Australian Government
Australian Trade and Investment Commission

Australia UNLIMITED

CYBER SECURITY

US CLUSTERS

TABLE OF CONTENTS

INTRODUCTION

The United States is recognised as a global leader in cyber security, with a culture of innovation and a federal government focussed on building secure networks for government, private enterprise and users.

Australia and the US have a strong allied history and a shared commitment to addressing cyber security. For Australian companies working in this sector, the US is an excellent location to explore business development, investment, and strategic partnership opportunities.

This report provides an overview of the US cyber security industry. It covers the established clusters in the San Francisco Bay Area, DMV (Washington D.C., Maryland and Virginia), Massachusetts, New York Tri-State Area and the San Antonio-Austin Corridor, as well as emerging clusters.

INDUSTRY OVERVIEW

The US cyber security market makes up almost 40 per cent of the global cyber security industry, with four of the top five cyber security vendors headquartered in the US.[1]

The industry is largely centred around established technology centres, large research clusters, available cyber security professionals and access to government and private funding sources. Many of the clusters are home to world-leading research universities, and startups continue to thrive in these environments.

The federal government is the primary driver of the US cyber security industry, followed by the banking and finance, healthcare, critical infrastructure (energy) and ICT industries. The federal government's initiative to improve cyber security for critical infrastructure positions it as the biggest spender and funder of cyber security in the country, with US$19 billion (A$25.11 billion) budgeted for 2017.[2]

The banking and finance sector spends the most on cyber security outside of government, and is projected to spend US$68 billion from 2016 to 2020.[3] JPMorgan spent the most in the industry in 2015 at US$500 million[4], and Bank of America has announced cyber security is their only division without a spending limit.[5]

The healthcare industry, primarily concentrated on the East Coast, fell victim to the most cyber attacks in 2015,[6] and faces ongoing threats as the industry continues to digitise sensitive health information. The Health Insurance Portability and Accountability Act's provisions have had a wide-reaching impact on broader healthcare standards and procedures and the Act has driven the uptake of cyber security solutions within the US health sector. The global cyber security healthcare market is estimated to reach US$10.85 billion (A$14.26 billion) by 2022.[7]

THE GLOBAL CYBER SECURITY MARKET

GREW

4.5% FROM 2014 TO 2015.[8]

THE GLOBAL CYBER SECURITY MARKET

WILL REACH **US$170 BILLION** (A$223.37 BILLION) BY 2020.[9]

CLOUD SECURITY

&

HAVE THE HIGHEST INDUSTRY GROWTH PROJECTIONS.[10]

CYBER ATTACKS COST COMPANIES BETWEEN **US$400 TO US$500 BILLION** (A$525.57 TO A$657 BILLION) IN 2015.[11]

THE MOST PREVALENT

CYBER SECURITY THREATS

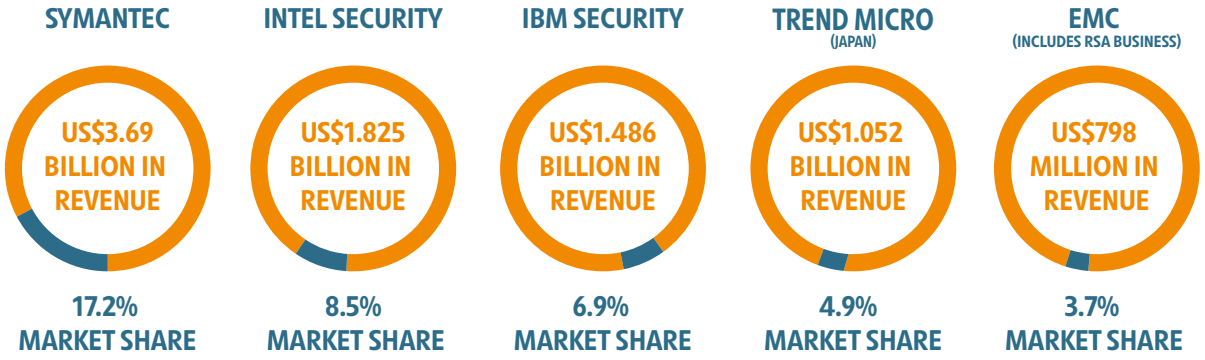
OVER THE NEXT THREE YEARS:

- ZERO-DAY ATTACKS
- CLOUD-DATA LEAKAGE
- MOBILE MALWARE
- TARGETED ATTACKS
- SQL INJECTION[12]

THE TOP 5 AREAS OF INCREASED CYBER SECURITY SPENDING BY ORGANISATIONS ARE

- **52%** NETWORK DEFENCES
- ENDPOINT AND MOBILE DEVICE PROTECTION **50%**
- **47%** DATA IN MOTION DEFENCES
- DATA AT REST DEFENCES **50%**
- **46%** ANALYSIS AND CORRELATION TOOLS [13]

LARGEST CYBER SECURITY VENDORS*[14]



* AS OF 2014

Cyber Security Job Postings by State[15]

Top States by Total Postings*

	State	Total Postings	% Growth (2010 – 2014)
1	California	288,744	75%
2	Virginia	20,276	38%
3	Texas	18,525	113%
4	New York	14,089	104%
5	Illinois	11,428	163%
6	Maryland	11,406	39%
7	Florida	9,847	135%
8	Georgia	8,757	121%
9	New Jersey	8,268	80%
10	Massachusetts	7,911	92%
11	Colorado	7,688	111%
12	North Carolina	7,503	127%
13	Ohio	6,281	141%
14	Pennsylvania	5,745	69%
15	Arizona	5,502	87%

US CYBER SECURITY CLUSTERS

CLUSTER OVERVIEW

Established Clusters

The San Francisco Bay Area

DMV (Washington D.C., Maryland And Virginia)

Massachusetts (Boston)

New York Tri-State Area

The San Antonio-Austin Corridor

Emerging Clusters

Atlanta

Chicago

Colorado (Boulder and Denver)

Dallas

Houston

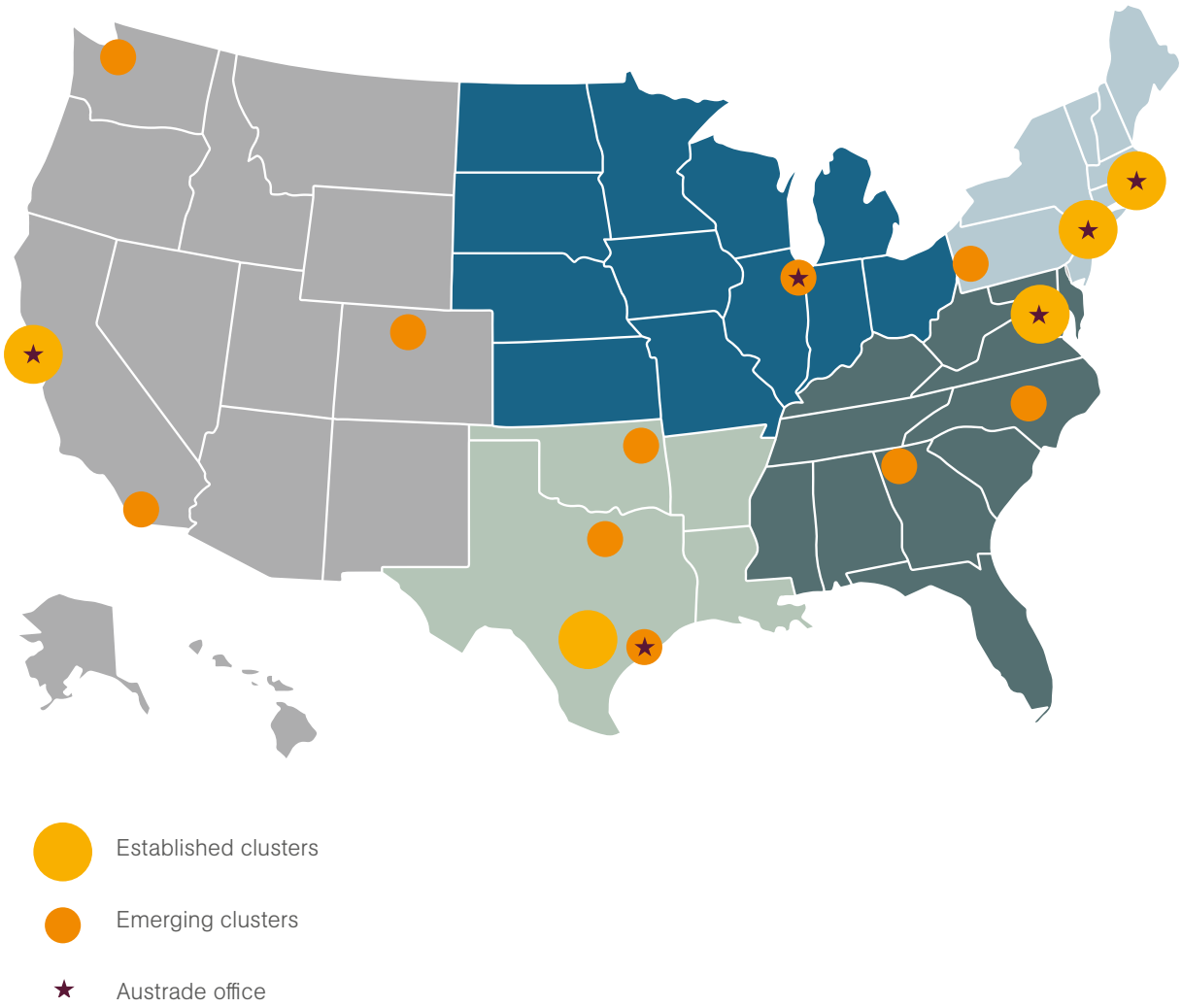
North Carolina (Research Triangle: Raleigh-Durham-Chapel Hill)

Pittsburgh

Seattle

Southern California (Los Angeles and San Diego)

Tulsa



THE SAN FRANCISCO BAY AREA

Description

The Bay Area is home to the US technology industry, and is the centre of the cyber security industry. The Bay Area has the most cyber security firms in the US.[16] The region attracts a top-tier cyber security labour force to meet the demand for both outsourcing services and in-house expertise (researchers and professionals), and it also possesses major sources of capital and technology expertise. The Bay Area receives the most venture capital investment in the country, with US$12 billion (A$15.77 billion) received in the first two quarters of 2016.[17]

Leading global cyber security firms Symantec, Intel, Palo Alto Networks and Cisco have their headquarters in the region, along with other giants Alphabet (Google) and Apple. The region is an attractive location for startups due to availability of capital, a business-friendly environment, educated workforce and strong university and research institutions.

Major Australian connections

- San Francisco is home to one of five Australian Government administered Landing Pads – a co-workspace and accelerator for Australian startups looking to go global. For more information visit australiaunlimited.com/landing-pads
- All of the major US cyber companies have a presence in Australia, including Intel, Palo Alto Networks, Cisco, FireEye and Symantec.
- Australian cyber security company Quintessence Labs has an office in San Jose, California.
- Cyber security insurance company UpGuard (formerly ScriptRock), a successful graduate of Startmate in Sydney in 2012, has an office in Mountain View.

Key universities and facilities

- Stanford University's SLAC National Accelerator Laboratory is one of the Department of Energy's key science laboratories, focussed on projects including cyber security.
- University of California at Berkeley, University Center for Long-Term Cyber security (CLTC) supports a multidisciplinary approach to a campus-wide cyber security initiative.

Key facts and figures

- California is home to the most software security firms in the country.[18]
- FireEye, Fortinet and Symantec provide leading cyber security services supporting all industries, including US hospitals and the oil and gas industries.[19]
- In the first two quarters of 2016, the region received over US$12 billion (A$15.77 billion) of investment, by far the most of any region in the US.[20]
- San Francisco proper has over 300 IT firms and almost 80,000 IT professionals.[21]

DMV (WASHINGTON D.C., MARYLAND AND VIRGINIA)

Description

The US Federal Government and the DC metro area are a major contibutor to the US cyber security industry. With US$14 billion (A$18.7 billion) spent on cyber security in 2016[22], and US$19 billion (A$25.38 billion budgeted for 2017)[23], the federal government spends the most on cyber security in the country. The Department of Homeland Security sets the cyber security strategy for the nation and administers funding and partnership grants. As of 2014, eight government agencies had projects related to cyber security, including the Department of Justice, the National Institute of Standards and Technology and the Department of Energy (DOE). Their focus is to improve cyber security education to counter the labour shortage, to form centres of collaboration among the public and private sector for information sharing and big data analytics, and to create compliance guidelines and regulations to ensure critical industries are protected.[24]

DC agencies, such as the National Security Agency (NSA) and the Central Intelligence Agency (CIA) hire many cyber security experts. Three of the five federal cyber security contractors are also headquartered in the region (Northrop Grumman, Lockheed Martin and General Dynamics). They combine with multiple military installations, the Naval Academy and other government contractors to make the region a global centre of cutting-edge research and expertise.

Major Australian connections

- Launched in January 2016, the Center for Strategic and International Studies holds an annual Australia-US Cyber Security Dialogue in partnership with the Australian Strategic Policy Institute. This dialogue will engage senior representatives from both countries' businesses, universities and governments to strengthen Australia-US cyber security ties.
- Australian companies Nuix, Corvata, iWebGate, and ThoughtWeb have offices in the DMV.

Key universities and facilities

- The NSA Research Center, the Defence Information School, the US Army Intelligence and Security Command, the Naval Security Group Activity and the 694th Intelligence Group of the US Air Force all operate out of Fort Meade.[25]
- The National Cybersecurity and Communications Integration Center (NCCIC) (four branches) serves as an information sharing centre, promoting collaboration between federal, state, and local governments, international partners and critical infrastructure to analyse data and discern threats.[26]
- The National Cybersecurity Center of Excellence operates as part of the National Institute of Standards and Technology (NIST) Information Technology Laboratory, and currently has projects in mobile security, geolocation in the cloud, situational awareness, and identity, access and software asset management.[27]

Key facts and figures

- The Defence Advanced Research Projects Agency (DARPA) uses big data analytics to improve machine learning and catch the 60 to 70 per cent of threats that anti-virus solutions miss.[28]
- In 2014 the DOE recieved a US$20 million (A$26.28 million) grant to develop cyber security tools and tech for energy-related critical infrastructure.[29]

MASSACHUSETTS (BOSTON)

Description

Massachusetts is home to a number of top cyber security firms, and is a recognised leader in medical research and healthcare. The healthcare industry was targetted by the most cyber attacks in 2015,[30] and the global market for healthcare cyber security is estimated to reach US$11 billion (A$14.45 billion) by 2022.[31] Leading US medical institutions such as Harvard Medical School, Massachusetts General Hospital and the Brigham and Woman's Hospital are a natural driver for cyber security solutions. The region is also a centre for medical technology, which requires the adoption of cyber security measures to comply with US healthcare privacy laws.

Supporting to these institutions are a number of leading cyber security firms, such as IBM Security, RSA, Mimecast and Carbon Black. IBM Security is one the fastest growing companies in the industry[32] and RSA operates under industry giant EMC. These companies, plus the general wealth of research funding, means that Boston has the resources to serve as both a supplier of innovation and services, and a key centre for industry demand.

Major Australian connections

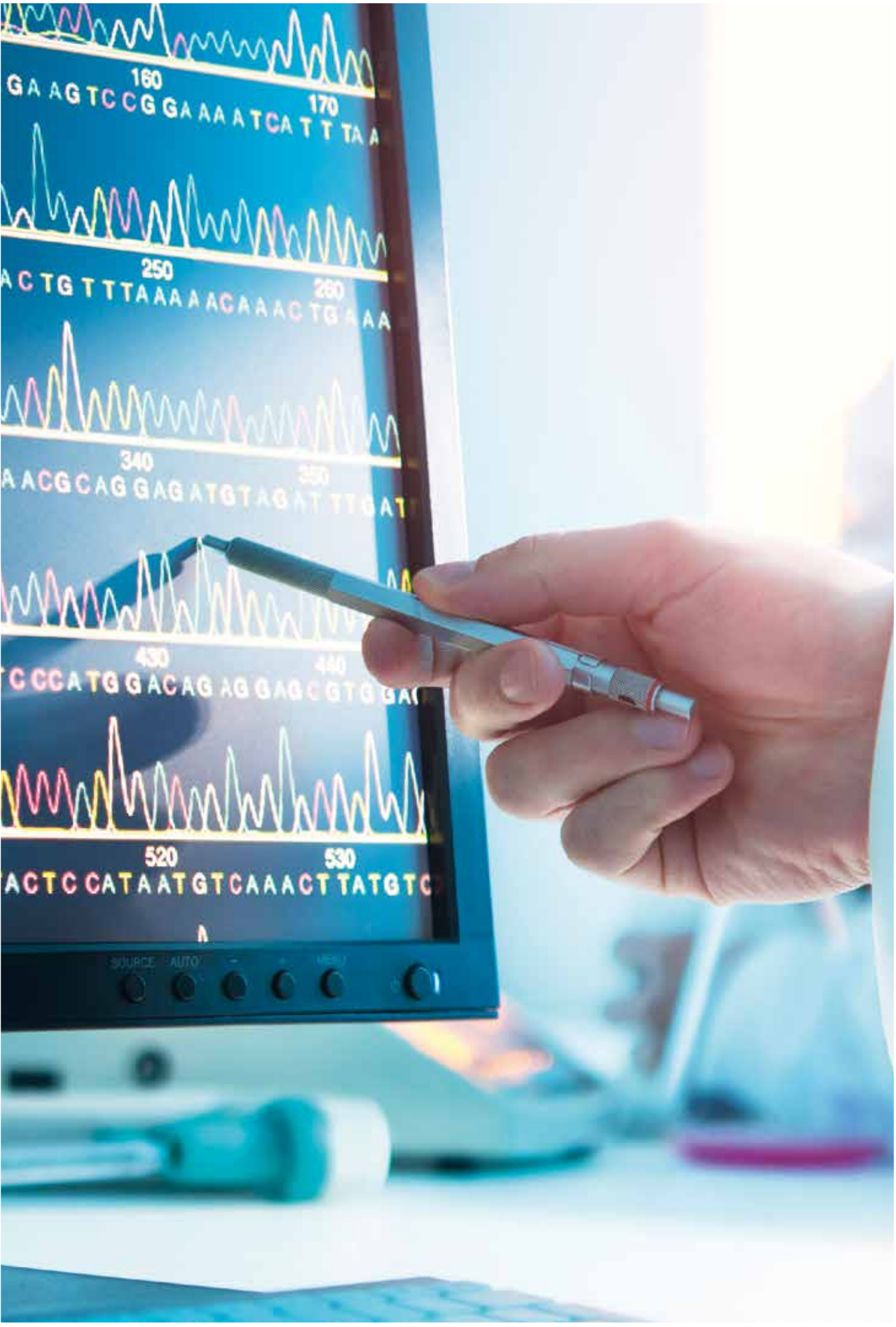
- IBM Security remains the fastest growing company in the industry, growing three times faster than the entire market in 2014 at 17 per cent.[33] IBM is planning an Australian National Cyber Security Centre in Canberra. The Centre will connect Australia with IBM's global network, providing access for the government and the private sector to IBM's security technology and expertise.

Key universities and facilities

- Massachusetts Institute of Technology (M.I.T) Lincoln Laboratory: Cyber Security and Information Sciences has some of the leading researchers in the cyber security industry and remains one of the top US universities for science and technology.
- The Advanced Cyber Security Center (ACSC) focuses on collaboration between industry, university and government organisations to further expand information sharing, research and development, education programs and public policy.
- University of Massachusetts at Amherst Cybersecurity Institute takes a multi-disciplinary approach to cyber security solutions, working with government, industry and university partners. The National Science Foundation (NSF) awarded them US$4.2 million (A$5.52 million) of funding in 2016.[34]

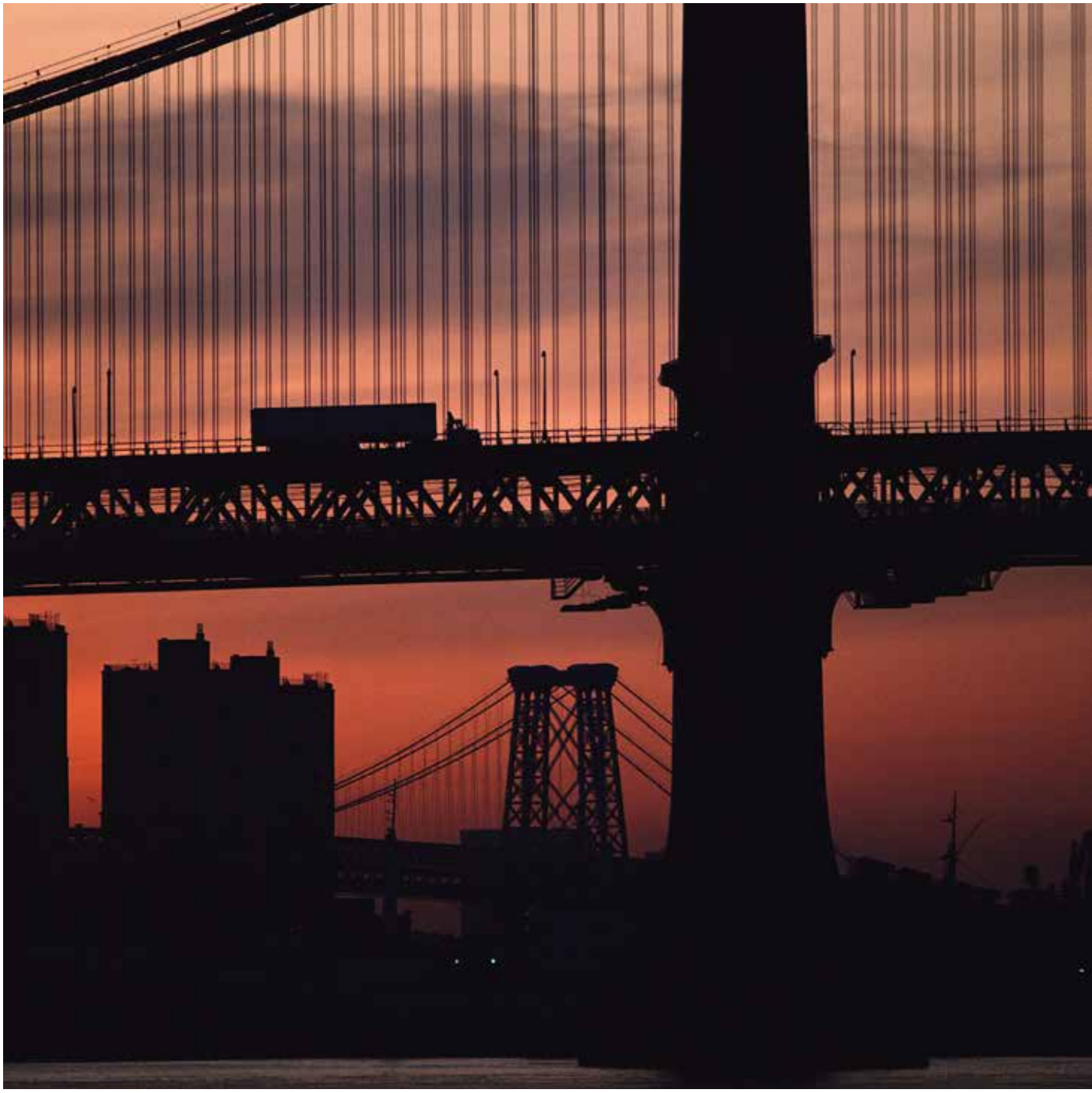
Key facts and figures

- RSA, Imprivata, Rapid7 and Carbon Black play key roles in the US cyber security industry, Carbon Black for encryption services (serving the oil and gas industry), Imprivata for health identity and access management, and Rapid7 for risk and compliance management (in health).[35]
- For the 2012-2013 school year Northeastern University received one of only four NSA and US Cyber Command awards as a Center of Academic Excellence in Cyber Operations.[36]
- The MassMutual Foundation announced in June 2016 that they will give the University of Massachusetts Amherst US$15 million (A$19.53 million) over 10 years to enrich their data science and cyber security programs.[37]


160
170
250
260
340
430
440
520
530
SOURCE
AUTO

Industries Experiencing the Highest Incident Rates[38]

Healthcare | Manufacturing | Financial Services | Government | Transportation



NEW YORK TRI-STATE AREA

Description

Driven by the US banking and finance industry, the New York Tri-State Area has a high demand for cyber security services. The financial services industry suffers the 3rd highest number of attacks out of any industry in the US.[39] Headquartered in New York City, two of the biggest cyber security spenders, JPMorgan and Citigroup, will spend a combined US$800 million (A$1.05 billion) in 2016.[40]

Major Australian connections

Australia's four biggest financial institutions (NAB, the Commonwealth Bank, Westpac and ANZ) all have a presence in New York. They spend a combined $A400 million on cyber security a year.[41]

Key university and facilities

- Columbia University Data Science Institute is one of the leading schools for cyber security research. Their data sciences cyber security sector focuses on mobile security, data analytics and more energy efficient cyber security systems. Their partners include AT&T Labs Research, DARPA and the New York-Presbyterian Hospital.
- Princeton University's Security & Privacy Research Group works under the Department of Computer Science. Researchers focus on cryptography, web security, distributed systems and networking and improving privacy technologies. The group also works collaboratively with Princeton's Center for Information Technology Policy.
- Rutgers University Center for Information Assurance (RUCIA) focuses on education in the field and research in computer security, information assurance, systems reliability and data mining.
- New York-Presbyterian Hospital is one of the largest hospitals in the country, and a leader in secure cyber security practices.

Key facts and figures

- The New York Metro Area currently ranks 3rd for the most venture capital funding in the US[42] and is ranked as the 2nd best city in the US for tech startups by availability of services.[43]
- Headquatered in the region, IBM, DataMotion, Verizon and LexisNexis are key spenders in the national cyber security industry.

THE SAN ANTONIO–AUSTIN CORRIDOR

Description

The San Antonio-Austin corridor's cyber security focus is defence, although the region also has a growing and influential commercial sector. San Antonio hosts one of eight NSA facilities, and ranks 2nd nationally for defence related cyber security missions and Department of Defence (DOD) partnerships with civilian companies.[44] 'Security Hill' remains the epicentre of cyber security activities in Texas, with operations supported by a sizable cluster of private-sector technology companies and startups in Austin, and to a lesser extent San Antonio.[45]

The bulk of industry research and government funding is directed to activities associated with the Cyber Command of the 24th Air Force (San Antonio). However, local government agencies supported by the region's private sector are also focussed on creating a business-friendly ecosystem to support the growth of private enterprise and a highly skilled workforce. Texas is home to the 2nd highest percentage of software security publishing firms in the US at 6.4 per cent, with Austin alone home to a total of 46 incubators, accelerators and co-working spaces.

Cyber security trained military veterans have joined forces with leading technology and government contractors to bolster the commercial cyber security sector in the region. For example, the establishment of Big Sec Foundry, a cyber security incubator, is a collaboration between entities spread between Austin and San Antonio, and is part of a growing inter-city connection.

Major Australian connections

- Dr. Raymond Choo from the University of South Australia currently works at the University of Texas in San Antonio (UTSA) on a Cloud Technology Endowed Professorship.
- Australian cloud security company StratoKey have operations in Austin. They are a leading innovator in the Cloud Access Security Broker market.

Key universities and facilities

- San Antonio is home to the Air Force Cyber Command of the 24th Air Force, the Federal Bureau of Investigation's (FBI) Cyber Security Task Force and NSA Texas.
- The University of Texas in San Antonio (UTSA) and in Austin (UTA) have institutions devoted to cyber security research and education. UTSA has achieved national recognition for their work.[46]
- The Southwest Research Institute is one of the oldest and largest non-profit research and development facilities in the US.[47]
- Austin Technology Incubator (ATI) is one of the country's most successful incubators with over US$650 million (A$854 million) raised by ATI companies since 2007.[48]

Key figures

- Lackland Air Force Base, Fort Sam Houston US Army Base, Randolph Air Force Base, Boeing and the Southwest Research Institute are key employers in San Antonio.
- San Antonio has the second largest concentration of data centres in the US[49], and is home to 1,000 IT companies, including 200 cyber security firms.[50] The economic impact of these IT companies is estimated at US$10 billion (A$13 billion).
- Austin had the highest growth rate amongst US cities for cyber security jobs at 209 per cent from 2010 to 2014[51], and ranks as the best place in the US for tech startups.[52]
- Notable commercial security businesses headquartered in the region include Ziften, Absolute Software and Forcepoint.


SPEED LIMITS ARE ENFORCED
EXPECT DELAYS
ROADWORKS AT PRINCES HWY
SPEED LIMITS ARE ENFORCED

EMERGING CLUSTERS

ATLANTA

Atlanta ranks in the top 10 for both cyber security job demand and growth. The Georgia Institute of Technology and 200 health IT companies with an annual revenue of over US$4 billion (A$5.26 billion) play a growing role in cyber security research and the development of health IT cyber security solutions. VixVerify, an Australian financial cyber security firm, chose Atlanta as its Americas headquarters.

CHICAGO

Boeing has recently relocated its headquarters to Chicago and the city has a high demand for cyber security experts.[53]

COLORADO (BOULDER AND DENVER)

Colorado is a major market for emerging cyber security companies, led by root9B. The cyber security industry in Colorado is well connected and supported by the large US Defence operations in the state. Colorado local governments are at the forefront of adopting cyber security initiatives, and the National Cybersecurity Center is about to launch in partnership with the University of Colorado in Colorado Springs. Colorado headquartered cyber security companies Level 3, LogRhythm, Webroot, and Ping Identity all have operations in Australia.

DALLAS

With the Federal Reserve, AT&T's headquarters, and the increasing global growth and importance of fintech, Dallas has some of the the highest demand for cyber security professionals in the country.[54]

HOUSTON

In response to the increasing digitisation of the critical infrastructure and healthcare industries, Houston will continue to drive demand for cyber security services. Houston's globally recognised innovative oil and gas industry, as well as its leading medical hub (Harris Health System and the Texas Medical Center), are central drivers to cyber security integration and supply chain adoption.[55]

NORTH CAROLINA (RESEARCH TRIANGLE: RALEIGH-DURHAM-CHAPEL HILL)

While mainly focusing on medical and biotech research, the Research Triangle remains home to cloud computing and has several notable IoT and big data analytics centres.[56]

PITTSBURGH

Widely considered the leading university in the country for cyber security, Carnegie Mellon University makes Pittsburgh a hub for industry innovation. The university has a campus located in Adelaide, South Australia with various cyber-related programs.[57]

SEATTLE

The cyber security industry in Seattle is largely dominated by Boeing, Lockheed Martin, Microsoft, Amazon, DOD and DOE. Seattle is a leading location for industry research, with most research occurring on government property such as the Pacific Northwest National Laboratory. Along with Microsoft and Amazon, the Seattle based company F5 has a large footprint in Australia.

SOUTHERN CALIFORNIA (LOS ANGELES AND SAN DIEGO)

Southern California received US$3.4 billion (A$4.47 billion) of venture capital funding in the first two quarters of 2016, 2nd only to Silicon Valley. Los Angeles ranks 6th nationally for demand for cyber security professionals, and San Diego hopes to use the Navy's Information Warfare System Command to increase the industry's estimated US$1.9 billion (A$2.50 billion)[58] economic impact.

TULSA

Since 2001 the University of Tulsa's Cyber Corp Program has worked with their Institute for Information Security (iSec) to field 350 students, 70 per cent of whom now work for the NSA or CIA.[59]

HOW AUSTRADE CAN HELP

If you are an Australian company ready to internationalise your cyber security business, Austrade can assist with market entry and expansion. We provide some tailored services, as well as access to a range of specialists, including:

- market research
- channel marketing consultants
- lead generation agencies
- legal, accounting, tax and immigration advisory services
- banking and financial service providers
- commercial real estate agencies
- relevant industry network specialists.

If you are looking to invest in Australia, Austrade can assist. We are able to provide the contacts and information you need to establish your business successfully within Australia or to make the right decision in sourcing Australian products or services. Assistance to potential international investors includes:

- initial coordination of investment enquiries and assistance
- information on the Australian business and regulatory environment
- market intelligence and investment opportunities
- identification of suitable investment locations and partners in Australia
- advice on Australian government programs and approval processes.

Commonwealth of Australia represented by the Australian Trade and Investment Commission (Austrade) ABN 11 764 698 227. ISSN: 1756-8528.

To find out more, contact Austrade in the US:

Austrade San Francisco
Frances van Ruth, Trade and Investment Commissioner
575 Market Street Suite 1800
San Francisco CA 94105
Tel: +1 415 644 3620
Email: USA@austrade.gov.au

Austrade Boston
745 Atlantic Avenue, 8th Floor
Boston MA 02111
Tel:+1 646 344 8111
Email: USA@austrade.gov.au

Austrade Chicago
123 North Wacker Drive
Suite 1325
Chicago Il 60606
Tel: +1 312 374 9401
Email: USA@austrade.gov.au

Austrade Houston
3009 Post Oak Blvd Suite 1310
Houston TX 77056
Tel: +1 832 962 8422
Email: USA@austrade.gov.au

Austrade New York
Australian Consulate
150 East 42nd St, 34th Floor
New York NY 10017
Tel: +1 646 344 8111
Email: USA@austrade.gov.au

Austrade Washington DC
Australian Embassy
1601 Massachusetts Ave, NW
Washington DC 20036
Tel: +1 202 454 9744
Email: USA@austrade.gov.au

1. 2015 CSO Cybersecurity Business Report http://www.csoonline.com/article/2946017/security-leadership/worldwide-cybersecurity-market-sizing-and-projections.html. Accessed 17 October, 2016
2. 2016 Barak Obama Cybersecurity Op-Ed, Wall Street Journal http://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003 Accessed 4 November 2016
3. Homeland Security Research: U.S. Financial Services Report http://homelandsecurityresearch.com/2014/10/u-s-banking-financial-services-retail-payment-cybersecurity-market-2015-2020/ Accessed 17 October, 2016
4. J.P Morgan CEO, James Dimon, at Institute of International Finance Panel Discussion on October, 10 2014
5. Bank of America CEO, Brian Moynihan during a Bloomberg Television interview on January 21, 2015
6. IBM 2016 Cyber Security Intelligence Index www-03.ibm.com/security/data-breach/cyber-security-index.html Accessed 17 October, 2016
7. 2016 Grand View Research Healthcare Cyber Security Report https://www.grandviewresearch.com/press-release/global-healthcare-cyber-security-market. Accessed 17 October, 2016
8. 2015 Forbes Report: The Business of Cybersecurity http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#52a1cbb910b2 Accessed Oct 17 2016
9. Cybersecurity Ventures Q3 2016 Cybersecurity Report
10. Ibid
11. The Australian. Drake soars on cybersecurity deal. Genome CEO, Amir Rasilevski in an interview 10 March, 2016. http://www.theaustralian.com.au/news/latest-news/drake-soars-on-cybersecurity-deal/news-story/5bf3802fbee35c015536317007354314
12. Business Insider, Ponemon Institute and Raytheon. This one chart explains why cybersecurity is so important. April 5, 2016 http://www.businessinsider.com/cybersecurity-report-threats-and-opportunities-2016-3/?r=AU&IR=T
13. 2015 Vormetric Insider Threat Report. https://www.vormetric.com/campaigns/insiderthreat/2015/ Accessed 17 October, 2016
14. 2015 CSO Cybersecurity Business Report
15. Job Market Intelligence: Cybersecurity Jobs, 2015. Burning Glass. http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
16. Cybersecurity Ventures 500 List http://cybersecurityventures.com/cybersecurity-500/ Accessed 17 October, 2016
17. PWC Investment by Region 2016 https://www.pwcmoneytree.com/CurrentQuarter/ByRegion Accessed 17 October, 2016
18. IBISWorld Industry Report 51121f: Security Software Publishing in the U.S. published April 2016
19. Frost & Sullivan Reports: Cybersecurity in the U.S. Oil and Gas Industry Report published 3 February 2015, and the U.S. Hospital Cybersecurity Market 2015-2021 Report published 24 July 2016
20. PWC Investment by Region 2016 https://www.pwcmoneytree.com/CurrentQuarter/ByRegion Accessed 17 October, 2016
21. San Francisco Center for Economic Development http://sfced.org/why-san-francisco/sectors/information-technology/ Accessed October, 17 2016
22. 2015 Forbes Report: The Business of Cybersecurity http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#52a1cbb910b2 Accessed Oct 17 2016
23. Cybersecurity Ventures Q3 2016 Cybersecurity Report http://cybersecurityventures.com/cybersecurity-market-report/ Accessed October, 17 2016
24. National Governors Association (NGA) Federal Cybersecurity Programs (2014) http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1410FederalCybersecurityPrograms.pdf Accessed Oct 17. 2016
25. US Military Bases http://dc.about.com/od/communities/a/MilitaryBases_2.htm Accessed October, 17 2016
26. US Computer Emergency Readiness Team https://www.us-cert.gov/nccic Accessed October, 17 2016
27. National Governors Association (NGA) Federal Cybersecurity Programs (2014)
28. Defense Advanced Research Projects Agency (DARPA) http://www.darpa.mil/ Accessed October 17 2016
29. Frost & Sullivan Report: Cybersecurity in the US Oil and Gas Industry, published 3 February 2015
30. 2016 IBM X-Force Cyber Security Intelligence Index. Accessed. 17 Oct 2016
31. 2016 Grand View Research Healthcare Cyber Security Report https://www.grandviewresearch.com/press-release/global-healthcare-cyber-security-market. Accessed 17 October, 2016
32. 2015 CSO Cybersecurity Business Report
33. Ibid
34. UMass Amherst Cybersecurity Institute https://cybersecurity.umass.edu/ Accessed 17 October, 2016
35. Frost & Sullivan Report: U.S. Hospital Cybersecurity Market – 2015-2021 published 24 July 2016
36. NSA National Centers of Academic Excellence in Cyber Operations. Accessed 17 October, 2016
37. UMass Amherst Press Release http://www.umass.edu/newsoffice/article/new-massmutual-foundation-and-umass Accessed 17 October, 2016
38. IBM 2016 Cyber Security Intelligence Index www-03.ibm.com/security/data-breach/cyber-security-index.html Accessed 17 October, 2016
39. 2016 IBM X-Force Cyber Security Intelligence Index. Accessed 17 October, 2016
40. 2015 Forbes Report: http://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#cd96af61112b Accessed 4 November 2016
41. Australian Financial Review, http://www.afr.com/technology/banks-are-now-paranoid-about-cyber-threats-20160207-gmnnkc Accessed 4 November 2016.
42. PWC Investment by Region 2016 https://www.pwcmoneytree.com/CurrentQuarter/ByRegion Accessed 17 October, 2016
43. 2016 Sungard Availability Services Report http://www.sungardas.com/us-cities-for-business/Pages/index.html Accessed 17 October, 2016
44. Cybersecurity San Antonio http://cybersecuritysa.com/ Accessed 17 October, 2016
45. San Antonio Economic Development Foundation Cybersecurity Factsheet 2015
46. Ibid
47. Southwest Research Institute http://www.swri.org Accessed 17 October, 2016
48. Austin Technology Incubator http://ati.utexas.edu/about-us/ Accessed 17 October, 2016
49. San Antonio Economic Development Foundation Cybersecurity Factsheet 2015
50. Cybersecurity San Antonio http://cybersecuritysa.com/ Accessed 17 October, 2016
51. Burning Glass Technologies Job Market Intelligence: Cybersecurity Jobs 2015 http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf Accessed 17 Oct. 2016
52. 2016 Sungard Availability Services Report
53. Burning Glass Technologies Job Market Intelligence: Cybersecurity Jobs 2015 http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf Accessed 17 Oct. 2016
54. Ibid

55. 2016 HealthCare's Most Wired Winners
56. Research Triangle Region Pervasive Computing Report http://www.researchtriangle.org/clusters/pervasive-computing Accessed 17 October, 2016
57. Carnegie Mellon University Australia http://australia.cmu.edu/
58. San Diego's Cybersecurity Industry. San Diego Cyber Center of Excellence http://sdccoe.org/wp-content/uploads/2015/01/CCOE-EIS-2016-.pdf
59. The University of Tulsa Cyber Corps https://engineering.utulsa.edu/academics/centers-institutes/cyber-corps/

austrade.gov.au