AADA
AUSTRALIAN AUTOMOTIVE DEALER ASSOCIATION

Committee Secretary
Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations
PO Box 6021
Parliament House
Canberra ACT 2600

Date: 4 September 2026

E : cssmbo.reps@aph.gov.au

AADA Response to the Inquiry into cyber security for small to medium sized businesses and organisations.

The Australian Automotive Dealer Association (AADA) welcomes the opportunity to respond to the Inquiry into cyber security for small to medium sized businesses and organisations.

The AADA is the peak industry advocacy body exclusively representing franchised new car and truck dealers in Australia. There are more than 3,900 car and truck dealerships across the country, ranging from family-owned small businesses to large publicly owned businesses operating in regional areas and capital cities. The new vehicle retailing sector employs more than 64,000 people, including approximately 7,500 apprentices, contributes more than $21.5 billion to the national economy, has total turnover of $91.3 billion and generates more than $8.2 billion in tax and duty revenue.

The automotive retail sector provides a useful example of the cyber security challenges faced by small and medium sized businesses which operate within increasingly interconnected digital environments and are reliant on systems, platforms and requirements established by significantly larger organisations.

While franchised new car dealers are proactive and responsible for the maintenance of appropriate cyber security practices within their own businesses, their ability to manage cyber risk cannot be considered in isolation from the broader networks in which they operate. Franchised dealers interact with vehicle manufacturers, financiers, insurers, government agencies and technology providers and rely on a range of digital systems to undertake essential business activities, including ordering stock, processing transactions, arranging finance, communicating with customers and managing vehicle sales and servicing.

In many cases, the systems used to perform these functions are provided or controlled by other organisations. Vehicle manufacturers may require dealers to use particular platforms or software, while other systems are operated by third-party providers endorsed or selected by the manufacturer. This can create a high degree of digital dependency and means that the cyber resilience of an individual dealership can be affected by systems and decisions beyond its direct control.

Against this background, the AADA considers that there are a number of issues which should be taken into account when considering how Government can most effectively improve the cyber security preparedness of small and medium-sized businesses.

Proportionate cyber security requirements

The resources and technical capability available to businesses vary considerably, including within the franchised automotive sector. While larger dealer groups may have dedicated information technology and cyber security resources, smaller dealerships may rely on general IT staff or external providers and can face significant costs in obtaining specialist cyber security expertise.

Any minimum standards, regulatory requirements or other measures developed for small and medium-sized businesses should therefore be proportionate to the size, risk profile and capability of the business. They should also recognise the extent to which the business can practically control the relevant risk associated with particular activities.

This is particularly important where cyber security requirements are imposed through multiple channels. Dealers may be subject to Government requirements as well as standards, systems and processes required by vehicle manufacturers, financiers, insurers and technology providers. Government should seek to avoid unnecessary duplication or the development of additional prescriptive requirements where existing obligations or practical guidance can achieve the same objective.

Government guidance should be clear, consolidated and capable of being implemented by businesses without specialist cyber security expertise. Practical tools, templates and training resources which assist businesses to identify common risks and establish appropriate baseline protections are likely to be more useful to smaller dealerships than complex or highly technical compliance frameworks.

Cyber security within supply chains

The AADA particularly welcomes the Committee's consideration of the relationship and participation in large corporate and Government supply chains in the context of cybersecurity preparedness, as this is an important issue for franchised dealers. Although franchised dealers are independent businesses, they operate within networks involving multinational vehicle manufacturers and other large organisations and may be required to use systems or technology determined by those organisations. As a result, a dealer may maintain appropriate protections for its own systems while remaining exposed to a cyber incident affecting a system operated elsewhere in the network.

The AADA has previously observed the consequences of this dependency. Over the past few years there have been a number of examples where a cyber-attack resulted in systems operated and managed by a manufacturer becoming unavailable to franchisees, disrupting essential business processes across areas including financial services, direct debit arrangements and dealer email communications.

The experience demonstrates why cyber security responsibility within a corporate supply chain should reflect the practical ability of each party to control and manage the relevant risk. Consideration should be given to which organisation selects and controls the relevant

system, establishes its security requirements, determines how information is collected and shared, has the technical capability to identify and address vulnerabilities, and is able to restore or remediate the system following an incident.

Dealers should be expected to maintain appropriate cyber security practices for the systems and activities within their control. However, where a dealer is required to use a system selected, provided or controlled by another organisation, it may have limited ability to assess its underlying security or address vulnerabilities within it. Cyber security policy and standards should recognise this distinction and avoid transferring disproportionate responsibility or cost to smaller businesses for risks which they have limited capacity to manage.

Similarly, where larger organisations require dealers to adopt particular cyber security standards as a condition of participating in their networks, those requirements should be proportionate and supported by appropriate technical guidance, training and implementation assistance.

Communication and support following a cyber incident

The interconnected nature of these systems also raises important questions about communication following a cyber incident. Where an incident affecting a manufacturer, technology provider or other organisation has the potential to affect connected dealerships, dealers need timely information to determine whether their systems, business operations or customer information may be affected and what action they should take.

The AADA's experience following manufacturer cyber incidents highlighted the difficulties which can arise when businesses are dependent on another organisation for this information. While investigating the nature and extent of a cyber incident necessarily takes time, affected or potentially affected dealers need sufficient information to protect their businesses and customers and, where necessary, establish alternative arrangements to continue trading.

The AADA considers there would be value in Government guidance establishing clearer expectations for larger organisations following cyber incidents that have potential downstream impacts on small and medium-sized businesses. At a minimum, connected businesses should be promptly advised of an incident which may affect them, provided with available information about potential impacts and immediate protective measures, given a clear avenue through which to obtain assistance, and kept informed as the incident is investigated and resolved.

These expectations should apply even where the full extent of an incident is not immediately known. For example, early notification that an incident has occurred, accompanied by appropriate qualification about what remains under investigation, may allow connected businesses to take precautionary action rather than waiting until a complete assessment has been undertaken.

Skills, training and access to support

The availability and affordability of cyber security expertise is also relevant to the ability of smaller dealerships to improve their cyber resilience. Maintaining specialist capability

internally will not be practical for every business, particularly smaller and regional dealerships, and many will continue to rely on external providers for technical support. Government initiatives should therefore focus not only on increasing the supply of specialist cyber security skills but also on making those skills and services more accessible to smaller businesses. Consideration could be given to practical mechanisms which help businesses assess the quality of external cyber security providers and identify the level of support appropriate to their risk profile.

There is also an important role for workforce training which can be delivered without requiring specialist technical knowledge. Resources addressing common risks such as phishing, fraudulent communications and appropriate handling of information should be practical, regularly updated and capable of being incorporated into ordinary workplace training.

Conclusion

The experience of franchised new car dealers demonstrates that improving the cyber resilience of small and medium-sized businesses requires more than considering the security practices of individual businesses in isolation. Increasing digital integration within supply chains means that smaller businesses can be exposed to risks arising from systems and platforms controlled by significantly larger organisations, while at the same time facing increasing expectations regarding their own cyber security capability.

In responding to these challenges, the AADA encourages the Committee to consider the need for proportionate and practical cyber security requirements; clearer and more accessible Government guidance and training, improved access to appropriate cyber security expertise, avoidance of unnecessary duplication between regulatory and commercial requirements, appropriate allocation of responsibility across digital supply chains, and clearer expectations regarding communication and support where a cyber incident affecting a larger organisation has downstream impacts on smaller businesses.

These measures would provide a more practical basis for strengthening cyber resilience while recognising the different capabilities of businesses and the increasingly interconnected environments in which small and medium-sized franchised dealers operate.

Yours Sincerely,

James Voortman
Chief Executive Officer
jvoortman@aada.asn.au