27 August 2021

Strengthening Australia's cyber security regulations and incentives

The National Retail Association welcomes the opportunity to make a submission to the Australian Government on strengthening Australia's cyber security regulations and incentives.

About the National Retail Association

The National Retail Association (NRA) is Australia's most representative retail industry organisation, servicing more than 39,000 retail and fast-food outlets nationwide.

Our members cover all types of retail including fast food, cafes, restaurants, fashion, groceries, department stores, household goods, hardware, auto, and services. Our membership includes the majority of national retail chains and thousands of small businesses, independent retailers, franchisees and other service sector employers.

The NRA helps retail businesses succeed and grow within an ever-changing regulatory environment. Our role is to influence government policy towards more commercially-aware outcomes and keep public debate focused on important issues that retail businesses face.

National Retail Association Technical Standards Committee

The NRA Technical Standards Committee is a group of quality assurance and product compliance specialists who come together from many of Australia's retail businesses to discuss the challenges of product safety and compliance.

The Committee is an important forum for the development of retail industry policy. It communicates regularly, on behalf of the industry, with government decision-makers and agencies, including Standards Australia, the ACCC, offices of Fair Trading and Consumer Affairs, the National Measurement Institute and others, conveying the issues and concerns of the retail sector.

Introduction

We understand that the Government is seeking feedback in three key areas:

- Clear minimum expectations - mandatory or voluntary cyber security standards for corporate governance, smart devices and personal information.
- Transparency – security labelling for smart devices, health checks for small businesses and improved disclosure of software vulnerabilities.
- Consumer rights – clear legal remedies for victims.

We submit that any outcome needs to be understandable, actionable, and simple.

Mandatory product standards

On 3 September 2020, the Australian Government released the voluntary Code of Practice: Securing the Internet of Things for Consumers (Code of Practice), listing 13 key principles. The Code of Practice prioritises action on default passwords, vulnerability disclosure and security updates as these principles will bring the largest security benefits in the short term. The National Retail Association supports the Code of Practice but questions whether there has been a sufficient amount of time from publication to assess its uptake and allowed for industry to self-regulate before mandatory product standards are required.

If mandatory product standards for smart devices are pursued, there are a number of considerations to be made.

1. Clearly outline which elements of the standards apply to the software (i.e., apps) and which apply to the hardware (i.e., chip sets)
2. Will there be requirements in relation to terms and conditions?
3. International alignment wherever possible is essential. We submit that the European Telecommunication Standards Institute (ETSI) baseline standard on smart devices (ETSI EN 303 645) is the preferred industry standard.
4. Voluntary removal of non-compliant product should be supported for both online and bricks-and-mortar retail
5. Costs – further consultation should be undertaken by the Australian Government to understand costs and ensure regulation applies to all businesses, regardless of size or category, to ensure a level playing field.
6. Range of unintended consequences, including increased e-waste with "obsolescence" of hardware and promoting consumer mindset of excess consumption.

The National Retail Association will be open to providing ongoing consultation throughout any mandatory product standards development.

Labelling for smart devices

Option 1 – Voluntary star rating label

We understand that labelling schemes can be effective in changing consumer behaviour, and are widely used in Australia for nutritional information and energy, water and fuel efficiency. Whilst a cyber security star rating system would be intuitive and support consumer understanding, there are a number of valid issues that will detract from any net security benefit.

Foremost, the cyber security star rating system criteria will not be static thus failing to create a functional comparative tool. A criteria definition of a 'five-star' smart device will fluctuate over its lifetime as technology and cyber security capabilities advance and cyber security threats adapt and become more sophisticated. This fails to create a useful decision-making tool for consumers to compare between smart device brands, models and newer and older releases and essentially makes a star rating redundant within a short timeframe. Updates will need to be constantly made to ensure the rating remains current over the lifetime of a product, only decreasing consumer clarity and increasing administrative burden and costs on businesses.

Option 2 – Mandatory expiry date label

Our members have expressed reservations regarding a mandatory expiry date label.

Firstly, it is difficult to predict an accurate expiration date, especially considering that software may need improvements prior to the expiry date.

Secondly, expiry dates will likely see an increased turnover of hardware as devices become "obsolete," in turn promoting excess consumption and e-waste production. Clear labelling or consumer education is needed to ensure the expiry date is not misconstrued as a device replacement date.

Mandatory labelling scheme for mobile phones (Q20)

The National Retail Association submits that any regulation should be applied fairly across all players, to ensure a level playing field. As such, all devices should be included in the mandatory labelling scheme. However, we note that there may be resistance from some international brand suppliers.

Digital and physical labelling for manufacturers (Q21)

Digital labels represent a lower cost and can be 'permanently' attached to the device, but not necessarily visible at point of sale. We note that physical labelling may assist customers at the time of purchase, but will not likely provide any long-term benefits as information on product packaging is lost once packaging is disposed of.

Voluntary health check for small businesses

The National Retail Association submits that small businesses selling IoT devices should have to abide by the same rules as all other businesses to ensure a level playing field. If a business is selling and profiting from the sales of a smart device, a proportional investment into cyber security measures should be made.

Clear legal remedies for consumers

We note that the Australian Consumer Law (ACL) does not prevent the import of defective products.

We also suggest that the bulk of Australian Government focus should be dedicated to law enforcement to pursue offenders of cyber-attacks with one member giving an analogy of prosecuting a window manufacturer because a thief broke into a house and not pursuing or prosecuting the thief.

Thank you for this opportunity to provide our submission on behalf of the retail industry and our members. Should you have any queries, I can be contacted on [redacted] or [redacted].

Yours sincerely,

[redacted]

David Stout
Director Policy
National Retail Association

Ph: [redacted]
E: [redacted]