KPMG
cutting through complexity

Cyber security and digital identity management

At the 2015 CeBIT conference, a panel of three technology and digital identity management experts sat down to discuss cyber security and how identity management is being used to enable digitally led customer growth strategies.

As a society, our reliance on online services continues to grow, as do consumers' service expectations. With much of the ability to deliver a quality service experience depending on personal information, it's become critical for organisations to consider the balance between service experience and privacy, the difference between a credential and an identity, and the trust that is placed in digital identities. Mark Tims, Partner, Technology Risk and Assurance, and facilitator for the session, comments: "Digital identity is the new frontier for customer retention and differentiation." Even our national regulators are considering this issue, notes Tims, quoting Greg Medcraft, ASIC Commissioner: "The great draw card of digital disruption is the opportunity it brings. Digital disruption offers new forms of access, greater competition, and greater efficiency."

Defining consumer identity

There is sometimes a preconception that consumer identities are used by organisations for the purposes of controlling and tracking, but John Havers, Director at KPMG First Point Global, explains that access policy enforcement is really only one side of identity management. He comments that with consumer identity: "It's about being able to transact or seek information … using your digital identity as a credential and establishing an online relationship with a service provider or business." For Australia Post, an organisation based on trusted credential collection, consumer identity is about providing empowerment. Tien-Ti Mak, Chief Technology Officer of Australia Post, explains: "For us it's about enabling consumers to connect better with businesses and government."

Healthdirect delivers health services by contracting with service providers, managing ongoing operations and implementing governance structures so that Australian health services are provided safely and efficiently. One of their challenges, Bruce Haefele, Chief Architect of Healthdirect, explains, is that "identity at a consumer scale is quite a different problem than identity at an enterprise scale because when we have to scale to millions of consumers and they all have such different needs, we [need to] make sure that we're capturing just the information that we need to identify them and no more. So for us the digital identity needs to be something that's at the convenience of the consumer… at the same time we need to make sure that the interaction is appropriate."

Balancing privacy and experience

Haefele also explains how balancing privacy with a good consumer experience can be a tricky act. "We make a lot of mistakes trying to do it. On the one hand, if you try to push things into too rigid a fashion, consumers balk at the user experience and then no one wants to take the service. I think the key we've uncovered is that it needs to be a choice. We need to do it in a number of different layers and in a number of different ways because we're all so individual and what makes sense for me doesn't make sense for someone else." The layering he describes illustrates a stepped approach, whereby the service provider offers levels of assurance in accordance with the level of service being requested.

In order to be successful, Havers believes commercial businesses need to adopt "security concepts" and apply them to their business model. "At the end of the day, it's using the privacy concepts, the opt-in, the consent … to have a more enjoyable customer experience and to ensure that [customers] are retained by that organisation." Retaining customers also requires a deep understanding of their behaviours. Haefele explains: "We've had to move from analysing traffic to really understanding usage." This involves not only pinpointing exactly what users are doing, but also connecting all the dots over a set of visits.

"It's about being able to transact or seek information… using your digital identity as a credential and establishing an online relationship with a service provider or business."

Federated identity management

All panelists agree that a federated identity model is where we're headed in the future. This model would allow for identity providers to supply trusted identities to businesses using a common set of protocols and practices. Haefele outlines the main benefit of a federated-style model using the example of a company that does not have decades of data available to identify individuals. "I don't really want to go down the route of collecting a hundred points of ID and having to store it and make it accessible and auditable. We need mechanisms where there are organisations within industry that can provide those services to us. That then provides [another] leg where both of us [the consumer and the company] can trust that third party rather than everyone having to trust everyone individually." With this type of model, the consumer maintains the ability not only to grant the access, but also to revoke it at any time.

In order to develop this model, Mak believes the industry needs to come together and collaborate more so that we can take a wider view of how a digital identity might work. "We need to ask how do we create the standards, and how do we create the ways of inter-working and build organisational trust ... I think it starts with that first and foremost," he comments.

New forms of identity

When we consider the vast number of ways consumer identity is currently being used, its form seems likely to evolve. Says Mak: "I think identity today is still largely physical. It's me clutching my physical passport or my driver's license … and therefore it tends to come from a very small number of highly trusted government-based organisations owning that. I think in the future, it will become much more digital: your identity could be on your mobile phone or it could be on a smart chip."

If this sounds like something that would open up consumers to enormous security risk, Haefele suggests that consumers will have the ability to put time caps around permissions, "I also think we'll get to the ability to tokenise personal information, in other words, I can give you access to my personal information for a period of time after which it expires and you no longer have access to it. That will allow us to do transactions with highly personal information but I know I'm not leaking the information to sources I don't want it to fall into."

Where the challenges lie

In order to make effective use of digital identity, organisations need to understand the potential for it to be used in improving the consumer experience. Havers reports that over 50 percent of the work of KPMG First Point Global is now in the digital enablement of organisations, such as banks, but that they have to get the corporates to also have trust and confidence in the technology so that they can maintain shop fronts on various devices anywhere, anytime.

However, being able to track people anytime, anywhere comes with a level of ethical responsibility. Haefele says: "We are going to require codes of conduct for what you can do with the data. More and more we're starting to do marketing analysis, at a neuro-behavioural level where we try to ascertain what types of thought processes people go through to make purchases so we can position product. That's going to lead at some point to an ethical boundary that we're going to cross. And I think we've got to remember that there's a lot of literacy that will have to go around that."

And what will identity mean for the end consumer? According to Mak, it will serve a much broader purpose than it does currently, "I think identity [will] become very intimately linked with broader notions such as your reputation or your trust and so it's not just whether you are who you say you are, but 'are you a decent person' and 'can I trust you?'"

Ultimately, who you are matters more than ever. How we define who someone is will go beyond matching a name with an address and banking details – identity will include a record of behaviours. It's knowledge of the latter that can enable organisations to offer a much richer experience, but how we regulate the sharing of that information is still to be determined.

"It tends to come from a very small number of highly trusted government-based organisations owning that. I think in the future, it will become much more digital: your identity could be on your mobile phone or it could be on a smart chip… and therefore the number of organisations who are searching for your identity becomes much larger."

Contact us

Mark Tims
Partner,
Technology Risk and Assurance
+61 2 9335 7619
mtims@kpmg.com.au

John Havers
Director,
KPMG First Point Global
+61 7 3233 9766
jhavers@kpmg.com.au

kpmg.com.au

June 2015. QLDN12972ADV.