there's a new world, uh, created by the pandemic. Some organization are, are hiring people without having them on site. So you need to be able to prove the identity and identify properly, uh, the person you are hiring.

Another very important one is, uh, onboarding process. So there's a lot of information related to onboarding process of your employee. one example is if you want to do a background check or gather banking information in order to pay your employee. There's several processes which involve the gathering, manipulating, storing information of your employee.

And the third one, which is very important is, granting access to your employee. You want to make sure you grant access related to the job of that new employee. You don't want to give your employee more access than what they need. So that's the third challenge.

Narrator

Of course today, there are many safeguards in place to make sure that new candidates and existing employees are indeed who they say they are. HR teams in organizations all across Canada put tremendous effort into ensuring that hiring, onboarding and offboarding processes are streamlined.

But these efforts are still very manual and repetitive. As such, Digital ID still stands to make its mark. Let's explore one potential scenario.

Dramatization 3.1 – New Employee

FADE IN:

SFX - Office. Keyboard. Light chatter. Water cooler glug's

NATASHA

Did you hear about that flag HR caught yesterday?

JUNG

Yeah, I heard it's the second one this week since we launched the new ID system.

NATASHA (SHOCKED)

Seriously? I'd obviously heard of people embellishing on their resumes, but I didn't know that it was this common.

JUNG

Honestly, I'm not that surprised. Before the centralized system, who would take the time to check if that diploma was real? I mean, I could photoshop one from Harvard in about five minutes.

(in a hushed tone)

I mean, don't tell anyone, but for my first job at Purple Juice when I was 16, I lied on my resume – said that I had worked at a coffee shop before. Hey, they hired me and I made some goooood juice.

NATASHA

(laughs) Well your secret is safe with me.

But obviously this is a different ball game. I can't believe that they not only lied about their alma mater, but also their senior-level work experience.

JUNG

Just imagine if we had offered them the Director role, they wouldn't have know which way is up.

NATASHA

It's fascinating to me what people do when they think they won't get caught.

JUNG

Except, now they will be.

FADE OUT

Narrator

When we embrace trusted sources and ongoing validation, fraud becomes much easier to catch. This alone can act as a deterrent for fraudsters.

Beyond attracting and hiring talent, Digital ID will also improve other facets of HR.

Marc Chaput

There's a way to be more efficient about the way we are doing

onboarding. We'll have a strong source tool that removes the need to store temporary files or paper ID of your employees.

And it will allow you to do a better job in evaluating the need for accesses of your new employee and to do access provisioning based on a need to know basis and, and the least privileged principle.

Narrator

Speaking of granting access, think about a scenario where access management can be the make-or-break point in a client interaction.

Dramatization 3.2 – The secure floor

FADE IN:

SFX – Busy office floor. Typing. Footsteps get closer.

HARJIT

Meredeth, it's done.

The contract is signed. Halper and his team are on the way to the secure floor as we speak.

MEREDETH (EXCITED)

Wow! You guys pulled it off, huh. That's amazing news. It's a huge contract, high profile too.

HARJIT

Yes, and the big boss wants you on our client's team.

MEREDETH (SHOCKED)

You're kidding?! That's incredible. Thanks so much for putting my name in.

HARJIT

Of course, you're the best person for the job and you've earned this. Do you have any meetings right now? If you do, cancel them. Come with me.

MEREDETH

Sure thing.

SFX – Both start walking. Two set of footsteps (men's and women's). Elevator dings and doors open. The two get in. Doors close.

ELEVATOR VOICE

Going up

MEREDETH

Wait, did you say they're meeting on the secure floor?

HARJIT

Yes, floor 28.

MEREDETH

Oh, but my security clearance hasn't been transferred from my old department yet.

HARJIT

Already done. Took only a moment or so too with the right approvals.

A year ago, it would've been a nightmare waiting for the transfer. Now it's all nearly real-time.

ELEVATOR VOICE

Twenty-eighth floor

SFX – Elevator doors open. Both walk out. Keycard swipe. Approving beep. Door opens.

MEREDETH

Definitely an improvement. I'm just glad I can be there for the client without having to explain that a security clearance kept me.

[FADE OUT]

Narrator

There is no second chance to make a first impression, so when it comes to strong client relationships, it's worth adopting

technologies that securely speed up administrative processes and make sure your people are where they need to be at the right moment.

In this episode, we've explored a few ways that the advent of digital identities might benefit businesses. As with any technology, digital identity will not be the magic solution that smooths out all the kinks and solves all internal access issues on its own. It does bring with it the potential for improved data security, lower customer acquisition costs, increased efficiencies and stronger client relationships. But, realizing this potential will depend on how we build the bridge from today to tomorrow.

More on what that'll take in the fourth and final episode of this series.

I have been your host, Tamara Stanners, and you've been listening to Beyond – A KPMG Cyber Podcast. Until next time.