Submission No 112

Inquiry into potential reforms of National Security Legislation

Organisation: Cisco Systems Australia Pty Limited

Parliamentary Joint Committee on Intelligence and Security

Cisco Australia

Response To

Australian Government Inquiry

into

Potential Reforms of National Security Legislation

20th August, 2012

Cisco Systems Australia Pty. Ltd.

20th August, 2012

Dear Secretary,

Reference: Chapter 3, Telecommunications Sector Security Review (TSSR), *'Equipping Australian Against Emerging and Evolving Threats'*, Attorney-General's Department, July 2012

In response to your request for information relating to the investigation being undertaken by the Australian Government as referenced above, Cisco provides this dot-point paper for your consideration. The paper outlines our perspective on the current trends, challenges, as well as opportunities, to enhance the security of the Telecommunication Carriers/Carriage Service Provider (C/CSP) environment, and can be considered a document for public release.

Cisco would support the Government discussion paper recommendations as outlined in the summary of this document, and highlight the following items:

- Reinforce the importance of looking at trustworthiness around all elements of a C/CSPs vendor choice, including international certifications like the Common Criteria, to address issues including supply chain risks, hardware and software vulnerabilities, and security risks to the confidentiality, integrity, and availability of telecommunications infrastructure.
- Reinforce the role of public-private partnerships using a 'trusted community' model between Government, C/CSPs, and Vendors (both product & services), in achieving a more secure national telecommunications infrastructure.
- The deepening of the public-private partnerships for increased information sharing may also enhance the concept of 'trustworthy systems' and 'multilayered network security', which would improve management of security outcomes for C/CSPs.
- The role of Government in placing greater emphasis on a Public-Private partnerships for security with C/CSPs may provide additional momentum in accelerating the introduction of identity-based services, combined with the other megatrends, to drive the market to a tipping point where security and new service generation paradigms are aligned.

Cisco would welcome the opportunity to provide the Parliamentary Joint Committee on Intelligence and Security further information as required.

Regards,

Signed

Richard Kitts
Vice President, Asia Pacific
ANZ Regional Manager
Cisco Systems Australia Pty Limited
Level 11, 80 Pacific Highway
North Sydney NSW 2060 Australia
Website: www.cisco.com

Australian Telecommunications - 2012 & Beyond

- As highlighted in the Australian Government's *'Equipping Australia against emerging and evolving threats'* discussion paper (p4) (herein known as the 'Government's discussion paper'), advances in technology and communications have resulted in unquestionable benefit to society and the economy, and this must continue to be a focus moving forward.
- Today, the average person undertakes multiple personal and work-related business tasks, often using the same device, where work is no longer a place they go, but rather an activity they undertake (i.e. location independent from their place of employment).
- The virtualization of data centres and the adoption of cloud-delivered IT services, along with Bring Your Own Device' (BYOD), Internet of Things (IoT), Collaboration technologies, and the introduction of IPv6, continue to increase the amount of material that can be accessed through the explosion in end-user devices, while accelerating the growth and increasing complexity of networks for Telecommunication Carriers/Carriage Service Providers (C/CSPs). Cisco's Visual Networking Index (VNI), which is now used as a de facto industry standard in Internet traffic projection, includes Australian forecasts through to 2015 and can be found at*:* *http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html#~Country*
- These trends are in turn driving change in the IT and security landscape, encouraging competition in technological and service innovation, while shifting the security model away from network perimeter-only defences, to a model that accounts for awareness of applications.

Challenges

- Given the rapid growth outlined above, several challenges are presented to C/CSPs that are looking for new opportunities to evolve their business and increase profits. These challenges include:
  - Networks are increasingly complex; particularly as legacy architectures are patched together in an attempt to deliver video-rich and mobile-capable services that may not have been part of their original design. As a result, many networks are just not optimized to handle the coming onslaught of traffic, devices, and content.
  - Complex conglomerations of legacy networks may remain and are unprepared for network convergence, not necessarily optimized for exponential growth of traffic, devices, content and services, while siloed networking and business paradigms impede services, access and profitability.
  - While it remains imperative for C/CSPs to closely examine their overall architecture, they need to review it beyond just the technical viewpoint, ensuring they are creating a business-centric architecture that is designed to meet their business needs and is capable of growing to suit their future goals. This architecture must include security as a key design paradigm, and must provide enhanced and differentiated services for customers.

- The National Broadband Network (NBN) aims to provide Australia with solutions to the following additional challenges:
  - Overcome the limitations associated with aging copper infrastructure and lagging broadband performance from other countries.
  - Prepare infrastructure for the future.
  - Provide services to the population.
  - Encourage economic growth.

C/CSP Vendor Environment

- If Australia is to fully realize the benefits of a NBN and the next wave of growth in the digital economy, then addressing security must become a high priority. The Australian government is looking for ways to mitigate threats by helping C/CSPs better understand and prevent attacks. Cisco would observe that C/CSPs spend significant resources to keep their networks secure and to continue to provide effective service for their customers. As a general matter, network defences need to be agile, flexible, and able to change with the constantly changing threat landscape. At the end of the day, driving innovation and security into the network is the best defence. Finally, robust public-private information sharing should be a centrepiece to achieving increased network security.
- As noted in the discussion paper, the trustworthiness of suppliers and network elements is a fundamental underpinning to a secure network. The use of international standards, like the Common Criteria for product assurance, cryptographic standards, and other emerging standards are useful to consider when addressing their (C/CSPs) vendor choice around supply chain risks, hardware and software vulnerabilities and/or security risks to the confidentiality, integrity and availability of telecommunications infrastructure, as such topics are discussed in the discussion paper (p32, last paragraph). While this is primarily mentioned in relationship to the TIA Act, it is also relevant to the TSSR in creating a ‘vendor trusted baseline’ for the C/CSPs. While no-one vendor is perfect, and flaws will be found, the processes and partnerships it uses to prevent, as well as address any post-product release shortfalls or risks, is a key element of becoming a trusted partner with the Government & C/CSPs.

Trustworthy Systems Concept

- The concept of ‘Trustworthy Systems and Products’ is key to achieving the Australian Government’s objectives and involves three parts:
  - A ‘trusted network baseline’ that underpins the ‘root of security’ which is based upon the security of the vendor’s hardware and software, and includes use of international standards like the Common Criteria for product assurance, active product testing for preventative, and post-product release testing and defect rectification;
  - A multilayered security capability that can evolve to meet both the existing and future evolutions of malicious software (malware), Advanced Persistent Threats (APTs) and other threat vectors. This would include multiple, flexible layers of defence designed to discover, destroy, and manage attacks through advanced technologies and comprehensive processes.

    - Creation of a ‘community of trust’ in a public-private partnership between key vendors, the C/CSPs, their customers, and the Australian government, to share vital information on threats and remediation.

- Today’s trustworthy systems must continue to evolve with the threat. To assure a trustworthy network and to maximize security, ‘trusted products’ must be a foundational priority in any public-private partnership, with four pillars, requiring a broad-based approach from product development, to delivery and support, and even disposal:
    - Secure hardware is engineered to be secure throughout the development process, with device identity and anti-counterfeiting measures incorporated.
    - Secure software is designed to resist attacks and is tested through methods like the international Common Criteria certification process. Together secure hardware and secure software help create a secure product.
    - Understanding your parts suppliers as an integral part of your supply chain, and how they combine to create your product, are critical factors in the secure development process. Supply chain issues are considered a major threat in some quarters today; according to industry estimates, approximately seven percent of product revenue is lost to counterfeiting, which produces inferior products, and will likely contain flaws and/or security risks. Buying from authorized distributors of a vendor’s product can help address this issue.
    - Independent certification, through methods like the Common Criteria, which is undertaken by governments and its authorized independent labs, including Australia, who are continually certifying Cisco products for use in Government architectures.
- In conjunction with the four pillars of Trusted Product, is the need for on-going product security testing. Cisco’s Product Security Incident Response Team (PSIRT) is focused on finding security flaws in our products, and feeding those findings to our Business units, and ultimately with customers, to create any patches to address security flaws. This on-going process is part of the continuing evolution of our ‘trusted product’ process.
- Cisco is widely recognized as a security leader committed to protecting its users and sharing best practices for security. As IT organizations move into the future of trustworthy computing, Cisco will continue to invest in the development of a comprehensive framework for security that constantly evolves to meet current and future threats.
- Cisco can provide guidance to the Australian Government to reduce hardware vulnerabilities, misconfiguration, external and internal hacking. As a vendor Cisco has been providing this same guidance to many countries including the Australian government.

Evolving Threats & Multi-Layered Security

- Cyber threats are evolving; as the industry mitigates old threats, new threats emerge and adapt to find new vulnerabilities. Malware has advanced to a state in which it can hide from many host-based services which rely on ‘signature-based' protections. In an environment where malware is changing shape and evading classic detection techniques, a multilayered approach to security — one that utilizes an advanced collection of tools such as reputation and behaviour analysis — is required.

- Cisco’s Security Intelligence Operations (SIO) dynamically collects threat information through a real-time global threat-monitoring network that is comprised of over 1.6 million Cisco security devices. These data sources span intrusion prevention systems (IPS), email security, web security, firewall devices, a historical threat database, and third-party threat intelligence feeds. Cisco SIO analyses and develops global, real-time threat data and incorporates it back into the security devices that ultimately enforce policies and protect customer networks.
- Cisco’s SIO works with our Computer Security Incident Response Team (CSIRT) to track and disrupt security threats. Our CSIRT monitors Cisco’s networks 24x7 to gather threat intelligence to develop security patches. Cisco’s CSIRT provides these patches to any SensorBase subscribers, whether company, government agency, or organization. CSIRT provides a reliable and trusted single point of contact for reporting computer security incidents worldwide. Cisco passes traffic information onto CSIRT so that once the threat is known and the vulnerability is patched, other systems can be searched and secured.
- An important increasing trend is the introduction of identity-based services that support the metadata identification of devices and entities in using the network, while providing additional metadata around network flows that support identification of security issues. Importantly, this same capability will also drive future context-based services capabilities and is a key underpinning for BYOD and other megatrends.
- With this in mind, the market may be reaching a tipping point where, for example, the installation of identity-based services could reinforce both the future security, and service generation, paradigms – a win/win for C/CSPs where, along with the security services provided today, these additional services add to the top-line revenue generation opportunity. The role of Government in placing greater emphasis on a partnership for security with C/CSPs may provide additional momentum in accelerating the development of this trend.

Conclusion

- Cisco strongly supports the following Government discussion paper concepts:
  - Cisco would reinforce the importance of looking at trustworthiness around all elements of a C/CSPs vendor choice, including international certifications like the Common Criteria, to address issues including supply chain risks, hardware and software vulnerabilities and security risks to the confidentiality, integrity, and availability of telecommunications infrastructure. These topics are introduced in the discussion paper with respect to the TIA Act (p32). Not only is this important in relationship to the TIA Act, it is also a crucial underpinning in creating a ‘trusted vendor baseline’ for the C/CSPs.
  - Cisco would reinforce the role of public-private partnerships using a ‘trusted community’ model between Government, C/CSPs, and Vendors (both product and services), in achieving a more secure national telecommunications infrastructure. This would include public-private partnership activities such as:
    - The Government’s increased information sharing in helping ensure C/CSPs have an even deeper understanding of the threat environment.

        - Shared knowledge of, and focus on, security outcomes to inform telecommunications infrastructure design, acquisition, deployment and support decisions, thereby minimising disruptions to the build-out of new services and infrastructure, while maximising security outcomes.
        - Sharing best practices for network security and on-going and active information sharing for cyber threat management, to help C/CSPs more effectively secure their networks, and their customers' networks.
    - The deepening of the public-private partnerships for increased information sharing may also enhance the concept of 'trustworthy systems' and 'multilayered network security', which would improve management of security outcomes for C/CSPs.
- The introduction of identity-based services within a public-private partnership, combined with the other megatrends, may see the market reach a tipping point where the future security and service generation paradigms are aligned. The role of Government in placing greater emphasis on a partnership for security with C/CSPs may provide additional momentum in accelerating this development including the deployment of a 'security-as-a-service' model by C/CSPs as a future service offering differentiator.

Trademarks

Every effort has been made to identify trademark information in the accompanying text. However, this information may unintentionally have been omitted in referencing particular products. Product names that are not so noted may also be trademarks of their respective manufacturers.

Cisco is a registered trademark of Cisco Systems, Inc.

The Cisco logo is a registered trademark of Cisco Systems, Inc.