Cautio

Your information security mate®

Contribution to the 2023-2030 Australian Cyber Security Strategy

15/04/2023

Phone	1300 152 129
Email	contact@cautio.com.au
Web	www.cautio.com.au
Address	Level 10, 440 Collins Street Melbourne, VIC 3000

Contents

What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030? 2

Introduction 2

Let's treat security the same way we did other sciences: 2

focus on the three pillars of capabilities: 3

The doers "People": 3

Let's get the Executives onboard: 4

Conclusion 4

What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

Introduction

Security is a rapidly evolving field that has reached a certain level of maturity and is now being used as a foundation for revolutionizing all industries. With the increasing number of cyber-attacks and the growing sophistication of cyber criminals, security has become a critical issue for individuals, businesses and governments alike. As a result, there has been a significant increase in investment in cybersecurity research and development, which has led to the creation of new technologies and tools that are designed to protect against cyber threats.

The evolution of security has been driven by the need to stay ahead of cyber criminals who are constantly developing new techniques and tools to bypass security measures. This has led to the development of new security technologies such as artificial intelligence (AI), machine learning (ML), blockchain and quantum computing.

To help Australia achieve its goal of becoming the most cyber secure nation by 2030, it is important to take several measures. These include **treating security as we would any other industry**, understanding that for security to work we need to **focus on the three pillars of any capability - "people, process, and technology"**, and lastly, we need **executives to understand that security is not about restrictions and constraints but rather an enabler**, and **it is not an IT issue**.

Let's treat security the same way we did other sciences:

Throughout the last century, we have witnessed the birth of multiple majors in universities such as medical and engineering. Both fields have contributed to the advancement of civilization and have gone through the process of growing to the point where they had multiple sub-majors. For example, medical has ENT, Cardiology, Dermatology, Neurology, and others while engineering has Civil, Mechanical, Electrical, Biomedical, and others. Therefore, it would be beneficial to treat security in the same way. We can start by introducing TAFE certificates and diplomas and then at a later stage create sub-majors in universities that cover the various domains of security. Although there is a big difference between security and other fields such as medical and engineering - one thing that comes to mind

is the frequency of update and innovation – but this should not prevent us from building a solid education structure and degrees that cover the main domains of security.

An initial proposal of certificates and courses would be:

- Governance, Risk, and Compliance (GRC)
- Data Security (which we refer to as Information security)
- Security Architecture
- Infrastructure Security
- Security Operations
- Threat Management
- DFIR
- And lastly, the part that is overlooked, Physical Security

The content for these sub-domains is readily accessible and there is no need to create anything new. To develop skilled resources that would enhance the industry progress in security, it would entail establishing certification III or IV courses and promoting them to the public. This way, prospective students who are interested can comprehend what to look for and pursue the required education to become proficient resources in the field of security.

focus on the three pillars of capabilities:

The industry is inundated with vendors and technologies that purport to solve all our security issues, but we have to be pragmatic. Some of these tools are impressive in their capabilities, but they are not panaceas. We need to inform businesses that they can attain some of their security objectives without investing excessive amounts of money in these technologies, and that there are other measures that mitigate risks besides technologies.

The doers “People”:

The first point about developing skilled resources mentioned in the “Let’s treat security the same way we did other sciences” section is part of the solution, another point we need to emphasize is informing the businesses that any new technology they acquire, they need a certain number of hours to operate it and make it achieve its objective, that means either allocating the responsibility to an existing available resource or hiring a new resource.

Let’s get the Executives onboard:

One of the common misunderstandings about the industry is that it is regarded as a subset of IT, you would be astonished how many times I came across a security GRC professional who was under the supervision of an Operation Manager, not only does this generate a potential clash of interests, but also confines the scope of security to IT only.

One of the ways to address this misconception is to reach out to executives and demonstrate to them how security is not an isolated function, but rather a collaborative one that works closely with other departments such as HR, Finance, Supply chain, Legal, and Business operation. This would help to ensure that security is placed in the most suitable position in the organizational structure, and that it receives the necessary support and authority to carry out its tasks effectively and successfully.

One of the effective ways to address this issue is to organize executive workshops on a regular basis, either in person or virtually, depending on the circumstances. This would help to spread this awareness among the executives and enrich their understanding about the industry and what it can and should do to improve the security posture of the organization.

Conclusion

This paper reflects what I perceive as the flaws in our industry, and what I would like to see implemented to help businesses flourish, and instead of imposing hefty fines in case of data breach, we can help them invest a small fraction of this fine to considerably enhance their vulnerability, risk, and ultimately security postures.