Beyond: A KPMG Cyber Podcast

Series 1: Destination Digital ID

Episode 2: SecYOUrity!

Erik Berg

[excerpt from future segment]

Bank robbers before used to put their life on the line. It was high risk, high reward. It has now shifted to someone being in their basement, hacking for fun, because it's very lucrative and relatively easy to do.

Yassir Bellout

[excerpt from future segment]

It's important to understand that digital ID is not a magical solution that will make cybercrime disappear.

Narrator

Our personal identity cards, assets and information are invaluable. They grant us access to services, validate our histories, and prove who we are.

And in the wrong hands, the use of our identity information could have dire consequences.

SFX – Theme song fade in

Hartaj Nijjar

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

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

Let's explore together how businesses and Canadians can work together to protect what matters most in a digitally enabled future.

SFX – Them song crescendo and fade out

Narrator

And I'm your host, Tamara Stanners. Thank you for joining us on the second episode of our "Destination Digital ID" podcast series.

This time around, we will be navigating the perilous landscape of identity theft, fraud and cybercrime. We'll consider who might be out there looking to profit off of our personal information and how we can work together to keep our personal identity assets safe.

It might seem obvious, but let's consider for a moment: **Why** is it vital for us to protect our identities?

Erik Berg

Identity needs to be protected because it's the single source of truth. It proves that you are who you say you are.

Narrator

We're hearing from Erik Berg, a KPMG Technology Risk Specialist.

Erik Berg (EB2-2)

With access to identity information someone can cause some serious damage, such as identity theft, identity fraud, creating, fraudulent documents, passports, driver's license, the list goes on and on. It can cause damage to your credit information, tax debt, criminal records, and most importantly, the emotional damage that this causes individuals and the time that it takes to clear their records and their name is significant.

Think through an example where, you're trying to sell your home and you realize that there is actually a lean on your property, so you're not able to sell it. Trying to figure out what happened, you identify that, without you knowing, someone used your ID in a deal that went sideways and failed to pay. And, the victim of the scam tried to recoup their losses by placing a lean on your home.

Narrator

And that's just one of many possible scenarios of how identity theft or the loss of Personally Identifiable Information (or PII) could impact any one of us.

Nobody is immune.

What's worth noting is that cybercrime is just that – a crime. And just like in any crime case, there are victims and there are perpetrators. So, what are the stories of these cyber perps? What's their motive?

Erik Berg

There are many different types of bad actors out there, and they all have different motivations. So the first and foremost motivation for many cyber criminals is financial. So identifying, um, the easiest way between their hack and, um, monetizing the hack is, is critical for them. So there is, um, ways of, of monetizing their hack on, on the dark web, typically records, credit card information, healthcare information. It can be sold for hundreds, if not thousands of dollars. And many times hacks include hundreds if not thousands of records at a time. So it's very, very profitable.

There are also political motivations or "hacktivism" as we refer to it, as where they want to promote or, um, uh, promote the interest of their ideology or to make something happen for an interested party.

Revenge, typically internal threats, uh, include attacking with the intent to harm as a payback.

So we talked about motivations and let's just briefly talk of about, uh, ways in which, uh, access to, uh, um, information is obtained.

So there are many different ways of gaining access. So through the dark web, uh, it's as easy as actually just purchasing credit card information or healthcare records on the dark web and buying exploit kits where you can exploit systems. Uh, social engineering is also one of the easiest ways to gather sensitive information.

So one of the key takeaways is it's much easier than, than people think. So bank robbers before used to put their life on the line, um, robbing banks, and it was high risk, high reward. It has now shifted to someone being in their basement, uh, uh, hacking for fun because it's very lucrative and relatively easy to do.

Narrator

They might be depicted as these faceless mysterious figures hidden behind a wall of screens, but they're often not. With the risk and reward paradigm having shifted, a cybercriminal could be anyone. It could be your neighbour, your taxi driver…or maybe even someone you went to college with.

Dramatization 2.1 – Coffee with a hacker

FADE IN:

SFX - Busy Tim Hortons. Customers making orders and orders being called out.

TIM HORTONS WORKER

2 medium double doubles a cruller and an apple fritter.

HACKER (FEMALE)

Thanks

SFX - She grabs the drinks and food and walks to sit down. Passing by customers and tables.

She sits down at a table with a man, passes his coffee and the bag with his donut.

HACKER

Here's your coffee and fritter.

FRIEND (MALE – CONTINUING PREVIOUS CONVERSATION)

Thanks. So let me get this straight? Your boyfriend from UofM was a hacker and after we graduated you got into it too?

SFX - She takes a sip of her hot coffee. He unwraps his donut and takes a bite.

HACKER (NONCHALANTLY)

Yeah. I mean I was always naturally really good at coding and building programs, so it came easy.

Honestly, it's way easier than most people think.

FRIEND(BEWILDERED)

Wow… (pause)so you're really a hacker, huh? Honestly, I imagined hackers being these faceless characters in hoodies.

HACKER (LAUGHS)

Well, I do own a few of those.

FRIEND

(chuckles)

No, but seriously.

If you don't mind me asking, how does it work exactly, what you do?

HACKER

Okay, umm, let me try to explain.

SFX – Takes a bite of donut and gets distracted or a moment.

Damn these are so delicious.

Okay, think of it like in the physical world. You've got your house, right? It's got all your valuables in it. That means there's always a chance that someone might try to break in and steal them.

So, what do you do? You lock your door.

SFX – Coffee shop sounds throughout scene.

But some people…well they leave that door open. That's where I come in. I'll go house to house checking for these open doors.

SFX – Takes a sip of coffee.

I rarely use the front door. Too obvious. But the back door or a window, that just might be open. And if I get in, there's even a chance nobody would even notice.

Of course there are some houses that have security systems. I check for those first thing. It's too risky to hit a house with an alarm, so I mostly avoid them.

But sometimes (and you'll be surprised how often) there won't be any security system and a door or a window won't be locked. That's when I just stroll on in and gather up as much valuable data as I can. Then, it's mine to do with as I please. Most of the time I just auction it off to the highest bidder.

FRIEND

Huh, it's that simple…

(pauses, takes sip of coffee)

You're really inspiring me here to amp up my security at home.

(laughs nervously

FADE OUT:

Narrator

You - checking that your door is locked.

A security firm - coming to install an alarm system in your home.

Your neighbour - watching your house while you're away.

Or, the police - coming to your aid if there's a suspected break-in.

In the case of protecting your home, it takes a village to keep it safe. When it comes to your identity that responsibility is also shared.

Erik Berg

In this paradigm where we have bad actors, we also have good actors. So, people that work tirelessly to keep identity information safe.

Ultimately identity information, it's everyone's responsibility, whether it's governments, businesses, or consumers -- everyone has a role, and everyone has a place in securing identity.

The consumer is responsible for the protection of their ID and for who they provide that information to.

Once it's provided to the other party, there's a lot of blind trust being placed in that party to be the custodian and secure that information properly.

So when you share personally identifiable information with businesses, there's a certain expectation that they are protecting it to a certain level or standards.

Narrator

Today, businesses and governments are already investing heavily in protecting our personally identifiable information. Yet, many Canadians are feeling the tremendous impact of identity theft.

So, **why** is it that our current system leaves citizens so vulnerable?

Erik Berg

IDs are issued and it's the citizen's problem to protect that information. So citizens are then asked to share this information in every walk of life. So whether it's renting a car, booking, a hotel, opening a bank account, or requesting a loan, this information is shared with all those businesses and external parties. It's then the citizen who's left holding the bag if, and when these organizations suffer a breach, or if in the process of sharing their IDs, the information is stolen directly.

Narrator

As we go through various life stages, we will share our personally identifiable information thousands upon thousands of times. And though it's easy to think "oh, it'll never happen to **me"**, even the most cautious of us are not immune.

But having secure, digital sources for identity verification can make a big difference.

Yassir Bellout

Digital ID will change the risk landscape, because it will offer more control to protecting our IDs, protecting who we are in a digital world. Uh, digital ID will place focus more on, uh, sharing the information, how to share the information, what information to share and who it's shared with. It will provide them with more assurance of how they deal, uh, whether it's a commercial transaction or, uh, social media dealing or, or interaction, uh, on the internet for businesses.

It provides them with more control and more assurance around who they are talking to, and especially for commercial transactions, give them more assurance about the identity of the people they are talking to, and that those business transaction are ultimately legitimate.

Narrator

What's at stake here is a feeling of security – a knowledge that even if your personal information is somehow captured, there is a system in place to catch the leak and revoke access at the **right** time before any further damage can occur.

Imagine a world where your virtual assistant could help flag and prevent fraud.

Dramatization 2.2 – Mortgage application

FADE IN:

SFX - Kitchen setting. Water boiling. Instrumental Jazz in the background. YUSUF is cutting vegetables on a wooden cutting board, preparing dinner

A notification from IRIS (SIRI) sounds and a voice comes on

IRIS

You've received an Urgent Notification.

YUSUF

Open and read the notification, Iris.

IRIS

This message is to inform you of the use of your identity in a mortgage application.

SFX - Cutting sounds stop.

YUSUF

Iris, summarize details of the application please.

IRIS

Here are the details.

Your identity was used at the Beaujoler location at 451 Rue Montagne at 4:03pm today, April 15th.

The mortgage application submitted to La Fleur bank, totaling 745 thousand Canadian dollars, requires your approval.

To grant approval, say APPROVED. To flag fraudulent activity, say FRAUDULENT ACTIVITY.

YUSUF (IN HIS HEAD – CONFUSED, REASONING)

What? This makes zero sense.

Could Aisha have used it? Why would she? No…

Mom? She's owned her house for 30 years… Khalid?

No this definitely isn't them.

YUSUF (OUT LOUD)

FRAUDULENT ACTIVITY

SFX - potatoes get dumped into boiling water. Lid put back.

IRIS

Thank you. Fraudulent activity statement received.

IRIS
Please confirm your identity via retinal scan

SFX - Scan and beep. Processing sounds.

IRIS
Scan confirmed

2 Factor identification required

YUSUF
Send PIN via Text

SFX - Text arrival beep. Four keys typed and text send sound.

SFX - Confirmation beep

IRIS
Your authentication was successful. Access to your identity has been revoked and the mortgage application cancelled. We have notified Le Fleur bank of fraudulent activity.

YUSUF (RELIEVED)
Great. Now that that's settled…

Iris, remind me in 20 minutes to turn off the potatoes.

[FADE OUT]

Narrator
In the trusted pan-Canadian identity ecosystem of the future, identity will be verified in real time, giving Canadians a near-immediate resolution to otherwise very stressful situations. In essence, we stand to gain peace of mind.

But even with added controls, increased oversight and strong cybersecurity defenses, the system won't be perfect. That's to say that bad actors are relentless. They get smarter and more savvy by the minute. **And**… they're not going anywhere.

Yassir Bellout
It's important to understand that digital ID is not a magical solution that will make cybercrime disappear.

It's, uh, a way of better protecting what we have right now. Um, bad guys will always be looking for ways to circumvent, whatever protection measures we, we put in place, whether it's in the electronic word or in the real world, you see crime evolving around the same objectives in the digital word.

It's important for organizations to design systems by default, that offer ways, uh, of putting protection measures that will prevent the act and any potential malicious behavior. And usually that malicious behavior is just a way for us to say, a security breach, or tentative hacking activity.

Narrator
As Yassir points out, the **whole** ecosystem must be protected, not just elements of it. Cybersecurity must be baked into the process from the very beginning.

The secret sauce of security is when the right controls meet a secure supporting environment. To get this right and ensure we create a secure and resilient Pan-Canadian Digital Identity ecosystem, stakeholders from across the country will need to get involved.

Yassir Bellout
We need to make the digital transformation of digital ID safe. This is one of the, the challenges. This is the initial challenge. Now that being said, it's not the first time that in the digital word, call it whatever you want. Right now, we have these kind of challenges. We have every three to four years, we have major transformation in how we work and how we see our technology 10 years ago. Uh, smart phones were very young or just invented and not as broadly used as they are right now, where they changed our life. Five years ago, cloud technologies were not as used as they are used right now and so on and so forth. So one of the next things is digital ID.

One thing that we need to make sure is to bring all the stakeholders together. So from governments, technology vendors, legislators to basic consumers, which is not really done right now in other sectors, but they, we all have to sit together and make sure that we are designing it the right way -- the right secure way for the future in a sustainable fashion.

This is not an area where we can just let technology vendors, in my opinion, innovate. Uh, we certainly need them to invent, we certainly need them to come up with new ideas, but we need to make sure that these innovations work for everybody. So of course we, we need include all the regulations, regulatory frameworks, uh, make sure we broaden them, that we adapt them to the new reality, to the new world. We make them sustainable also for the future.

Narrator
It's not just about adopting the latest technology for the sake of innovation. It's about making sure that the adoption of that technology is well thought out, inclusive, and secure.

Our personally identifiable information is an extremely valuable asset, which will continue to be a target for attack. As Canada moves forward with digital identity adoption, it'll be crucial to bake privacy and security into the foundations of our digital ID ecosystem.

Thank you again for listening and don't miss Episode Three, where deep dive into how digital ID will impact Canadian businesses and the key factors that will amount to success today, tomorrow and beyond.

I'm you host, Tamara Stanners, and this has been "Beyond: A KPMG Cyber Podcast".