Managing Risk in the Scramble for Identity Data

Author

Michael Cerny
Partner – Tech consulting
michael.cerny@pwc.com
+61 (3) 8603 6866

Mary Attard
Director – Tech consulting
mary.attard@pwc.com
+61 (3) 8603 0773

Last year, Australian National University found itself on the wrong side of a cybersecurity debacle when Chinese hackers infiltrated its website, putting sensitive national security data at risk.

According to a July 2018 ABC report, holes in the university's IT security strategy had left the organisation vulnerable to attack from cyber criminals. But the case was also part of a pattern of Australian organisations who've neglected the role that identity and access management — a set of attributes or traits that confirms the legitimacy of a user's digital credentials — can play when it comes to safeguarding their organisation from external threat.

Our understanding of identity and access management often revolves around its implications for cybersecurity — especially in an online world that's shaped by tetra-bytes of our private and professional data. This focus isn't surprising given that only 53 percent of businesses embrace proactive risk management from the beginning of their digital transformation process and only 23 percent of companies align security precautions to their business objectives according to PwC's 2018 Digital Trust Insights Survey.

But failure to optimise and streamline identity and access management leaves companies open to more than just cyber-attack. It can delay human resource processes such as onboarding, leading to countless hours of lost productivity. It can add pointless barriers to the customer journey, leading to missed sales and dwindling loyalty. And it can lead to privacy concerns among citizens who've shared their most personal data with government institutions, making it challenging to regain their trust in the process.

Happy customers, empowered employees

You've probably experienced the pain of joining a company only to find out that you can't access mission-critical apps and programs that allow you to do your job to the best of your ability. For many large companies, inadequate identity and access management stem from HR systems that have failed to successfully capture quality data. The challenge? Understanding a new recruit's digital persona, the role that they will play in an organisation and accurately defining those entitlements.

Ideally, identity and access management should be proactive rather than reactive. Setting the profile for a new hire's digital attributes in advance can turn onboarding into a seamless process that empowers the employee. By the same token, a real-time, responsive approach to identity ensures that employees lose their access to programs and confidential data as soon as they leave an organisation, reducing the probability that a disgruntled ex-staff member will cause a future breach.

Investing in identity and access management systems that are seamless and accurate are also increasingly intrinsic to creating compelling customer experiences. In short, they ensure that your company provides the right services to the right person at the right touchpoint in the customer journey. The customer that starts a credit card application online and requires minimal authentication when they transition to a call centre is an example of identity and access management at its frictionless best.

Creating seamless digital citizens

These days, users demand government services more quickly. They're also less willing to traipse through red tape and bureaucracy. But how do government organisations balance this transition to customer-centric services and method such as biometric and global authentication with the public's fear that their data is unsafe? The introduction of My Health Record, a scheme that sees healthcare professionals match the identities of digital citizens with data on their drug allergies and medical history — one that's only been taken up by 20 percent of Australians according to a July 2018 article in *The Sydney Morning Herald — is a case in point.*

The Internet of Things — identity's newest frontier?

In the future, identity and access management won't just apply to people. From driverless trucks operated by multinational mining companies to drones owned by the military and GPS units that help us navigate, the process of managing digital identities will increasingly encompass things as well. Over the next few years, businesses will need to invest in agile systems and platforms that correctly identify and grant the access privileges to a growing universe of connected objects. This new IoT ecosystem will call for a centralised approach to authorising and de-authorising data and the ability to segregate user roles and privileges across different scenarios and environments.

Ultimately, the significance of identity and access management isn't just limited to security. It cuts across every aspect of an organisation and will become increasingly important over time. Businesses addressing and investing in problems associated with identity and access management will benefit from strong internal controls and better customer experience while a reduction in data loss and cyber attacks. Most importantly, they will pave the way for higher levels of risk resilience — equipped with the resources and systems to emerge from future challenges stronger than before.

References

https://www.pwc.com/gx/en/issues/assets/pwc-GSISS-2017-uncovering-the-potential-of-iot.pdf

https://www.abc.net.au/news/2018-07-06/chinese-hackers-infilitrate-anu-it-systems/9951210

https://www.smh.com.au/business/companies/you-can-t-undo-that-damage-how-safe-is-your-health-data-20180629-p4zokx.html

https://press.pwc.com/News-releases/pwc-digital-trust-insights-survey-identifies-10-opportunities-for-businesses-to-build-digital-trust/s/c8ce85d9-2369-4e41-a5b0-d127658de3eb