VIRGINIA ECONOMIC DEVELOPMENT PARTNERSHIP INTERNATIONAL TRADE

Virginia
ExportVirginia.org
BUSINESS WITHOUT BORDERS

Cyber Security Export Market: Australia

2014

Sponsored by the Virginia Economic Development Partnership's (VEDP)
Going Global Defense Initiative

George Mason University (School of Public Policy)

This study was prepared under contract with the Commonwealth of Virginia, with financial support from the Office of Economic Adjustment, Department of Defense. The content reflects the views of the Commonwealth of Virginia and does not necessarily reflect the views of the Office of Economic Adjustment.

Virginia loves Exports

CONTENTS

EXECUTIVE SUMMARY

- Australia provides United States (US) companies looking to export cyber security solutions an excellent, competitive opportunity. With benefits of similar business culture, legal entities, and language, it is no wonder that many US companies have successful branches and subsidiaries based throughout Australia.

- Defense spending is at approximately 2 percent of gross domestic product (GDP).

- The Australian cyber security market is a niche market that is growing for certain types of products and services. US cloud security companies can pursue this market. The development of the National Broadband Network in Australia, which is estimated to cost approximately $36 billion[1] also, provides myriad opportunities for US exporters because of the requirement to secure the fiber optic network. Mobility expansion also provides additional opportunities.

- The Australia-United States **Australia-United States Free Trade Agreement (AUSFTA),** provides a framework that has strengthened trade relations, economic integration across all sectors, and has provided greater incentive for US investments.[2]

- Australia is a member of the World Trade Organization (WTO) and bound by its basic rules and regulations. It is an observer to the WTO's Government Procurement Agreement. The agreement's principles emphasize transparency and non-discrimination against foreigners.

- Australia's economy is favorable with low unemployment, contained inflation, low debt, strong financial systems, and strong industrial demand. With a current shortage in labor, the services sector provides additional welcome solutions.

- Australia has the institutions to protect intellectual property and business rights.[3]

[1] (All figures in US$ unless otherwise specified)
[2] (Australia-United States Free Trade Agreement)
[3] (Export.gov)

CYBER SECURITY IN AUSTRALIA

TECHNOLOGY USE IN AUSTRALIA

Like all advanced countries, Australia relies on networked systems for a range of critical functions including communications, storage of intellectual property, energy, and air traffic control. It has a growing demand for newer technology deployments including bring your own devices to work and migration to cloud computing. The Australian government is investing $43 billion over a period of eight years to create a National Broadband Network.[4]

The internet contributes approximately $50 billion or 3.6 percent of GDP (2010) to Australia's economy.[5] Internet World Stats cites Australia as having the fifth highest level of Internet penetration globally as a proportion of the total population (90 percent penetration).[6] Mobility use grew 49 percent in 2012 with 49 percent of the adult population having a smart phone. In 2009–10, nearly all (99 percent), businesses with 200 or more employees had Internet access, while the proportion was 87 percent for businesses with 0–4 employees. Most businesses with 200 or more employees had a web presence (94 percent), while over a quarter (29 percent) of businesses with 0–4 employees had a web presence.[7]

The key to the growth demand for cyber security is the investment in internet, mobility, and cloud computing. All three of these technology advances create a need for cyber security products and services in Australia.

CYBER CRIME

Security company, Symantec estimated that cybercrime in Australia was worth $4.5 billion in 2012. The Cyber Security Operations Centre (CSOC) identified 1260 cyber security incidents with over 310 of these qualified as serious in 2011. In 2012, CSOC identified over 1250 cyber security incidents, of which over 470 were serious enough to warrant a CSOC response. More than 65 percent of intrusions observed by the CSOC are economically motivated. A recent Symantec report on Australian cybercrime[8] noted that the average cost per cybercrime was $187 in 2013 compared to $317 and that 46 percent of Australian adults have experienced cybercrime in the past 12 months. Increasing cybercrime is another reason why cyber security is in demand in Australia.

GOVERNMENT PROGRAMS AND INITIATIVES

The Australian government has identified cyber security as a priority issue for national security. It has a developed a Cyber Security Strategy which identifies and explains the objectives and planned action to protect the nation against cyber-criminal activities. Various ministries and government organizations have launched multiple programs and initiatives for this purpose at the government and civilian levels.

According to the Australian Cyber Security Strategy 2009 report, there are seven strategic priorities: developing threat awareness and response, changing civilian security culture, promoting public–private partnerships, securing government systems, pursing international engagement, creating an effective legal framework and building a skilled cyber workforce.[9]

[4] (Australian government's cyber security strategy, 2009)
[5] (Speech to the Defence Signals Directorate (DSD)." Cyber Security Conference. Australia. -2012/
[6] (Nielsen Online Ratings January 2012)
[7] (internetworldstats.com)
[8] (Symantec." Norton Report 2013)
[9] (Australia. Federal Govt. Cyber Security Strategy)

A lead agency in Australia for cyber security is the Attorney-General's Department that is responsible for policies. In addition, the inter-departmental cyber security committee, the Computer Emergency Readiness Team (CERT), the Cyber Security Operations Center (CSOC), the Australia Communications and Media Authority (ACMA) along with other bodies are some of the important organizations concerned with implementing cyber security programs and initiatives.

Defense and government agencies involved in cyber security include the following:

- » Australian Defence Force
- » Defence Intelligence Organisation
- » Defence Science and Technology Organisation
- » Australian Security Intelligence Organisation
- » Attorney-General's Department
- » Australian Federal Police.[10]

These agencies perform different roles. The Defence Science and Technology Organization's role is to investigate the application of key enabling technologies for computer security and aid in cyber warfare.[11] This Organization has an annual budget of approximately $440 million and a staff of around 2,600. The Australian Security Intelligence Organization, a cyber-investigations unit established in March 2011, focuses on response and intelligence regarding "state-sponsored cyber-attack."[12] The unit operates under the supervision of the First Assistant Director-General for Counter-Espionage and Interference.[13] These agencies are designed to create a hub for greater collaboration with the private sector, State and Territory governments and international partners to combat the full breadth of cyber threats. [14] Together, these agencies provide US-based cyber security companies an opportunity to do business.

CYBER SECURITY SPENDING

The Australian government initially (2008) allocated approximately $114 million (A$125.8) over a period of four years on cyber security initiatives. Since then, it has published its recent (2013) National Security Strategy to combat cyber security problems. Within this document is outlined a $1.31 billion (A$1.46 billion) expenditure on IT security. The budget also allocated funds to establish an Australian Cyber Security Center. Additional expenditures on information technology are included in the budget of which cyber security is a significant part. For example, around $8 million (A$8.4 million) is to be spent on border processing for customs and immigration offices in the country. The development of the National Broadband Network also provides opportunities for US exporters to sell their cyber security products and services.

- » Specific spending amounts on security measures for the 2013-2014 year are available here.

[10] (Australian Signals Directorate." CSOC.)
Department of Defence, Defending Australia in the Asia Pacific Century: Force 2030, Australia, 2009, p. 134.
[12] (Tom Espiner, "UK helps Australia's cyber-spy unit get to work", 2011.)
[13] (Senior Mgmt Organization Chart. Australian Government)
[14] (Cyber Security and Cyber Warfare. Center for Strategic and International Studies, 2013)

MARKET ACCESS

Australia offers similar language and business frameworks but there are cultural and market differences that cannot be overlooked. Working with local partners, agents, and distributors may assist with these issues especially on the onset of doing business. Due diligence in choosing agents or distributors are applicable to Australia as with all countries.

- More details related to exporting to Australia are available through the US Commercial Service's resources on Australia and from the Virginia Economic Development Partnership/'s International Trade resources.[15]

TRADE AGREEMENTS

The Australia-United States **Australia-United States Free Trade Agreement (AUSFTA)** provides a framework that has strengthened trade relations between the two countries and economic integration across all sectors. The free trade agreement provides US businesses with easier access to Australia's market[16]. While AUSFTA primarily addresses agriculture trade, goods, and services, there are also regulations that cover cyber security and information technology (IT). Key rules that apply to the cyber security market include:

- Duties on more than 97 per cent of US non-agricultural tariff lines became duty free from day one of the Agreement, with all trade in goods free of duty by 2015.
- A mutual recognition of qualifications in professional services. Problems with recognition of qualifications can be a major hindrance for the export of professional services.
- In telecommunications, there are commitments on market access and a solid framework for pro-competitive regulation, as well as a mechanism for continuing engagement.

As part of the AUFTA, there are no tariffs on software imports into Australia. However, a goods and services tax applies to imports.

GOVERNMENT PROCUREMENT AGREEMENT

While Australia is a member of the World Trade Organization (WTO) and bound by its basic rules and regulations, it has not committed to the WTO's Government Procurement Agreement. The agreement's principles emphasize transparency and non-discrimination against foreigners. However, Australia is an observer to this plurilateral Agreement on Government Procurement (GPA). Australia is also a participant to the World Trade Organization's Information Technology Agreement, which eliminates duties on several IT products.

DEFENSE TRADE

An advantage for US defense companies doing business with Australia is the revised treaty, *Defence Trade Controls Act 2012, which* commenced on 6 June 2013. The original agreement "*Treaty between the Government of Australia and the Government of the United States of America concerning Defense Trade Cooperation* (the Treaty) was enacted September 5, 2007. The Treaty is intended to improve the efficiency of eligible two-way transfers between Australia and the US, by facilitating the export of controlled goods without the need for an export license. However, some conditions must be met for US exporters to be eligible.

[15] (Export.gov/Australia)
[16] (Australia-United States Free Trade Agreement)

The Directorate of Defense Trade Controls (DDTC) a part of the US Department of State Defense manages and oversees all of these requirements. The Treaty Reference System (TRS) assists US exporters in confirming whether a facility is a member of the Australian Approved Communities (AC), and therefore eligible for export exemptions created by the Treaties.

Benefits under the Treaty Framework for Treaty eligible projects include reduced delivery time for new defense projects; permitting transfers within the Approved Community without further Australian or US approvals; a more efficient way for US companies to share technical data with the Australian Community without licenses; consistent compliance requirements across the Australian Community; and the avoidance of delays sometimes associated with the export licensing process.[17]

GOVERNMENT PROCUREMENT

Defense procurement in Australia is streamlined and structured. The Defence Procurement Policy Manual outlines all the important details of the procurement process including the cycle, requirements and other information.

- A portal for information on government tenders and contracts for cyber security can be accessed here.
- The government's procurement information system publishes procurement plans, multi-use lists and other opportunities.
- The Department of Finance's procurement page is another useful resource for detailed procurement information throughout Australia.
- Details on procurement policies and procedures in the Information and Communication Technology industry are available here. Also see 'Selling to the Australian Government'.
- Lead agencies for cyber security and related procurement information can be found here.
- Future government vision and plans related to national and cyber security are available from the Department of the Prime Minister and Cabinet.
- There are certain Mandatory Procurement Procedures and Contracting Procedures that should be followed in Australia for government contracts.

MARKET SIZE AND GROWTH

DEFENSE SPENDING

The Australian government's spending on defense is low compared with that of other developed countries. The 2012 defense expenditure was $24.2 billion and comprised 1.63 percent of gross domestic product (GDP) compared to that of the US in 2012 which was $645.7 billion and comprised 4.12 percent of GDP.

[17] (Defence Trade Controls Act 2012)

Tony Abbott, the new Australian Prime Minister has made political promises of bringing defense spending back to 2 percent of GDP in the future. The past 2013 -2014 defense budget reports a $1.31 billion (A$1.46 billion) expenditure on IT security.[18]

Table 1: Military Spending in Australia

Year	Military Spending (billion US$)
2008	24.8
2009	26.6
2010	27
2011	26.6
2012	25.6

Source: SIPRI Military expenditure database 2008-2012

CYBER SECURITY MARKET SIZE AND SECTORS

According to the US Commercial Service's report on Information Technology Services (2013) in Australia, the market size for IT services is estimated to be worth $1.14 billion in 2013 and expected to grow to $1.56 billion in 2014. Of this market, approximately $1.4 million is through imports from the United States in the year 2013. Import of IT services is also expected to increase in the coming years.

The Australian cyber security market is a niche market, which is growing for certain types of products and services. For example, there is considerable demand for cloud security. Overall, Australia has been slow to adopt cloud computing but as it embarks on the adoption process, the market is estimated to double in the next couple of years from its current value of approximately $1 billion[19]. Cloud security forms a significant part of this expenditure. Thus, US cloud security companies can pursue this market (as an example, see list of suppliers to the government for launch of its data center). The development of the National Broadband Network in Australia which is estimated to cost over $36 billion[20] also provides myriad opportunities for US exporters because of the requirement to secure the fiber optic network.

[18] (Attorney-General's Department, Australian Transaction Reports and Analysis Centre (AUSTRAC) 2013)

[19] (US Commercial Service, Information Technology Services, Australia, 2013)

[20] (All figures in US$ unless otherwise specified)

LEGAL ISSUES

Australia's legal and corporate frameworks are similar to the US making it easier to interpret and do business in than many other Asian countries [21] Tax considerations should also be examined and hiring a qualified tax accountant versed in Australian laws is highly recommended.

INTELLECTUAL PROPERTY RIGHTS

Property rights are secure and adequately enforced in Australia. To protect one's intellectual property (IP) rights it is recommended that the US company submit a patent application in Australia to protect the asset or file a single international application under the Patent Cooperation Treaty (PCT), administered by the World Intellectual Property Organization (WIPO). The PCT allows application for a patent in a number of countries at the same time, including Australia. For trademark protection, US companies have the two choices of applying for a trademark in Australia or applying to the Madrid Protocol, which, in many cases is a simpler and more cost effective option. The Madrid Protocol is a simplified process for international registration of trademarks. Its web site provides information on Australian IP rights and searchable IP rights database)[22].

- » More details on intellectual property laws pertaining to cyber security can be accessed here.

BUSINESS LAW

US based companies looking to establish a business in Australia may elect to register a subsidiary or branch of a foreign company. A foreign company operating through a branch must register with the Australian Securities and Investments Commission (ASIC).

If entering by acquiring an Australian business or property, one must go through an approval process with the Foreign Investment Review Board ("FIRB"). In the majority of industry sectors, smaller proposals are exempt from notification and larger proposals are approved unless judged contrary to the national interest.

- » For Australian import laws, please click here.

CYBER LAWS

The 2013 National Security Strategy drew information from a series of documents including the Defence White Paper, a 2011 and 2013 Independent Review of the Intelligence Community, and the Cyber Security Strategy (2009). Its goal is to develop plans that outline changes to strengthen the legal frameworks to ensure that enforcement agencies have the appropriate tools to fight terrorism and combat organized crime.

The government of Australia has amended the Commonwealth Criminal Act of 1995 to incorporate laws against cybercrime (Cybercrime Act 2001). More details are available here. The cyber security strategy developed by the government also contains rights and protections related to information technology. The Attorney-General's Department provides information related to all applicable laws. Other laws related to telecommunications, privacy, spam, surveillance, and intelligence also come under the legal framework applicable to cyber security.

[21] (Doing Business with Australia. Australian Embassy, 2013)
[22] (www.ipaustralia.gov.au)

POLITICAL ENVIRONMENT

The Commonwealth of Australia (Australia) is a politically stable country, which maintains strong political and economic ties with the US. The Australia-US Ministerial (AUSMIN) forms the basis of the strategic alliance to maintain peace and stability in the Asia-Pacific region. Australia has agreed to work closely with the United States (US) and the United Kingdom (UK) to fight cyber intrusions. This partnership agreement provides US based cyber security companies an advantage in doing business with Australia.

- » Details on the US-Australia political and defense relationship can be accessed from the following resource: Congressional Research Service report.

Australia's open market offers trade and investment opportunities with few restrictions on goods and services. Australia actively pursues bilateral trade agreements on a global basis that work toward lower tariff barriers, and boost integration into global supply chains. Australia also has partner ties with East Asia as this region accounts for more than 50 percent of the country's exports.[23] Australia is active in the World Trade Organization, (WTO), the Asia-Pacific Economic Cooperation, G20 and other trade organizations.

- » For travel to Australia to make or build business contacts, please refer to the Department of State's travel advisory portal for Australia.
- » There are many similarities between the US and Australian markets because of the use of a common language. But, there are cultural differences which exporters should pay attention to in order to increase their chances of success in the Australian market – Australian culture.

ECONOMIC ENVIRONMENT

Australia is the 19th largest economy in the world with a 2012, gross domestic product (GDP) of $1.542 trillion, unemployment at 5.2 percent and taxes comprising 32.3 percent of GDP. Although 75 percent of its work force is in the services sector, there is a current shortage of labor in this sector, according to the American Chamber of Commerce. Australia is home to 42 of the 2013 Forbes Global 2000 companies list which had a combined market value of $1.019 trillion, with $4.024 trillion in assets; generating $638.4 billion in revenues and $67.6 billion in profits.[24]

There is a large number of U.S. based companies having branches and subsidiaries throughout Australia. This creates the advantages of a large expatriate community and possible teaming arrangements for large contracts. Large government contracts are known to require products and services from multiple vendors to make up enterprise solutions in technology.

US based companies with presence in Australia include not only multinational companies but also large integrators such as Lockheed Martin, Northrup, SAIC, CSC, and Booz Allen Hamilton to name a few companies.

Risk factors to export to Australia include the impact of weak global growth and concurrent weaker growth in prices for the country's commodity exports. The recent depreciation of the Australian dollar will be beneficial to import prices, but weak external demand is estimated to minimize this benefit. Shifting

[23] (Country Intelligence Report, Australia.)
[24] (Forbes Global 2000 May 2013. All figures are consolidated and in US dollars.)

expectations on monetary policy and fiscal problems will ensure a weaker Australian dollar into the future.[25] Growth estimates have been lowered to 2.4 percent for 2013.[26]

PRIVATE SECTOR DEMAND

CYBER INCIDENTS AMONG AUSTRALIAN BUSINESSES: A MARKET FOR US EXPORTERS

According to the US Department of Homeland Security, Australian businesses spent an estimated $1.37 billion to $1.95 billion for the period from July 1, 2006 to June 30, 2007.[27] To better understand and develop a base line for computer security, Australia commissioned its first national survey (2009), the Australian Business Assessment of Computer User Security, (ABACUS) to study computer security incidents against businesses in Australia. Surveying 4000 companies ranging from small and medium-sized to large firms, the report had many findings. Key to understanding Australia's private sector requirements include the following:

- Virus or other malicious code was the number one security incident.
- A security incident had an average loss of $49,246 per business.[28]
- Large businesses reported having more comprehensive security measures, with nearly all reporting the use of one or more security tools and the use of one or more security policies.
- Most businesses dealt with incidents internally, with only eight percent reporting the most significant incident to police.

This report concluded that they know very little about the extent, or effects of computer security incidents due to a number of reasons including underreporting of computer security incidents and the definition of a breach or security incident.

US DEFENSE FIRMS IN AUSTRALIA: A STARTING POINT FOR NEW US EXPORTERS

The domestic Australian cyber security industry is entering into partnerships with US cyber security parties in order to gain technical and strategic insights into the domain.[29] Some details about the American companies doing business in Australia are as below.

- Raytheon Australia– "one of the main markets for Security Solutions is the Australian Intelligence Community (AIC), which includes civil and defence agencies."[30]
- Lockheed Martin's - Lockheed Martin opens a $10m cyber-security center in Australia.[31]
- SAIC - announced it has been awarded two contracts by the Australian Defence Materiel Organization - These single-award, prime contracts have a total contract value of AU $13.5 million (approximately US $12.5 million) over 49-months if all options are exercised.[32]

[25] (Country Intelligence Report, Australia. 10)
[26] (Country Intelligence Report, Australia. 5-7)
[27] (https://www.asdreports.com/news.asp?pr_id=502)
[28] (AIC Reports 102. 2013)
[29] (https://www.asdreports.com/news.asp?pr_id=502)
[30] (Raytheon Australia)
[31] (Investor Update: Lockheed Martin Opens A$10m Cyber-security Centre in Australia)
[32] (www.pcmag.com/article, 2013)

- Top 25 Virginia-based integrators all have offices in Australia.
- These US base companies provide the network and community to assist and grow successful cyber export business in Australia.

DEMAND IN THE AUSTRALIAN PRIVATE SECTOR

There are many industries in Australia that require cyber security services. These include financial institutions, telecommunications, media, mining, and others of national interest. The US Commercial Service report on Australia contends that the large banks in Australia spend almost $3 billion on information technology services including cyber security in a year.[33] This market is expected to grow. In leading democracies such as Australia, a considerable portion of the national infrastructure is managed by the private sector. This implies that along with government contracts, US exporters should not lose sight of the plentiful opportunities for exports to the private sector in Australia.

[33] (US Commercial Service, Information Technology Services, Australia 2013)

Table 2: Australia’s Cyber Security Market at a Glance

Strengths

- Strong political and defense relationship with the US
- Open and transparent market access
- Revised defense treaty with USA

Weaknesses

- Small defense budget

Opportunities

- Niche market for cyber security
- Cloud security, network security
- Partnerships with other US based companies
- Private sector opportunities

Threats

- Significant competition from other domestic and foreign companies

APPENDIX: USEFUL LINKS

US Export Controls

- International Traffic in Arms Regulations (ITAR) – U.S. Department of State
- Export Administration Regulations (EAR) – U.S. Department of Commerce
- Exporting from Virginia
- Australia Import Licenses

US Laws Governing International Business

- US Anti-corruption guide
- Corruption Map

US-Australia Political Relationship

- US-Australia Political Relations
- Congressional Research Service report

Australia Country Information

- Country Information
- Culture

Doing Business in Australia

- US Commercial Service

Intellectual Property Rights

- International Patents

Resources in Australia

- Australian Information Industry Association
- Internet Industry Association of Australia
- Australian Government Information Management Office
- National Broadband Network

REFERENCES

Aerospace & Defense in Australia. (2012). No. 0125-1002. MarketLine Industry Profile, 2012. Print.

American Chamber of Commerce in Australia. (2013). *American Chamber of Commerce in Australia*. Web. 03 Nov. 2013. http://www.amcham.com.au/vpLink.aspx?ID=1

Australia Defence & Security Report. (2013). Q3. Business Monitor International. Print.

Australia. Federal Govt. Cyber Security Strategy.(2009). Web. www.ag.gov.au.

Australian Signals Directorate.(2013). *CSOC*. N.p., n.d. Web. 10 Nov. 2013. http://www.asd.gov.au/infosec/csoc.htm.

Australian Government, Australian Institute of Criminology. (2013). ASIO *Senior Mgmt Organization Chart*.

Australian Government. (2013). Part 2: Expense Measures (Continued). Budget Measures 2013-14. Australian Government, 2013. Web. 03 Nov. 2013. http://www.budget.gov.au/2013-14/content/bp2/html/bp2_expense-23.htm.

Australia-United States Free Trade Agreement - Australian Government Department of Foreign Affairs and Trade. (2013) *Australia-United States Free Trade Agreement - Australian Government Department of Foreign Affairs and Trade*. N.p., n.d. Web. 03 Nov. 2013. https://www.dfat.gov.au/fta/ausfta/outcomes/01_overview.html

Bureau of Industry and Security. (2013). *Federal Register*. Web. 10 Nov. 2013. http://www.bis.doc.gov/index.php/forms-documents/doc_view/334-encryption-export-controls-75-fed-reg-36-482-june-25-2010.

Central Intelligence Agency. (2013). The World Factbook. Web. Retrieved on November 3, 2013 from https://www.cia.gov/library/publications/the-world-factbook/geos/as.html

Computer Security Incidents against Australian Businesses. (2010). Australian Government,, Sept. 2010. Web. http://www.aic.gov.au/documents/6/9/F/%7B69FC108B-D437-47E0-9C17-93B5DEFC8D96%7Dtandi399.pdf.

Country Intelligence: Report, Australia. (2013). Aug 1. IHS Global. Print.

Country Intelligence Report. (2013). Sept 5. IHS Global. Print.

CSO. (2013) *Despite $1.46b Furphy, 2013-14 Budget Offers Slim Pickings for Cyber Security*. May 16. Web. 03 Nov. 2013. http://www.cso.com.au/article/462015/despite_1_46b_furphy_2013-14_budget_offers_slim_pickings_cyber_security/

Cyber Security Strategy. (2009): n. p. Commonwealth of Australia. Web. http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

Defence Trade Controls Act 2012. (2013) Web. 10 Nov. 2013. http://www.austlii.edu.au/au/legis/cth/num_act/dtca2012207/

Defence Minister For. (2012) Speech to the Defence Signals Directorate (DSD). Cyber Security Conference. Canberra Australia, 23–24 October 2012 Speech. Web. http://www.minister.defence.gov.au/2012/10/24/minister-for-defence-speech-to-the-defence-signals-directorate-dsd-cyber-security-conference-2012/

Doing Business In Australia(2013). *Hall Chadwick*. Web. 10 Nov. 2013. http://www.hallchadwick.com.au/services/doing-business-in-australia.html.

Export.gov - Home. (2013). *Export.gov - Home*. Web. 10 Nov. 2013. http://export.gov/australia/

Guidebooks to Doing Business in Australia. *Guidebooks to Doing Business in Australia*. Web. 10 Nov. 2013. http://www.austrade.gov.au/Invest/Doing-business-in-Australia

Homeland Security Spending Is Expected to Increase at a CAGR of 10.60%during the Forecast Period. (2013). *Homeland Security Spending Is Expected to Increase at a CAGR of 10.60%* Web. 10 Nov. 2013. https://www.asdreports.com/news.asp?pr_id=502.

Lewis, James A., and Gotz Neuneck. (2013). *The Cyber Index, International Security Trends and Realities*. Rep. New York and Geneva: United Nations, 2013. Print.

Lockheed Martin (2013). *Investor Update: Lockheed Martin opens A$10m Cyber-security Centre in Australia*. Web. 10 Nov. 2013. http://www.austrade.gov.au/Invest/Investor-Updates/2013/1106-Lockheed-Martin-opens-A-10m-cyber-security-centre-in-Australia.

PCMag (2013). *Northrop Grumman Launches Cyber Defense Team.* Web. 10 Nov. 2013. Web. http://www.pcmag.com/article2/0,2817,2356575,00.asp.

Raytheon Australia (2013). *Raytheon Australia: Growing Raytheon's Cybersecurity Capabilities*. Web. 10 Nov. 2013. http://www.raytheon.com.au/newsroom/features_archive/growing_cybersecurity/index.html.

Richards, Kelley. (2009) AIC Reports 102. The Australian Assessment of Computer User Security: A National Survey. *Australian Government*. Australian Institute of Criminology. Web. Oct.-Nov. 2013. http://www.aic.gov.au/documents/3/B/3/%7B3B3117DE-635A-4A0D-B1D3-FB1005D53832%7Drpp102.pdf.

Symantec. (2013). Norton Report: Total Cost of Cybercrime in Australia Amounts to AU$1.06 Billion. *Symantec*. Web. Retrieved on November 10, 2013 from http://www.symantec.com/en/au/about/news/release/article.jsp?prid=20131015_01

Thales in Cybersecurity Partnership; New Cybercenter in Australia.(2013). *UPI*., 3 Oct. 2013. Web. Retrieved on November 3, 2013 from http://www.upi.com/Business_News/Security-Industry/2013/10/03/Thales-in-cybersecurity-partnership-new-cybercenter-in-Australia/UPI-51001380815771/

Trade Services (2013). Doing Business with Australia. *Australian Embassy*, Web. 03 Nov. 2013. http://www.austrade.gov.au/Invest/Doing-business-in-Australia