Media release

16 October 2025

QBE research reveals cyber blind spots and generational habits shaping workplace risk

A new report from QBE Insurance, *'Click, breach, repeat'*, reveals that cyber risk in the workplace is shaped by employee behaviour, not just technology. The findings point to vulnerabilities driven by everyday habits, misplaced confidence, and a lack of shared responsibility.

The research uncovered a striking blind spot, nearly 60% of employees believe they've never made a cyber mistake at work. This overconfidence is reinforced by 86% of respondents saying they feel confident in spotting cyber threats, despite the reality that many breaches go unnoticed.

QBE's Global Head of Cyber, Serene Davis, says this disconnect between perception and reality is a concern for organisations.

"While confidence can be valuable, overconfidence can create risk and delay recovery action. Many breaches aren't immediately visible and attackers often wait, or pass stolen data to others who exploit it later," Ms Davis said.

Among the most surprising insights, Gen Z employees - often seen as the most digitally fluent – are more likely than older generations to dismiss security warnings (55%), delay critical software updates (46%), and reuse passwords across personal and work accounts (72%), contributing to a heightened risk profile. (See graphs 1-3 for comparison).

"These cyber hygiene behaviours from our younger generations can open the door to cyber threat actors, who are increasingly relying on human error to exploit an organisation's cyber security," Ms Davis said.

"Younger generations are often juggling multiple devices, apps, and logins, and can be less tolerant of security measures that interrupt their workflow. This can increase the likelihood of human error, which is the leading cause of most cyber incidents."

The research also revealed a gap between how employees view cyber responsibility and how organisations actually manage it. When asked who they would blame if a breach occurred, 31% of workers pointed to their IT department, far outpacing executives (13%), third-party providers (5%) and even hackers or cyber criminals (26%).

"In an effective cybersecurity culture, responsibility needs to be shared and understood across the organisation, from the front desk to the boardroom. Unfortunately, for too many

businesses, cyber remains siloed as 'an IT problem,' leaving leaders underprepared to manage during a crisis and employees unsure where they stand," added Ms Davis.

The report, '*Click, Breach, Repeat'*, is available for download on the QBE website: www.qbe.com/newsroom/news/qbe-cyber-research-report-2025

Table 1: How often do you dismiss a security warning on your device?

	Gen Z	Millennials	Gen X	Baby Boomers
Always/often/sometimes	55%	49%	37%	27%
Rarely	28%	32%	36%	31%
Never	17%	19%	27%	42%

Table 2: How often do you use the same password (or slight variation), across work and personal accounts?

	Gen Z	Millennials	Gen X	Baby Boomers
Always/often/sometimes	72%	62%	60%	53%
Rarely	22%	23%	20%	22%
Never	6%	15%	20%	25%

Table 3: Have you ever knowingly delayed or avoided a password change or major software update because it felt like a hassle?

	Gen Z	Millennials	Gen X	Baby Boomers
Yes	46%	41%	38%	33%
No	46%	50%	53%	64%
Don't know	8%	9%	9%	3%

ENDS

For media enquiries, please contact:

April Brown-Turner
External Communications Manager

Phone +61 434 231 851
Email: externalcomms@qbe.com | april.brown-turner@qbe.com
Web: www.qbe.com/newsroom