Moving into the New Year, us in the cybersecurity industry are excited! We're all anticipating the 2020 Cyber Security Strategy with an optimism & eagerness to contribute, in what's promising to be a big cultural change for Australian cyber safety at large.

With this in mind, big changes require big work! We've seen Australian cybercrime skyrocket in the past lustrum. 2016 housed a drastic increase in cybercrime, in which reported incidents *doubled*. They climbed an even further 25% in 2017, and when charting out the current growth rate of Australian cybercrime, we still haven't reached a peak in this epidemic.

Still, we're excited! In the same vein that we've approached upon other nation-wide risk crises such as road safety, OHS and health-care, we believe that our 2020 strategy should see an increased focus on one of Australia's most successful and frequently utilised tools for success: awareness!

The Government's 2020 Cyber Security Strategy should incorporate a push for awareness in two parts: at a business level, and at an individual level.

Raising awareness at a business level:

One of our biggest challenges is facing the "It'll never happen to me" mindset in Australian businesses. Many organisations aren't viewing cybersecurity as a priority, and are yet to implement basic risk-controls.

It's well-known at this point that 90% percent of data breaches are caused by human error (see Kasperky Report), yet we frequently see businesses approaching cybersecurity by merely automating end-point protection and/or delegating an isolated responsibility to I.T. staff.

While these are important, we know that *technology* is not the main driver in cybercrime anymore, it's *people.* Antivirus and firewalls alone don't address the ever-increasing amount of phishing scams and password compromise that work because of simple human mistakes.

And in our experience, business-owners tend to neglect their cybersafety either until the risk is clearly outlined, or until they've inevitably experienced an attack themselves. After a business witnesses the reputational and financial loss that cyber attacks cause, they tend to move very quickly in improving their safety practices.

This is where we believe government support is needed, raising urgency and awareness *before* an attack happens. Strategy should be aimed at clearing the air and bringing awareness to business-owners with simple, meaningful, clear statistics.

We already have fantastic resources (such as Scamwatch and the Australian Cyber Security Centre (**ASCS**)) that can promote the urgency and clear damages that occur from cybercrime;

it’s a matter of delivering them to business-owners in an impactful way.

For example, this **Kaspersky real-time cybermap** tool that displayed global attacks as they happened was a real eye-opener for many business-owners. We’d love to see a similar Australian threatmap, utilising Scamwatch or ACSC reports for a clear, tangible portrait of cybercrime in Australian businesses.

The Australian economy loses $1billion per year to cybercrime. It’s a financial sinkhole that’s only set to worsen, but we can shrink a lot of those damages with simple business awareness. When you demonstrate to business-owners (large or small) the risks that they face in cyber, the improvements are massive.

Examples: Local ads on trams or local papers: **Did you know 1254 Businesses in Melbourne were a victim of cyber crime last month?**

Raising awareness at the individual level:

The best way to reduce human error (and consequently, risk) is to bring cybersecurity to the public conscience. Australians need to establish why our identities and privacy are important, and how they are exploited by criminals online.

For example, driving into the CBD you’ll often see large-scale advertisements with statistics on the road-toll or the classic “shave off 5km” campaign. These are powerful awareness tools use to immediately put the foot on the brakes, literally.

Government advertisements on cybersafety can be applied in exactly the same way, to an awesome effect. Slip Slop Slap reduced melanoma in youth by 5 percent per year. It’s simple, and its effective. We’d love to see the same applied for basic cyber-security in slogan-based ads:

- “**Brush up on your password hygiene**”
- “**Who’s really behind that email?**”
- “**When’s the last time you ran a virus scan?**”
- “**What does your credit score mean to you?**”
- “**Who can pretend to be you tomorrow?**”

Not only do these small measures improve individual safety and raise understanding of online risk, but they also facilitate a demand for safer industry practice from Australian businesses across the board.

The same pattern applied to the tobacco industry's change in packaging, and the fast-food industry’s shift into healthier menu items, and we’re ready for the same changes to Australian cybersecurity.

We believe in a bottom up approach to change. Government resources are key to spreading the messages. By empowering people with knowledge and understanding about why cybersafety is important, particularly *their* cybersafety, we can change their behavior as individuals.

This behavioral change and active awareness carries into the workplace, into the quality of industry at large and into the expectations of corporations and colleagues when operating online.

Whether it's in a Small Business or an Enterprise level corporation, countless cyber-incidents start and end with *one* person's mistake. Individual awareness is invaluable to Australian cybersafety at large.

Our government is in a position where we can comfortably promote the basics and raise awareness. By educating the everyday Australian on their relationship with cybersafety, we can prevent a huge portion of human-exploitative cybercrime and drive the changes needed to put Australia on the map as a leading cyber-smart nation.