CYBER SECURITY STRATEGY DISCUSSION PAPER

Kris Parris
[redacted]

1 April 2023

Prepared for the Australian Government
In reply to the request made by the Hon Minister for Home Affairs and Cyber Security through linkedIn, "we are in the process of formulating a new cyber security strategy and would appreciate input from individuals in the industry, cyber experts, academics, and the community."

EXECUTIVE SUMMARY

Small & medium businesses are the backbone of the Australian economy, contributing to economic growth and employment opportunities. However, these businesses are also vulnerable to cybersecurity attacks that can cause significant financial and reputational damage. In the context of national security, it is essential to understand the impact of cybersecurity breaches on small businesses and develop strategies to mitigate the risks.

Australian government can play a critical role in supporting small businesses in cybersecurity by providing resources and training on security best practices.

This cybersecurity strategy discussion paper aims to identify gaps in the existing government and sector cybersecurity strategies. The focus of this paper is addressing the challenges faced by small to medium-sized businesses (SMBs) lacking the necessary resources, expertise, or funding to implement robust cybersecurity measures in the cloud computing environment.

Consider a small medical practice that may lack the capability to maintain secure records. If they were to fall victim to a cyber-attack, the impact of a cybersecurity breach could result in the leakage of sensitive data, which would be devastating for the victims. It is my belief that the current cybersecurity strategy approach does not adequately support this type of business.

This paper recommends the development of a new cybersecurity framework that is flexible, scalable, and adaptable to meet the diverse needs of SMBs operating in the cloud computing environment. It also recommends providing funding and resources to SMBs to implement and maintain effective cybersecurity measures, conducting regular cybersecurity awareness campaigns and training programs, encouraging collaboration between government agencies, industry associations, and SMBs, and reviewing and updating the existing cybersecurity controls and guidelines.

The paper also emphasizes the importance of effective communication strategies in the event of a security incident. These strategies should be reviewed to ensure that

COMPLIANCE

While the Essential 8 maturity model was a commendable initiative, it is not suitable for the modern cloud computing environment. The majority of our customers operate in the cloud, rendering the model outdated. Though the ISM framework contains useful security guidelines, it fails to strike the appropriate balance for addressing the varied business models, particularly in the current SMB space.

RECOMMENDATIONS:

•Develop a new cybersecurity framework that is flexible, adaptable, and scalable to meet the diverse needs of SMBs operating in the cloud computing environment.

•Provide funding and resources to SMBs to implement and maintain effective cybersecurity measures, which can be achieved through grants, subsidies, and tax incentives.

•Maintaining a strong partnership with the business is important.

•Conduct regular cybersecurity awareness campaigns and training programs for SMBs to educate them on the latest cyber threats and best practices for mitigating them.

•Encourage collaboration between government agencies, industry associations, and SMBs to share threat intelligence, best practices, and cybersecurity resources.

•Develop a new Security Operation Centre for the shared use of SMBs subsidized by the government.

•Review and update the existing cybersecurity controls and guidelines to align with the modern computing environment and the needs of SMBs.

•To effectively manage cyber security incidents for SMBs, it is crucial to proactively provide assistance to these businesses. This involves promptly identifying, containing, and mitigating cyber security incidents that may occur, as well as developing effective response plans to minimize the impact of such incidents.

•The government should actively assist SMBs during a cyber security incident by providing guidance on how to resolve the issues, implementing mitigation controls, and coordinating an effective response. This can be achieved by offering incident response teams, providing access to cybersecurity experts and tools, and facilitating information sharing between government agencies, industry associations, and SMBs. By actively assisting SMBs during cyber security incidents, we can minimize the impact of cyber-attacks and help these businesses recover from such incidents quickly and effectively.

•Governments can encourage or mandate small businesses to have cybersecurity insurance to help them recover from a cyber-attack. Cybersecurity insurance policies can provide coverage for losses resulting from cyber-attacks, such as data breaches, network disruptions, and cyber extortion.

•In developing the new compliance model, it is essential to use simple language as much as possible. Since SMB are more focused on their business rather than cybersecurity, it is crucial that they understand the objective of the security requirements. The model should be designed to protect their assets and data, and therefore, it is necessary to communicate the security requirements in a clear and concise manner. By using simple language, we can ensure that the compliance model is accessible and understandable to all businesses, regardless of their technical expertise. This will promote compliance and help businesses to better protect their assets and data, which in turn will contribute to the overall security of the area. Therefore, the new compliance model should prioritize clear communication of security requirements in simple language to ensure that all businesses can easily understand and implement the necessary measures to protect their assets and data.

they align with the objectives of the organization and the victims of the cyber-attack. Additionally, it recommends the avoidance of assigning blame without concrete evidence, consulting the victims of the cyber-attack before making any public statements, and providing support to the affected organization, including assistance with recovery efforts and ensuring that they have the necessary resources to prevent future attacks.

Lastly, the paper highlights the importance of incorporating software development, coding, and cybersecurity into both early and ongoing education programs through developing age-appropriate curricula, providing training for teachers, partnering with industry leaders, providing funding and resources, and encouraging ongoing education opportunities.

COMMUNICATION

Following a security incident, effective communication is paramount in the realm of cyber security. Although there may be political benefits to blaming the affected organization, it is crucial to acknowledge that any organization is susceptible to such attacks. Therefore, it is imperative to consider the perspectives of all stakeholders, including the victims, prior to assigning blame. Furthermore, it should be noted that attributing blame to the impacted organization can have detrimental effects on its reputation, which is often a goal of hackers during cyber-attacks. Consequently, the communication strategy of the government should be thoroughly assessed, and external communication should be restricted to a "need to know" basis. This approach will assist the victims of the attack and instils confidence in the impacted organization to seek help from authorities without hesitation.

RECOMMENDATIONS:

•The government should review its communication strategy to ensure that it aligns with the objectives of the organization and the victims of the cyber-attack. This should include an assessment of who needs to know about the incident and what information should be communicated.

•The government/organizations should consult the victims of the cyber-attack before making any public statements or assigning blame. This will ensure that their perspectives are considered and that they are not further victimized by the incident.

•It is crucial to avoid assigning blame without concrete evidence, as this can damage the reputation of the organization and discourage other organizations from reporting similar incidents. The government should work with the affected organization to investigate the incident and gather evidence before assigning blame.

•The government should encourage organizations to report cyber incidents without fear of repercussions or negative publicity. This will help to identify and address vulnerabilities in the system and prevent future attacks.

•The government should provide support to the affected organization, including assistance with recovery efforts and ensuring that they have the necessary resources to prevent future attacks.

EDUCATION

In addition to existing online safety measures, it is advisable that the government incorporates software development, coding, and cybersecurity into both early education and ongoing education programs.

RECOMMENDATIONS:

The government can take several steps to incorporate software development, coding, and cybersecurity into early and ongoing education programs. This may include.

- developing age-appropriate curricula
- providing training for teachers
- partnering with industry leaders
- providing funding and resources
- encouraging ongoing education opportunities

EMPLOYEMENT

Recruiting young employees, particularly new graduates, is encouraged in today's computing environment, especially in the realm of cybersecurity, to achieve a balance that leverages new technology while safeguarding it. This approach helps to protect new technologies while also benefiting from the experience of senior staff.

RECOMMENDATIONS:

To implement a strategy of recruiting young employees, particularly new graduates, while maintaining a balance of experience and leveraging new technology in the field of cybersecurity,

•Government/organizations should establish clear job descriptions and requirements,

•develop partnerships with universities and technical schools,

•provide ongoing training and development opportunities,

•establish mentoring programs, encourage cross-generational collaboration,

•prioritize diversity and inclusion in recruitment efforts.

This approach helps to protect new technologies while also benefiting from the experience of senior staff.