“It’s not a risk when I do it” – Australian workers’ attitudes fuelling rising cybersecurity concerns

New research from Forcepoint reveals half of Australian employees use Shadow IT at home, despite understanding the increased risk

SYDNEY, Australia – 24 August, 2021 – Global cybersecurity leader, Forcepoint, has revealed that more than half of Australian workers (53%) use their corporate devices at home for personal use, and a further 19% allow other members of their household to do the same – exposing companies to increased cybersecurity risk.

Rise in shadow IT

The newly released research, which investigates how the shift to working from home has impacted people’s behaviours and attitudes, shows that Australians are using Shadow IT at concerning rates. In addition to using corporate devices for personal use, half (52%) of workers are using personal devices to access their employer’s documents and services while working remotely; 40% use personal email or file-sharing cloud services for work purposes; and 29% use a personal back up device to save corporate data.

The main reason for this behaviour is simplicity – 35% of workers say company policies make it difficult to do work well without Shadow IT, and the same proportion say they need Shadow IT to get their job done. This number jumps to 43% of people who hadn’t worked from home prior to the pandemic.

Interestingly, Australians aren’t blind to the risks they’re taking with their Shadow IT use. In fact, the majority of workers say they understand the cybersecurity processes for using devices like tablets and smart phones (68%) and that they received additional training or reminders on cybersecurity from their organisation (59%).

Dr Margaret Cunningham, Principal Research Scientist at Forcepoint, commented on the results: “People use different criteria for judging others than the criteria they use when judging themselves, a phenomenon called the fundamental attribution error and self-serving bias. For instance, if we see someone merge across multiple lanes of traffic without a turn signal, we conclude that the person is a terrible reckless driver. Alternatively, when we do this, we justify our behavior using relevant context such as noticing a check-engine light. Risky technology use follows the same principles, where end users interpret their choices to use unapproved devices through a perspective that includes contextual factors like security friction, usability issues, and convenience.

“When looking at the results of this survey, we can see evidence of self-serving bias as many of Australians are engaging in risky behavior and Shadow IT use, while also reporting that they understand best cybersecurity practice.”

Who is putting organisations most at risk?

The research also reveals that certain demographic groups use Shadow IT more than others. One of the biggest differences is between men and women. Although both report similar levels of support from their organisation – whether that’s additional training, the right equipment to do their job or feeling valued at work – men are more likely to report that technology is a barrier for getting work done and report higher instances of using shadow IT.

Almost three in five (58%) of men stated that they use corporate devices at home for personal use, compared with 47% of women, and men are also more likely to tap into their neighbour's Wi-Fi connection to do their work (17% men vs 11% of women).

There are also significant differences between younger and older employees. Younger employees (under the age of 30) report far higher shadow IT usage as well as riskier behaviours with systems and devices. Almost a quarter (22%) of young people said they allowed family members to use their work devices, compared to only 7% of older workers (aged 53+). Younger workers are also more likely to use personal USB sticks to store or transfer work data (41%, vs 29% older workers) and to use a personal back up device to save corporate data (33% vs 23%). Finally, 52% of young people use corporate devices at home for personal use, compared to 46% of older workers.

Queensland workers reported being less reliant on Shadow IT than their neighbours in NSW and Victoria – which may reflect differences in lockdown severity across states. Only 43% of Queenslanders reported using personal devices to access work documents and services, compared with 53% of workers in NSW and 52% in Victoria. Similarly, only 13% of Queensland workers allowed their family member to use work devices, versus 22% in NSW and 21% in Victoria.

Despite the growth in Shadow IT, positive interventions from business leaders can support and guide those people struggling with the changing nature of work. This includes accepting that people will make mistakes and working with employees to ensure they truly understand cybersecurity processes and systems. In addition, understanding user activity and behaviour can help organizations identify risky users more quickly and mitigate the impact of mistakes or vulnerabilities before the entire business is adversely impacted.

Dr Cunningham concludes: "Companies and business leaders need to take into account the unique psychological and physical situations of their home workers to ensure effective IT protection. They need to make their employees feel comfortable in their home offices, raise their awareness of IT security and model good security awareness behaviours.

"People in home offices usually use Shadow IT not out of malice or carelessness, but to be more productive. You won't be able to stop them from doing that. Companies should therefore no longer approach IT security exclusively at the technological system level. Shadow IT can in fact lead to great innovation and improved productivity, and black-and-white policies simply blocking access will only lead to more workarounds. The focus should be on uncovering Shadow IT uses and re-setting policies where required, but also and most critically, ensuring that critical data is defined and appropriately protected as we continue in our new patterns of remote and flexible working."

###

Methodology
This survey was carried out by PureProfile and Forcepoint, which sampled 1,000 working adults in May 2021.

About Forcepoint
Forcepoint is the global leader for data-first cybersecurity. Forcepoint's behavior-based solutions adapt to risk in real-time and are delivered through a cloud-native SASE security platform that protects users, devices, and networks as people access the web and cloud, prevents the theft or loss of sensitive data and intellectual property no matter where people are working, and eliminates breaches caused by insiders. Based in Austin, Texas, Forcepoint creates safe, trusted environments

for thousands of enterprise and government customers and their employees in more than 150 countries. **www.forcepoint.com**

Join Forcepoint on Social Media
Facebook: https://www.facebook.com/ForcepointLLC/
LinkedIn: https://www.linkedin.com/company/forcepoint
Twitter: https://www.twitter.com/forcepointsec
Instagram: https://www.instagram.com/forcepoint

Media contact
Shannon Cuthbert
Shannon.cuthbet@n2n.com.au
0405 652 703