AGE IS JUST A NUMBER

Gernot Hacker *explains why all generations have a role to play in cybersecurity*

The pandemic has had a profound effect on almost every aspect of our lives, with one of the most visible impacts on the business world being the shift to remote work. Less discussed however, is the way Covid has influenced the labour pool, with older workers retiring at a much higher rate than in previous years.

In-depth research commissioned by Appgate found that workers at state pension age, 50-66, are now leaving the tech industry at a rate of one in 10, a serious shift compared with the one in 25 we saw before the pandemic.

Our research, conducted in partnership with intergenerational expert, Henry Rose Lee, discovered this issue is having a particularly profound impact on the IT security sector. With the industry already suffering from a severe and prolonged skills gap, it can scarcely afford another drain in skills and knowledge.

Organisations must consider the impact of this exodus on their security capabilities, particularly the need for younger professionals to take on new roles and responsibilities, as well as legacy technology that they may be less familiar with.

An intergenerational approach that makes use of the strengths of different age groups is the key to success. Achieving this, however, often means overcoming some deep-seated misconceptions about what different generations bring to the cybersecurity table.

Ageism is prevalent in most aspects of our society, but is especially visible when it comes to the fast-moving field of digital technology. Older people are often regarded as being out of touch with the latest developments in technology and working practices. Indeed, research from Gallup found that workers in the Baby Boomer generation are often overlooked when it comes to skills progression and career development.

Juxtaposing this, our research found that younger workers are often unfairly seen as being altogether too technology dependent and always chasing the latest fad, with our research finding that Boomers frequently see young generations as being too trusting with technology and too keen to quickly adopt and utilise the latest tech. Accordingly, older workers often see their younger counterparts as an increased security risk due to acting too hastily and lacking knowledge about the organisation's systems.

Organisations can overcome the natural inclination towards ageism by acknowledging that each generation's traits and experiences provide value. Taken together, these strengths can also compensate for each group's weaknesses. Based on our research, we found that millennials, for example, can capitalise on the tech savviness that comes with having grown up in the onset of the digital age. They are quick to adjust to technology and working practices and can rapidly adapt to operational changes. However, the tendency to look for fast solutions must be tempered to prevent them from circumventing security controls and inadvertently exposing the company to increased cyber risk.

Boomers, meanwhile, have a caution born of experience that can be very beneficial when it comes to cybersecurity. Our study found that the increased emotional intelligence that comes with age is a useful trait for the problem solving and decision making skills needed for effective security.

Finally, Gen-Xers, the middle generation, can serve as a bridge between the two – sharing the adaptability of their younger counterparts and the experience of the older generation. Our research also highlights that this group mixes innovation with a desire for structure, with most regarding themselves as strictly adhering to homeworking security guidelines.

Those businesses struggling with the skills drain of retiring Boomers should also consider the possibility of hiring them back as consultants. 80 percent of respondents in our research said they would consider returning to the workforce in a consultant position, while younger respondents believed returning consultants would be valuable assets.

BOOMERS FREQUENTLY SEE YOUNG GENERATIONS AS BEING TOO TRUSTING WITH TECHNOLOGY

This approach enables organisations to retain the experience and expertise built over long years in the field. Boomer consultants can be particularly valuable when it comes to accelerating Zero Trust security frameworks and dealing with legacy technology, such as migrating data from mainframes, an area with which very few younger workers have familiarity. Organisations should consider transitioning to a Zero Trust security framework, which will allow greater cybersecurity control with less administration.

Those organisations that are fully aware of the strengths and weaknesses of different age groups can work to create an effective intergenerational approach. Actively mixing older and younger generations within cybersecurity teams can help to overcome a natural inclination towards segregating into age groups and deliver a balance between the digital agility of youth and the experience and caution that comes with age ●

Older workers have a caution born of experience that can be very beneficial when it comes to cybersecurity

Gernot Hacker is Sales Engineering Manager EMEA at Appgate