Strengthening Australia's cyber security regulations and incentives

ISDEFENCE SUBMISSION - SUPPLY CHAIN RISK

Version	1.0
Date Created	Thursday, 26 August 2021
Last Review Date	Friday, 27 August 2021
Security Classification	FOUO
Prepared By	Rey Gomez, Peter Francisco

Introduction

ISDefence is the largest Independent Cyber Security and Business Resilience Consultancy based in South Australia, we service clients right across Australia.

Cyber Security regulations are becoming increasingly important as technology is advancing far greater than Australian laws or regulations. As such, ISDefence wanted to be part of the review process and have engaged in the group's discussions around the new incentives. Although the outcomes are some way off from becoming acted upon, we wanted to highlight the importance in third party / MSP / supply chain risks which we feel were not adequately addressed. This document summarises our thoughts at a high level for consideration.

Supply chain risk must be a key area of action for large businesses

Why take action?

Most organisations depend on business relationships to perform commercial activities. As such, the supply chain is now seamlessly integrated in the commercial operations of any business, from procurement to manufacturing and then warehousing, sales and transportation; each one of these components have their own subset of processes that could communicate directly with the company as part of a complex ecosystem. These relationships are critical in today's competitive world and any disruption could mean significant loss in terms of money, resources (staff and technical), commercial trades, reputation etc.

Recent cyber-incidents have disrupted thousands of businesses around the world and in Australia by performing *supply chain attacks*, where threat actors infiltrate third party software used by MSPs to perform regular IT operations to their clients [1] [2] [3] [4]. Likewise, supply chain attacks have been performed to exfiltrate information from target organisations by compromising channel accesses from a third-party provider. Furthermore, a 2020 study resulting from a survey of nearly 500 professionals across Australia and New Zealand reports that supply chain attacks are now over 50 per cent more likely than they were in 2016 [5].

> *Given the level of cybersecurity threats, companies not only should evaluate and elevate their own security controls, but also perform a very granular supply chain risk management from the information security perspective.*

Supply Chain Risk Management

Often, companies contract Managed Service Providers (MSP) to outsource the management and maintenance of IT services and resources within the organisation; MSPs may also provide a subset of services or products that the organisation offers.

Companies trust objectively that their MSPs are doing "the right thing" in regards of cyber security e.g., protecting remote access to the company systems and network devices, safeguard privileged credentials,

secure confidential information, and isolate critical environments from the corporate network, just to name a few among other security measures.

An organisation can be confident on its security controls in place to protect their information assets, but are its MSPs doing the same by protecting their access to different clients? Given the fact that MSPs are not required by any federal or local law to be compliant with any specific security framework such as NIST, ISO 27001, Australian Information Security Manual (ISM) or the recently updated Essential Eight, companies shouldn't be complacent and rely on assumptions.

Supply chain risk management is "*the implementation of strategies to manage both every day and exceptional risks along the supply chain based on continuous risk assessment with the objective of reducing vulnerability and ensuring continuity*" [6].

Possible Approaches

ISDefence recommends supply chain risk assessment be added as a key area of action within the new governance standards. Companies should be accountable for evaluating the standards and principles their MSPs have in place to manage information security; in addition, this evaluation should play a key role when selecting an MSPs in the first place.

Meanwhile, MSPs themselves should be more proactive in the adoption of security controls, such as the mitigation strategies from Essential Eight. Implementation of these mitigation strategies along with the inclusion of security controls detailed in standards such as ISO 27001/ 27002 and Australian ISM should provide a more reliable assurance for information security and business continuity.

Furthermore, a code of practice where MSPs are required by law to adopt a security assurance baseline should assist in the mitigation of supply chain attacks. This will not only help to regulate the market, but by ensuring that MSPs are being transparent and taking the necessary steps to mitigate cyber security incidents we can help to facilitate cyber security awareness across the supply chain.

References

[1] M. Mason, "Cyber agency confirms Australian firms hit by supply chain attack," 5 July 2021. [Online]. Available: https://www.afr.com/technology/cyber-agency-confirms-australian-firms-hit-by-supply-chain-attack-20210705-p586uq. [Accessed 27 August 2021].

[2] J. Becker, "Cyber attacks on rise as criminals target Australian agricultural supply chains," 4 June 2021. [Online]. Available: https://www.abc.net.au/news/rural/2021-06-04/cyber-attacks-on-rise-in-agriculture-industry/100188712. [Accessed 27 August 2021].

[3] D. Sadler, "Australian companies smashed by supplier cyber attacks," 8 April 2021. [Online]. Available: https://ia.acs.org.au/article/2021/australian-companies-smashed-by-supplier-cyber-attacks.html. [Accessed 27 August 2021].

[4] N. Morgan, "How cyber hackers are changing Australian agricultural supply chains," 20 July 2021. [Online]. Available: https://triskelelabs.com/how-cyber-hackers-are-changing-australian-agricultural-supply-chains/. [Accessed 27 August 2021].

[5] J. Doraisamy, "Supply chain attacks significantly more likely," 16 March 2021. [Online]. Available: https://www.lawyersweekly.com.au/corporate-counsel/30917-supply-chain-attacks-significantly-more-likely. [Accessed 27 August 2021].

[6] I. Heckmann, T. Comes and S. Nickel, "A Critical Review on Supply Chain Risk – Definition, Measure and Modeling".