Oracle's Comments on Australia's 2020 Cyber Security Strategy

Oracle respectfully submits our comments, perspectives, and recommendations to the Australian Government to aid in drafting the 2020 Cyber Security Strategy. As a cloud computing company and number one provider of business software whose products underpin the essential services used every day, Oracle has a unique perspective that can help inform the Australian Government's update of its Cyber Security Strategy.

The cyber threat environment

This strategy refresh comes at a critical time. We operate today in an increasingly complex environment, defined by unprecedented connectivity across a number of devices and sensors on which we now rely. With this increased connectivity and explosion in computing capability, malicious actors of all types – nation states, cybercriminals, insiders, and hacktivists – have more opportunities and greater incentive to identify and exploit vulnerabilities, and employees have more opportunities to make mistakes. Cybercriminals, for example, are particularly challenging. They are becoming increasingly sophisticated and are using far more complex attack methods than previously seen. Telecommunications networks have become criminals' next frontier as they are relatively easy to access and were designed to address different risks and threats.

Oracle's role in securing customers

Industry plays a critical role in the cybersecurity of its customers. For Oracle, security is foundational to who we are, and as a result we provide the most secure products and services, developed and deployed with an emphasis on supply chain security. As a technology company, we see it as our responsibility to out-innovate malicious actors. We focused our research and development efforts on changing the fundamental economics of offense and defense, and found that the best way we can serve our customers is to move them to the cloud, where we can concentrate and scale our resources, expertise, and engineering on our customers' security. Our Generation 2 (Gen 2) cloud[1] uses its unique technical architecture and built-in autonomous capabilities to prevent, detect, respond to, and predict sophisticated security threats throughout the network. As customers move to the cloud, we are their partner, taking on shared management of cybersecurity risks. By default, our customers can leverage sophisticated layers of defense designed to secure users, applications, data and the infrastructure across multi-cloud environments.

Building-in security

Oracle believes that security should be addressed by products and services at all levels, a position informed by decades of experience in using strong product development and supply chain practices to integrate security throughout Oracle products and services. While a regulatory approach to enhancing cybersecurity in products and services may seem like a natural step to achieving immediate ends, we strongly recommend the Government first engage industry partners to understand current programs and practices. Outreach of this type will help provide specific details that can inform the Government's awareness of industry's varied security posture and maturity levels. We also recommend, based on that landscape, to consider how best to incentivize the market to differentiate on security. Government efforts should seek to further

[1] For information to which we refer our customers, please see: https://www.oracle.com/cloud/

incentivize companies with robust programs to continue their investment while also fostering faster gains among those companies that have less acceptable standards and practices.

For example, Oracle’s software security assurance program provides guidance and direction to development teams on how to best integrate security, and how to not unintentionally introduce vulnerabilities, throughout the development lifecycle. This program is built on industry standards and best practices, which are tuned by Oracle professionals steeped in security expertise.

In addition to a strong software security assurance program, Oracle invests in our supply chain program, ensuring that our products and services are secure throughout their lifecycle. Key aspects of this program include:

- Maintaining complete ownership of all hardware and firmware intellectual property;
- Requiring stringent security audits for all design releases;
- Contractually mandating that our suppliers follow and enforce specified security procedures and policies;
- Transmitting design data only via encrypted means;
- Maintaining control over the systems qualification tests and validation instead of the suppliers;
- Digitally signing all firmware and software.

Practices such as these vary across industry; government attempts to create a one-size-fits all approach is likely to create unintended effects of decreasing security investments for some while burdening others with poorly suited security controls that are not tuned to specific customer or industry requirements.

Instilling trust in ICT supply chains

Supply chains are increasingly complex, dependent on a global network of suppliers which require governments and companies to make complex risk mitigation decisions. There is no shortage of supply chain risk management efforts; however, the results have not been overly useful and have largely resulted in a collection of existing standards and best practices instead of providing any direction or mandate.

An improved approach to risk management is a framework-based model, like the one developed at the Prague 5G Security Conference where nations agreed to a set of recommendations for governments to consider as they design and deploy 5G systems. These Principles include recommendations on supply chain security for telecommunications infrastructure and networks, and managing the risks associated with vendors vulnerable to third country influence. Such a framework can move supply chain discussions beyond cataloguing standards and best practices. Further, it provides a standard that removes the burden of “proving” a company is untrusted by finding evidence of implants or backdoors.

5G opportunities

5G fundamentally changes the underlying telecommunications architecture by moving away from a monolithic core network dependent on proprietary hardware to one that is IT and cloud-centric, leveraging software defined networks and virtualization. With this shift, a whole new set of competitors can enter the market, in particular cloud and software companies like Oracle. Recognition of this new competitive landscape appears absent in many of the 5G supply chain and vendor ecosystem conversations. Governments should look to foster an environment where firms with a history of IT expertise can fairly compete as they deliver new 5G services to the market. We encourage Australia to work with partners and allies to support fair competition necessary to realize the full ecosystem of 5G vendors while holding to account those who are not competing fairly.

Cybersecurity workforce

There is a global shortage of a skilled, cybersecurity workforce. Oracle's research and development arm, Oracle Labs, maintains a research group in Australia. Unfortunately, this group has been directly affected by this workforce shortage, as they struggle to scale highly technical teams comprising Australians. They have turned to filling permanent positions and internships with candidates who received advanced degrees from institutions outside of Australia, which comes with additional costs such as those associated with relocation and obtaining visas, along with the delay in recruiting internationally. Further, we find that the Computer Science programs within Australia do not offer students relevant courses, so Oracle Labs Australia trains its engineering staff in-house when they join, and recruits researchers from overseas. Oracle collaborates with academics throughout the world, including in Australia. A large grant tied to cybersecurity and The University of Queensland, School of Information Technology and Electrical Engineering, supports research and teaching in areas that are important to Oracle Labs Australia. However, this does not appear to be a scalable approach to address the larger problem. Oracle remains interested in partnering with the Australian Government to identify current and future needed skills, and to assist in building a roadmap to achieve this needed technical workforce.

Artificial Intelligence and Machine Learning

With inexpensive computing power and mass quantities of data, the market is driving rapid advancements in artificial intelligence (AI) and machine learning (ML) technologies. While high profile efforts to create self-driving cars and autonomous drones capture headlines, the real impact of AI/ML will come from its ability to augment human decision making and productivity. This is particularly true in cybersecurity. Oracle integrates AI/ML throughout all of our products and at all levels of our Gen 2 cloud so that we can fully automate functions like patching, and threat detection and mitigation. The rapid adoption of these types of autonomous systems is how customers can shift the balance in favor of defenders instead of malicious actors.

Encryption

The security and confidence that modern encryption technologies provide drive the digital – and physical – economy, while also protecting vital national security interests. Modern encryption is rooted in intelligence, statecraft, and commerce, and it is a vital technology that underpins everything from the security of military and civilian communications to the cybersecurity of our critical infrastructure. However, it is also a tool that bad actors use to create spaces where governments are challenged – or are even unable – to gain lawful access. Current encryption technologies, deployment methods, and use cases, are constantly evolving and changing to meet business and user needs. It is appropriate and essential for industry to work with governments and law enforcement entities to find solutions to enable lawful access to these spaces.

Industry – Government collaboration

Government and industry collaboration on cybersecurity is critical. Industry has deep cybersecurity expertise to leverage, and we stay on the cutting edge of technology, actively integrating critical technologies, like AI/ML, to enable automated threat detection and mitigation. One important area of collaboration is information sharing, the focus of which has been on sharing specific threat intelligence, which should continue. In addition, Oracle recommends governments consider how to best leverage industry expertise, including through regular engagement in standards development and security organizations, as a way to scale and incorporate insight and perspectives from a broader set of industry participants. This scale is necessary to inform a broader perspective of the threat environment, which Government and industry can use to build next generation technologies and modernize business processes to address emerging cybersecurity concerns.

Internet infrastructure

Australia's Cyber Strategy should give consideration to the security and stability of the global internet infrastructure that enables not only our ability to communicate but also fuels commerce and security. As much of this infrastructure is privately owned and operated, industry engagement is critical to ensuring its security and resilience. Establishing shared situational awareness of the health and functioning of the Internet is critical to alerting to any deviations to the norm, and organizations like Oracle Internet Intelligence can make significant contributions to that shared baseline. Armed with this insight, Government and industry can take appropriate action to address malicious activities that might disrupt the normal function of the global internet.

Conclusion

We appreciate the opportunity to provide our insights and recommendations, and we stand ready to further discuss our responses to provide additional context or information.