THE CASE FOR AN AUSTRALIAN CYBERSECURITY ACT

Australia requires a specific federal Cybersecurity Act. It's too easy to square the blame entirely on the Optus and Medibank data breaches, when what these successful attacks expose is a lack of effective and comprehensive federal legislation. The new federal Minister for Cybersecurity, Clare O'Neil, was right when she declared Australia a decade behind the rest of the world.

The good news is that we have a successful working international example - Europe's General Data Protection Regulation (GDPR), that we can iterate upon. There is no need to 'reinvent the wheel'.

The bad news is the urgency with which we must enact this legislation. We desperately need frameworks that encourage corporations and government agencies to enhance their cybersecurity defences and data protection (encryption) in the event these defences fail. We also need effective penalties that deter data owners and processors from acting irresponsibly, or mis-managing sensitive and personally identifiable data.

THE BIG PICTURE

The recent Optus and Medibank data breaches, and the community outrage that has followed, should not be confined to issues of citizens' privacy alone. There is a much bigger picture in play. One that necessitates a single, comprehensive federal Cybersecurity Act. Cyberattacks are not simply acts of criminals seeking financial gain through stolen identities.

Cyberattacks are also used as weapons of national and economic harm – even warfare – designed to bring down critical national infrastructure, cause catastrophic harm to business and government IT systems, steal sovereign intellectual property and render defence and military systems ineffective. The war in Ukraine and continued Russian cyber-attacks upon both Ukraine and its allies illustrate that.

Equally, measuring the effectiveness of cybersecurity defences should not just be about robust prevention technologies. If the plethora of breach stories over the past twenty years has taught us anything, it's that networks are vulnerable. The Optus and Medibank data breaches highlight organisations' failure to protect sensitive customer data with encryption, ensuring it would be rendered useless when stolen by cybercriminals.

So, when our federal Minister for Cybersecurity (facing a national data breach affecting a third of our population's personal identities), reached for Australia's cybersecurity legislation only to discover it was "absolutely useless", we have a much bigger problem than simply protecting the privacy of Australian citizens.

FRAGMENTED RESPONSIBILITIES

The Australian government and intelligence agencies' swift responses to the Optus breach highlighted the fact that cybersecurity is not just an IT issue. It is a national security issue. Cybersecurity legislation must get the same treatment.

Currently, cybersecurity responsibilities are fragmented across a myriad of privacy, national infrastructure security and corporate legislation. A confusing assortment of legal rabbit holes makes it difficult to get a consistent level of transparency from organisations, let alone a unified set of standards that everyone adheres to.

If we are to affect meaningful change in cybersecurity legislation, there needs to be a consensus among the states, territories and the Federal Government. Otherwise, we risk repeating the limitations of the United States. Frustrated with the Federal Cybersecurity Act, the Biden Administration is only able to deal with Federal responsibilities such as health, telecommunications or financial services, the rest is done by individual states. In Australia, some of our most sensitive data lies in our health and education sectors, which are state run. If we are to enact comprehensive laws, these areas need to be front and centre of a collaborative government approach. It cannot be allowed to be fertile ground for lobbyists' negotiations that result in a self-interest driven result.

Europe set the standard for an overarching cybersecurity act with the GDPR. It has a mandate for the protection of sensitive information, so if you're holding information that can reveal identities then executives and the corporations themselves are responsible.

For example: if an email exchange server is shown to be vulnerable, and its owner doesn't apply an available patch to prevent an attacker from exploiting this vulnerability, if that organisation is breached it will be noncompliant. On the other end of the spectrum, if it is breached but the data within is protected by 'strong encryption' it's deemed to not be a breach as you've effectively protected that data from nefarious use. It is sensible, easy to understand and motivating; without requiring executives to become cybersecurity experts to ensure compliance.

The key to creating legislation that maintains a healthy balance between prevention technology (which works to keep attackers out) and protection technology (encryption keeping data safe when criminals inevitably find a way in) lies in setting similar non-technical standards. This way we can ensure cybersecurity best practice is being adhered to, without prescribing a specific method.

That said, a simple copy and paste of the GDPR would be insufficient. An Australian Cybersecurity Act needs to address more than citizen privacy as shown in the GDPR. It's been four years since GDPR was introduced and there are areas in which time has shown it may be enhanced. However, it does act as a great example for how to clearly assign responsibilities and should be considered in the development of our own frameworks. It took the EU nation states just two years to draft and agreed upon the GDPR. By comparison, Australia's 'Notifiable Data Breaches Scheme 2018 amendments to the Privacy Act' took nearly five years.

EFFECTIVE PENALTIES

A decade of relative inaction on cybersecurity has one lesson; penalties that cause both financial and reputational pain are one way to make an example of poor behaviour, but they don't help solve the underlying issues.

In the US, breaches of federal cybersecurity legislation can be a criminal matter, not just civil. A breach of Europe's GDPR can see a maximum penalty of €20m or 4% of annual international turnover, whichever is greater.

What these harsh penalties do not address is corporate apathy, particularly at the executive level. Liability after a breach may give customers a sense of justice, but positive behaviour change within an organisation may be better attained by additionally penalising the failure to listen to, or act upon, the advice of cybersecurity professionals. This may address both the need to empower cybersecurity staff and nullify the 'she'll be right' philosophy of some commercial and government organisations.

Whatever motivators are chosen, Australia needs clear and all-encompassing cybersecurity legislation with sharp teeth. It must set the highest legislative standard required for a national security issue, whilst providing organisations the freedom to find their own solutions.

The Optus and Medibank breaches are terrible for all involved, but from them we have an unprecedented opportunity. We must avoid the limitations of the US and learn from Europe's GDPR to create a federal Cybersecurity Act that will help keep our citizens, intellectual property, government and business secrets safe for the long term.

ABOUT SENETAS

Senetas, is an Australian public company (ASX:SEN) specialising in cybersecurity. Senetas solutions have been trusted to protect much of the world's most sensitive information for more than 20 years.

A global leader in the protection of data transported across high-speed networks, Senetas provides network independent encryption hardware and virtualised solutions. These share a crypto-agile and quantum resistant cybersecurity platform.

Senetas content security solutions include the most secure file-sharing and collaboration application with 100% data sovereignty control, and proactive anti-malware solutions providing enterprise-wide file security.

Senetas solutions are distributed and supported internationally by Thales, the world's largest security company.

ENCRYPTION SOLUTIONS

Certified by leading independent authorities (Common Criteria, FIPS and NATO), Senetas hardware and virtualised encryption solutions leverage end-to-end encryption and state-of-the-art key management to provide long-term data protection without compromising network performance or user experience.

ANTI-MALWARE SOLUTIONS

Votiro Cloud leverages patented content disarm and reconstruction (CDR) technology to provide proactive protection against the most persistent cyberattacks, including unknown or zero-day exploits. Votiro is a subsidiary of Senetas and prevents malicious content and malware attacks via email, web and other high-risk file gateways.

COLLABORATION SOLUTIONS

SureDrop is the secure file-sharing and collaboration application with 100% data sovereignty control. It provides the information security and data sovereignty control essential in a world dominated by remote working. SureDrop has the usability of box-type file-sharing and collaboration tools, but with the added benefits of best-in-class encryption security and Microsoft 365, Active Directory and Azure integration.

Contact Senetas

Senetas Global

312 Kings Way, South Melbourne, VIC 3205 Australia

T: +61 (0)3 9868 4555 **E:** info@senetas.com

Regional Contacts:

Asia Pacific	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** infoemea@senetas.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

SENETAS