Introduction

As cyber threats continue to grow in complexity and scale, protecting the cybersecurity posture of small and medium businesses (SMBs) and not-for-profit organisations (NFPs) has become a critical national priority for Australia. These sectors often operate with limited resources and expertise, making them particularly vulnerable to cyber incidents, including ransomware, data breaches, and identity crimes. Government efforts to raise cyber awareness, promote uptake of protective resources, and foster collaboration between industry and the public sector are essential to strengthening national cyber resilience. This response outlines key strategies for improving targeted cyber awareness campaigns, scaling successful programs, encouraging resource adoption, addressing sector-specific challenges, and aligning domestic efforts with international best practices.

Discussion Items

Effective targeting and consolidation of governmental cyber awareness messaging requires developing a unified national framework that harmonises communications across all relevant agencies. Tailoring messages for diverse audiences, including SMBs, NFPs, and individuals, by segmenting communications based on sector risk profiles, ensures greater relevance and efficacy. Utilising plain language focused on actionable advice and disseminating it through multiple channels, such as social media, webinars, and community outreach, enhances engagement. Partnering with trusted entities, such as industry groups, educational institutions, and community leaders, further extends the message's reach and credibility. Feedback loops and iterative messaging updates ensure that communication remains current and responsive to threats. The United Kingdom's National Cyber Security Centre (NCSC) and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) provide robust models for sector-specific outreach and trusted partnerships that Australia can emulate.

Australia's existing initiatives, such as the Australian Cyber Security Centre's Small Business Cyber Security Guide and the Cyber Wardens program, have demonstrated success in raising foundational awareness and building capacity. However, scaling these efforts, particularly through integration with education systems, remains essential. Introducing comprehensive cybersecurity curricula within schools and vocational training, along with partnerships among government, industry, and education, will foster workforce readiness and community resilience from an early stage. Singapore’s Cybersecurity Lab @ School initiative demonstrates the effectiveness of integrating cyber awareness into education through active industry collaboration.

Adoption of government cybersecurity resources by SMBs and NFPs remains suboptimal. Simplifying access through a centralised and user-friendly portal that aggregates all relevant tools, guidance, and services would mitigate fragmentation and confusion. Wider promotion through chambers of commerce, professional bodies, and grant programs can raise awareness of available supports. Introducing financial incentives, certification schemes, and peer-led testimonials can motivate voluntary engagement. Embedding cybersecurity advice into broader business service offerings (e.g., accounting and legal advice) leverages trusted relationships to drive behaviour change. The United Kingdom’s Cyber Essentials certification scheme offers a practical framework for encouraging small businesses to adopt basic cybersecurity controls, which Australia may consider adapting.

Strong collaboration between industry and government is vital to increasing cybersecurity uptake in SMBs and NFPs. Establishing formal public-private partnerships with clearly delineated roles facilitates the co-development of resources, awareness campaigns, and mentorship programs whereby cybersecurity experts guide smaller organisations. Facilitating mechanisms for secure threat intelligence sharing enhance preparedness and response capabilities. The U.S. Multi-State Information Sharing and Analysis Centre (MS-ISAC) exemplifies how coordinated cybersecurity intelligence exchange can bolster the defence posture of community-level entities and small organisations.

Promoting the adoption of established cybersecurity standards such as the Australian Essential Eight mitigation strategies, ISO/IEC 27001, and the NIST Cybersecurity Framework is recommended. These internationally recognised frameworks provide structured approaches to managing risk but require translation into simplified, context-specific guidance for SMBs and NFPs to reduce barriers related to complexity and cost. The Cybersecurity Maturity Model Certification (CMMC), which is influencing U.S. government supply chains, offers a flexible model that could be adapted domestically to enhance maturity among smaller organisations.

The NFP sector faces unique challenges, including resource constraints, limited expertise, reliance on volunteers, and an often complex regulatory environment. Dedicated government support is critical to this sector's cyber resilience, including tailored guidance, access to subsidised cybersecurity tools and assessments, leadership training for board members, and funding programs. Encouragement of sector-specific collaborative networks aligns with international efforts such as the UK's Cyber Aware campaign, which provides customised support to NFPs.

Cyber insurance, while a vital risk mitigation tool, remains inaccessible or unaffordable for smaller entities due to high premiums, complex policies, and a lack of understanding. The government can play a role by facilitating public-private reinsurance arrangements to lower costs, educating organisations about insurance benefits and coverage, and encouraging insurers to develop targeted, SME-friendly products.

Ransomware is a significant and evolving threat, particularly affecting SMBs and NFPs through tactics such as ransomware-as-a-service and double extortion schemes. Government support could focus on subsidising cybersecurity hygiene measures, deploying rapid response teams to assist victims, and intensifying public awareness campaigns tailored to prevention and recovery. Canada's and the UK's ransomware task forces provide instructive models for cross-sector rapid response and intelligence sharing.

Specific vulnerable communities and sectors experience disproportionate impacts from cyber incidents because of technology disparities, training deficits, and socio-economic factors. Accessible, culturally sensitive training and cybersecurity resources tailored to these groups are needed to bridge gaps. Similarly, to enhance victim support for identity crime, given the rising demand, services should centralise reporting, promote seamless integration with law enforcement and financial institutions, offer multilingual access, and provide educational materials to aid prevention.

Regulatory frameworks such as Australia's Notifiable Data Breach scheme, the Security of Critical Infrastructure legislation, and the Privacy Act form a critical foundation for reducing cyber risk. However, the regulatory burden on smaller entities must be carefully managed through supportive programs to avoid inadvertently curtailing cyber maturity. Balanced

regulatory approaches observed internationally, combining enforceable mandates with capacity-building measures, serve as valuable references.

Adoption of secure technology standards can be accelerated through lessons drawn from the European Union's Cybersecurity Act, which introduces certification schemes for IoT and edge devices, and the U.S. NIST's guidelines for Operational Technology (OT). Germany's Trusted IoT Framework, emphasising hardware trust anchors and firmware security, offers additional insights relevant to Australia's critical energy resources and edge device environments. Layered defence and continuous monitoring are essential to protect these increasingly ubiquitous technologies.

To empower consumers, initiatives such as cybersecurity labelling schemes, which are emerging in the UK under "Secure by Design," can provide transparency around product security attributes and manufacturer update policies. This enables more informed decision-making and incentivises manufacturers to build security by default.

Managing foreign ownership and control risks in technology supply chains requires the development of comprehensive risk assessment frameworks that incorporate geopolitical considerations. Transparency requirements, continuous vendor risk monitoring, and collaborative information sharing should be formalised in partnership with industry to mitigate strategic vulnerabilities.

Regarding data governance, ongoing dialogue between the government and industry is necessary to map data flows and assess risk exposure across various economic sectors. Policies must strike a balance between innovation drivers and secure data sharing, leveraging privacy-enhancing technologies and secure multiparty computation frameworks. Harmonisation with international data transfer standards preserves competitiveness while protecting sensitive information.

Boosting innovation and economic prosperity requires trusted data sharing frameworks with robust governance mechanisms. Government-supported data trusts and incentives for adopting secure data handling practices facilitate responsible data exchange, preventing the exposure of intellectual property and exploitation. Cross-sector pilot programs help demonstrate practical benefits while managing risk.

Finally, the safe adoption of critical and emerging technologies necessitates early-stage government involvement in risk identification, development of best practice playbooks, certification support, and funding for secure design innovation. Promoting knowledge exchange across sectors ensures agility in responding to evolving threats.

Conclusion

Australia's cybersecurity resilience for SMBs and NFPs depends on a comprehensive, collaborative, and adaptive strategy informed by global best practices. A unified and audience-tailored cyber awareness framework, combined with scalable education and outreach programs, can enhance foundational knowledge and skills. Simplifying access to resources and incentivising their adoption, coupled with strong industry-government partnership models, fosters a protective ecosystem. Addressing unique challenges in the NFP sector and improving access to cyber insurance will reduce vulnerability. Learning from international standards for secure technology and emerging cyber threats such as ransomware enhances preparedness. Ultimately, a balanced approach to regulation, combined with innovative data governance

frameworks, will foster economic competitiveness and national security. These integrated efforts position Australia to meet the growing demands of a complex cyber threat environment and protect its vital economic and social sectors.

References

Australian Cyber Security Centre (ACSC). Essential Eight Strategies to Mitigate Cyber Security Incidents. Available at: https://www.cyber.gov.au/acsc/view-all-content/essential-eight

National Cyber Security Centre (NCSC), UK. Cyber Security Guidance for Small Businesses. Available at: https://www.ncsc.gov.uk/collection/small-business-guide

Cybersecurity and Infrastructure Security Agency (CISA), USA. Cybersecurity Awareness Resources. Available at: https://www.cisa.gov/cybersecurity-awareness-month

Cyber Security Agency of Singapore. Cybersecurity Lab @ School Program. Available at: https://www.csa.gov.sg/programmes/lab-school

UK Government. Cyber Essentials Scheme. Available at: https://www.cyberessentials.ncsc.gov.uk/

United States Multi-State Information Sharing and Analysis Center (MS-ISAC). Threat Intelligence Sharing Programs. Available at: https://www.cisecurity.org/ms-isac/

European Union Cybersecurity Act. Framework for Cybersecurity Certification of ICT Products. Available at: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-act-eu-framework-certification-cybersecurity-products-services-and-processes

National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Available at: https://www.nist.gov/cyberframework

UK National Cyber Security Centre. Ransomware Action Plan. Available at: https://www.ncsc.gov.uk/ransomware

Canada's National Cyber Security Strategy. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbrscrty-strtg/index-en.aspx

UK's Cyber Aware Campaign for Not-for-Profit Sector. Available at: https://www.ncsc.gov.uk/cyberaware/home

Germany's Trusted IoT Framework. Available at: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/IT-GrundschutzCatalogues/Recommendations/_node.html