Strengthening Australia’s cyber security regulations and incentives - submission form

Educating digital generations on data, privacy, security, and online best practices is paramount for a safe and paperless future.

I have worked within some of Australia’s largest companies and have noticed a significant trend. I was responsible for developing simulated phishing campaigns and when reviewing the results, it was apparent that the younger generations within the company, those being under the age of 30, were clicking links and failing these simulations. These roles were mainly intern’s and graduates; however, this points to a larger picture. Is there insufficient security training in Australian businesses and Australian schooling and tertiary systems?

I’ve witnessed employees open their mandatory security training, click play, walk away from the screen to get a coffee then sit back down after it was finished. Most security training given to employees is terrible. Its either filled with cartoons or people with poor acting skills with the story line of a non-relatable scenario. Its not engaging and people do not find it interesting hence the need for a change.

People respond and react to people face-to-face. People respond to people who are engaging. People respond to people who are enthusiastic about what they are interested in. People respond and react to situations that are relatable. People do not respond well to computer-based corny cartoon security training that an individual cannot relate to. This is the state that Australia currently finds itself in, regarding security education and awareness training. To assist with this statement, IBM conducted a study where they found that 95% of all security incidents stem from human error.

Experts need to address security risk and threats to employees face to face throughout Australia. The experts need to be well versed in the different threats that different industries face and what these threats look like. Employees who deal with sensitive information need to be shown real world examples of how a company can come to a screeching halt if they simply click on a malicious link. I completely understand why people don’t want to engage in security training. Firstly, although essential, it’s boring, and secondly, an IT security incident translates to “Not My Problem”. Employees around Australia are still yet to understand that, an IT incident is a business problem, not an IT problem. Technology is no longer there to support the business with everyday functions, it’s there to enable everyday activities.

Security training has been the same for years now and yet we still see employees clicking on suspicious links. It doesn’t matter how good your security control environment is, one click can undo it all. As was mentioned, younger people within the business environment are the ones that seem to be clicking on links. This has highlighted that throughout school and university, students are not exposed to these types of threats. In turn, businesses who hire these individuals are hiring potential security risks. There must be a foundational knowledge of threats that are out there, and this needs to start at the schooling and university level.