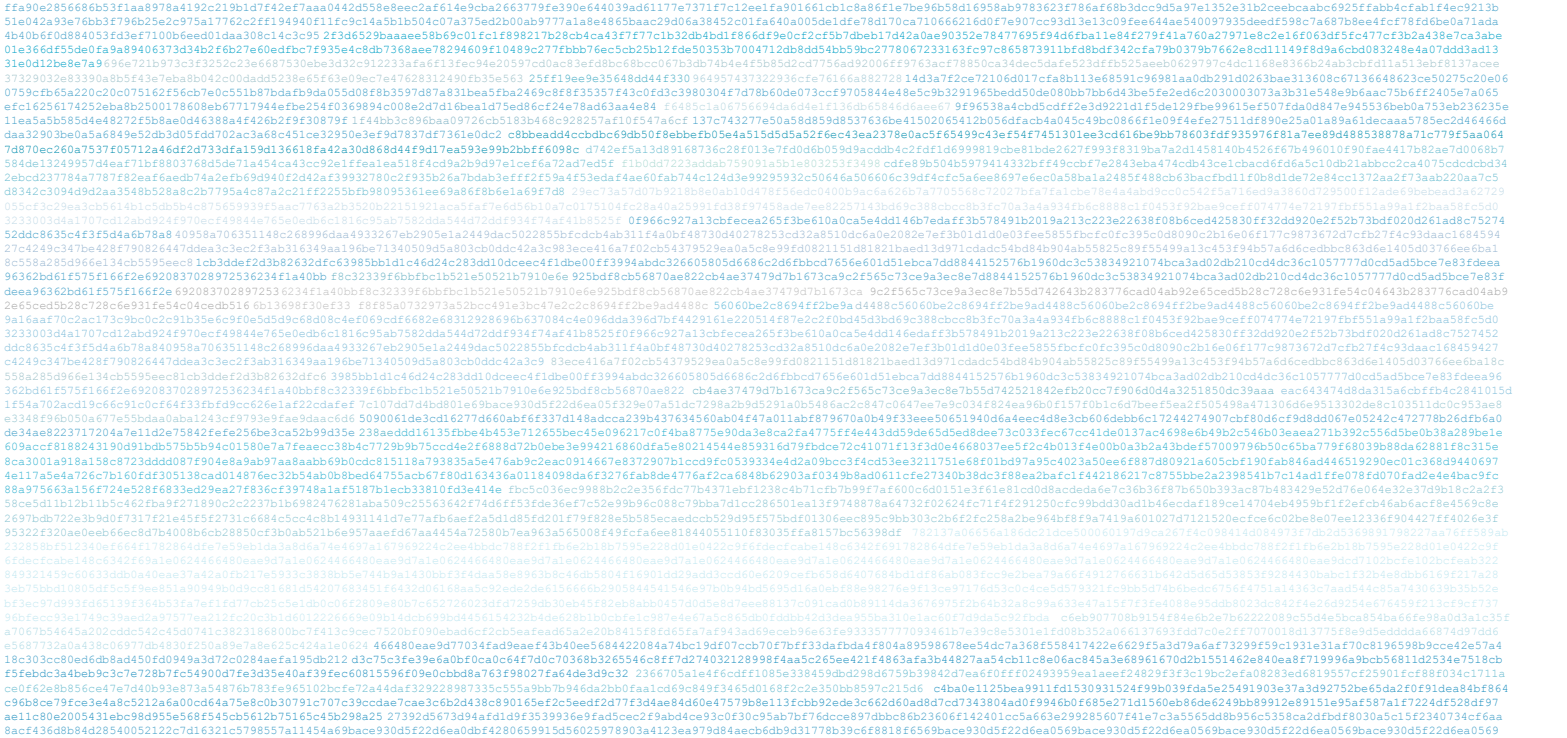
Australia's 2020 Cyber Security Strategy

What needs to be done so that cyber security is ‘built in’ to digital goods and services?



TERON LABS

Introduction

This response will address what needs to be done so that cyber security is built in to digital goods and services. We believe that cyber security can be built into digital products through the effective implementation of standards.

Standards and Cyber Security

The world of today is built on interconnected devices that communicate and operate using well defined, published standards.

These standards range from health and environmental protection standards to those concerning electrical, network and communication protocols. It is the continued development and proliferation of these standards that have allowed for technology to play an important role in our lives.

Traditionally, the two key motivations of standards are to promote interoperability and safety. Without proper interoperability, devices are unable to communicate; without safety, devices are unable to protect their users. Today, it is undisputed that security should also be a key goal in the development of standards.

The Role of Standards

The threats faced by the data that is stored and processed by digital products are not new. The increased connectivity of devices has only made these threats greater. Standards covering the tenets of data security (confidentiality, integrity, authenticity and non-repudiation) make data security accessible to all. The consensus and the public nature in which these standards are developed allow them to be rigorously examined and verified prior to their release. They allow for the democratisation of data protection.

Vendors, organisations and individuals can implement these standards with confidence as they are finalised and published. However, without a proper mechanism for validation, the implementations of these standards have to be taken at face value. This can result in poorly engineered products that advantage malicious actors.

Regardless of the testing that may have been undertaken by the creator of the product, without independent, third-party testing of the implementation of these standards, the security that is provided by a product cannot be guaranteed. This problem is exacerbated in critical infrastructure where a lack of oversight in the products that are utilised could pose catastrophic risks.

Assurance of Standards

It is possible for consumers to mitigate security threats introduced by potentially bad implementations of standards. One can perform a risk-based assessment which may result in mitigations being installed to offset potential risks. However, these assessments are subjective, non-standardised, non-repeatable, and at most times, superficial. Furthermore, the outcomes of these assessments cannot be verified by third-parties and must be taken, again, at face value.

In order to properly assess a digital product's implementation of standards, a well-defined approach must be taken. This allows for external parties to evaluate and validate the security of products in a standardised manner. Guarantees can also be built into the evaluation and

validation processes by setting up accreditation schemes to oversee and ensure their integrity.

A Global Approach

The problem of security assurance is one that needs to be addressed at a centralised level within government. We believe that it should be the responsibility of governments to demand minimum levels of security that are expected from products, especially those that secure critical infrastructure. Government already plays a large part in addressing the safety of food, transportation and medication. We believe that the security of digital products should not be treated any differently.

The European Union (EU) is currently at the forefront of this approach. The recently introduced EU Cybersecurity Act establishes an EU-wide cyber security certification framework for digital products. It helps the users of digital products understand the level of security assurance that products have undergone in order to help them make informed choices.

The approach taken by the EU builds upon current international standards and best practices. There are currently several international standards that help formalise the security assurance of digital products. We believe that Australia should be an active participant in the development of these standards. This will allow for our views to be heard on a global stage and help foster the development of a local industry that is skilled in this area. We are currently lacking in this sovereign capability and the greater involvement of Australia in the assurance of digital products will help in the development of this capability.

Our region is undergoing significant social, economic and political changes. Unless we are to support the growth of sovereign capabilities, we risk becoming dependent on other nations for our cyber security. Nations which have their own interests at heart. Therefore, it is imperative that we actively engage in the development of standards and practises that fosters local talent and expertise.

Conclusion

To lift the security of digital products to acceptable levels, we must follow the same standards-based, regulation-driven approach taken historically by the safety industry. We believe that an assurance-based approach should be used in ensuring the security of all digital products. The European Union is currently at the forefront of this approach. Australia should be an active participant in the development and promotion of standards that provide security assurance and foster the growth of the Australian product assurance sector. This will help us deliver a more secure digital landscape and promote the development of sovereign cyber security capability.