

CYBER SECURITY



Australian Government
Australian Trade and Investment Commission



Australia
UNLIMITED



DISCLAIMER

Austrade does not endorse or guarantee the performance or suitability of any introduced party or accept liability for the accuracy or usefulness of any information contained in this Report. Please use commercial discretion to assess the suitability of any business introduction or goods and services offered when assessing your business needs. Austrade does not accept liability for any loss associated with the use of any information and any reliance is entirely at the user's discretion.

©Commonwealth of Australia 2017

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Commonwealth, available through the Australian Trade and Investment Commission. Requests and enquiries concerning reproduction and rights should be addressed to the Marketing Manager, Austrade, GPO Box 5301, Sydney NSW 2001 or by email to marketing-commshelpline@austrade.gov.au

Publication date: January 2017

PROTECTING INNOVATION, GROWTH AND PROSPERITY



> INTRODUCTION

INDUSTRY
OVERVIEW

INDUSTRY
STRENGTHS

FURTHER
INFORMATION

Australia has been at the forefront of developments in safety and security in the online environment with robust legislation, advanced law enforcement capability, rigorous policy development and strong technical defences.

These defences are provided through:

- a string of dedicated research hubs, focused in academic institutions and supported by private sector efforts
- bespoke product development which provides technical defences in both hardware and software
- information security consulting services providing expert advice on current issues and future trends
- a wide variety of training and education services covering all aspects of technical and non-technical issues.

The Australian cyber security sector understands the scale of the cyber security challenge, including the social factors influencing individuals, organisations and

international attitudes towards cyber security. It assists organisations to understand and meet their obligations to protect customers' digital assets and information, while strong collaboration within the ecosystem fosters innovation.

This industry capability statement provides an overview of Australian capabilities in the cyber security ecosystem, including research and development, product development, security management, advisory and consulting services and education and training services. It contains examples of some of the many Australian organisations with specialist expertise.

Talk to your local Austrade representative for more tailored advice and information on connecting and partnering with the Australian cyber security sector.



INTRODUCTION

> INDUSTRY OVERVIEW

INDUSTRY STRENGTHS

FURTHER INFORMATION

RESEARCH AND DEVELOPMENT

Australia has world-class cyber security research capability, housed within the university sector but also within government and the private sector. Some of the best cyber security researchers in the world are based in Australia, providing an important platform for the development of critical mass and future growth.

In terms of citation impact, an indicator of research quality, Australian cyber security research ranks ahead of the US, Canada, England, Germany, Japan and Singapore.¹

Australia is a popular test bed for new technology and the recipient of commercial investment in research and development. This has seen the development of products such as world-leading payments technology developed by the Australian banking and finance sector.

Australian researchers focus on niche areas of cyber security such as quantum technology, wireless technology and trustworthy systems. CSIRO's Data 61, Australia's largest data innovation group, has developed the seL4 kernel, which provides the strongest operating system security available in the world (see case study opposite).

The Defence Science and Technology Group (DST) has developed award-winning approaches for the trustworthy use of commercial hardware (see case study page 8). Importantly Data 61 and DST are partnering to bring together these developments and provide feasible trustworthy software and hardware solutions with broad applicability.

In another field, an international team of scientists led by Swinburne University has set a new record for the complexity possible on a quantum computing chip (see case study page 10).

The Australian Chief Scientist has identified cyber security as one of the

nation's nine Science and Research Priorities. Focus on these priorities is designed to increase investment in areas of immediate and critical importance to Australia and its place in the world. Approximately A\$80 million is being directed to the cyber security priority area. [science.gov.au/scienceGov/ScienceAndResearchPriorities/Pages/Cybersecurity.aspx](https://www.science.gov.au/scienceGov/ScienceAndResearchPriorities/Pages/Cybersecurity.aspx)

In addition, the Department of Defence has announced A\$12 million in funding for a new purpose-built facility at the Australian National University (ANU) to improve Australia's cyber security. Once completed, the building will house 70 students, academics and staff from Defence's cyber agency, the Australian Signals Directorate. The investment will allow ANU and Defence to collaborate on research in areas including high-performance computing, data analytics and cyber security.

Data61 takes cyber security to a new level

CSIRO's Data61 is a group at the forefront of a rapidly emerging cyber security ecosystem. It is both Australia's largest data-focussed research and innovation organisation and one of the world's leading groups of its kind.

The Trustworthy Systems group at Data61 has developed the ground-breaking seL4 microkernel. The seL4 kernel runs at the core of a computer's operating system and provides secure software compartments. These compartments provide the means to isolate and contain faults and cyber attacks.

The seL4 kernel provides the strongest operating system security available in the world, and it provides the strongest evidence in the world that it does so. This evidence consists of a mathematical, machine-checked proof over the seL4 machine code. The proof is publicly available for independent verification.

seL4 is the world's most advanced operating system microkernel today. The team has demonstrated that seL4 not only achieves the highest levels of assurance and protection available, the kernel is also faster than any other microkernel that runs on the same machine architecture.

The seL4 kernel was released as open-source code in July 2014 with the aim of catalysing the widespread development of more dependable, safe, secure and reliable computer systems. Data61's Trustworthy Systems team continues to extend the research roadmap and develop further policy and application frameworks for commercial use cases.

There is confidence that the worldwide use of seL4 will eclipse its predecessor L4 kernel – developed by the same group in Data61 – which has been deployed by the billions and is used in all recent shipments of iOS-based mobile devices.

In recent trials, for example, Boeing's autonomous Unmanned Little Bird helicopter was protected from cyber attacks by running seL4, and the United States Government has provided significant funding to support multiple research and commercialisation projects utilising the technology.

data61.csiro.au



Image courtesy of Data61, CSIRO

Developing Resilient Cyber Systems - Defence Science and Technology Group

In the face of ubiquitous encryption, untrustworthy ICT and a sophisticated threat environment, Defence Science and Technology Group (DST Group) undertakes research and development of novel concepts and technologies to enable autonomous, resilient and effective cyber capabilities with an operational edge.

DST Group develops cyber solutions, applicable to fields such as the military and critical infrastructure space, that are resilient in the face of online cyber-attacks, and where the integrity of the underlying computer systems cannot be sufficiently guaranteed for critical applications.

The Digital Video Guard is an example of the research and development that DST Group is undertaking. The Digital Video Guard is a hardware-based security solution that was designed to allow the military to access classified networks from unclassified and untrusted sources. It has no traditional software footprint, sidestepping common vulnerabilities associated with traditional software-based solutions. It uses encrypted images to securely transport sensitive information

through untrustworthy networks and computers.

By utilising a hardware-based device external to the host computer system, and through the use of embedded hardware encryption, the Digital Video Guard is able to display confidential information without any concerns that the host computer, or the network to which it is attached, will modify or capture this sensitive information.

The Digital Video Guard technology has also been integrated into a commercial tablet, transforming an untrusted consumer device into a highly portable and secure information device for the military. The advantage of this approach is that the military can use the tablet for accessing the (insecure) internet without compromising the device when they then have to access sensitive information.

dst.defence.gov.au



Image courtesy of DST Group

Advanced Cyber Security Research Centre – Macquarie University

The Advanced Cyber Security Research Centre (ACSRC) at Macquarie University aims to achieve advances in cyber security in the theory, design and management of models and techniques that enable secure and dependable computing information systems and services. An important characteristic of ACSRC is its research capabilities and expertise in addressing the security challenges that arise in a heterogeneous mobile-distributed network environment involving distributed systems, wireless, broadband and peer-to-peer networks, mobile devices and distributed information services.

A feature of security research at the ACSRC is its multi-faceted nature, with security acting as a thread that sews multiple technologies, applications, models and policies together. Challenges (be they in healthcare, transportation or e-commerce) do not come in neat packages and it is critical for research in technology and policy to go hand-in-hand.

The ACSRC academic staff's expertise includes computing, information technology, systems engineering, risk analysis as well as legal issues. The Centre also has researchers and leaders from industry as Adjuncts and leading international academics from overseas universities as Associates.

Current research interests and projects include cloud services security, cloud data security and privacy, secure virtualization systems, trusted computing, software security, mobile applications security, wireless and mobile ad hoc networks security, security and privacy in big data applications, Internet of Things security, software defined networks security, advanced recognition techniques, secure RFID devices and applied cryptography.

The ACSRC has several international collaborations and also supports Masters Postgraduate Programs in Cyber Security and Internetworking.

mq.edu.au/research/research-centres-groups-and-facilities/innovative-technologies/centres/advanced-cyber-security-research-centre



Image courtesy of Macquarie University

Swinburne University

Swinburne University is leading an international team of scientists who have set a new record for the complexity possible on a quantum computing chip. This project is moving the world one step closer to the ultra-secure telecommunications of the future.

Quantum science and technology uses the notion of entangled particles – typically either electrons or particles of light called photons. These particles remain connected even if separated over large distances, so that actions performed by one affect the behaviour of the other.

The research team has created entangled photon states with unprecedented complexity, and over many parallel channels simultaneously, on an integrated chip. Importantly, the chip was created using processes compatible with the current computer chip industry, opening up the possibility of incorporating quantum devices directly into laptops and mobile phones.

The researchers use 'optical frequency combs' which, unlike the combs we use to de-tangle hair, actually help to 'tangle' photons on a computer chip. Their achievement has set a new record in both the number and complexity of entangled photons that can be generated on a chip. This development also generates entangled photon pairs over hundreds of channels simultaneously. These are vital steps in developing ultra-secure telecommunications, and with direct applications in quantum information processing, imaging, and microscopy.

This is the culmination of 10 years of collaborative research on complementary metal-oxide-semiconductor (CMOS) compatible chips for both classical and quantum nonlinear optics. The possibility of powerful optical quantum computers for everyday use is now closer than ever before.

swinburne.edu.au

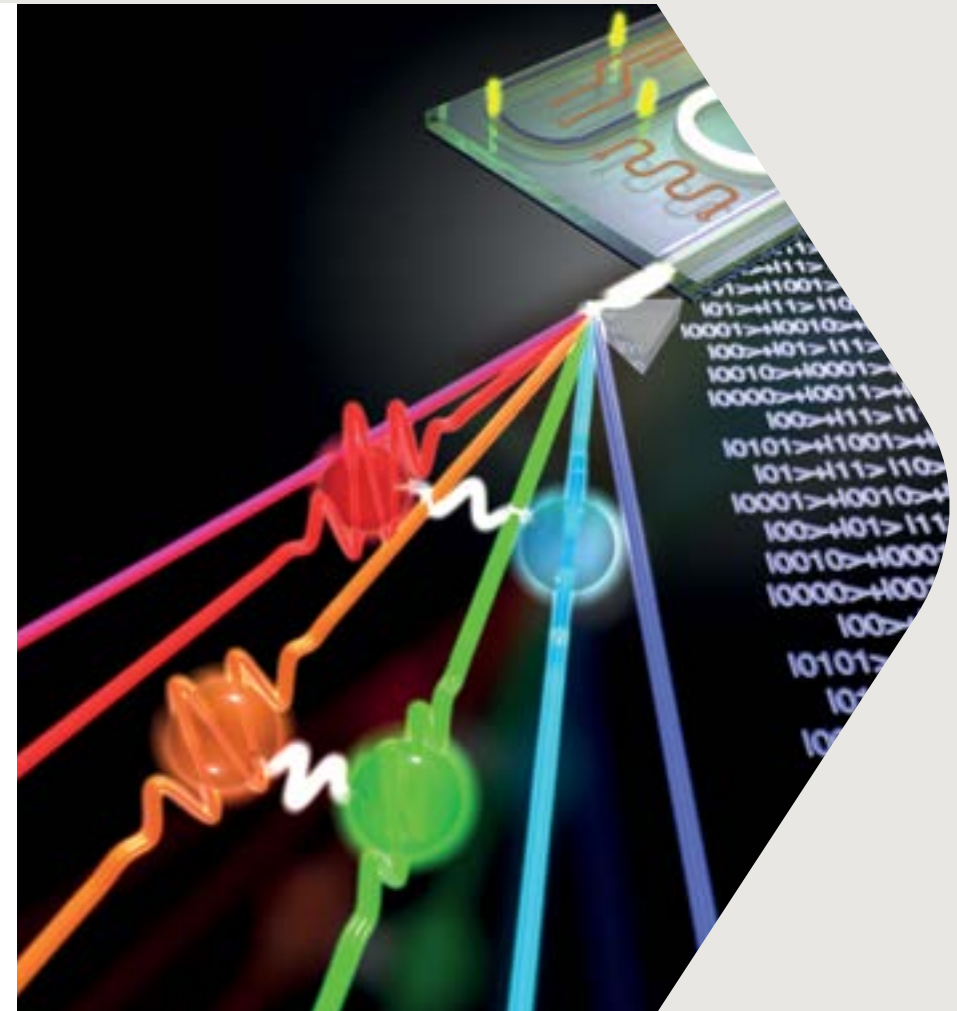


Image courtesy of Swinburne University

INTRODUCTION

> INDUSTRY OVERVIEW

INDUSTRY STRENGTHS

FURTHER INFORMATION

SOFTWARE AND PRODUCT DEVELOPMENT

A broad range of Australian companies are focused on developing niche value-added cyber security products and services. These companies range from innovative startups through to multinational organisations and have expertise in identity management, encryption, wireless technologies and trustworthy systems. Many also collaborate with government agencies and the higher education sector.

For example:

- iWebGate, founded in 2004, is pioneering a new form of virtualisation technology - the Virtualisation of Network Services, providing faster, more secure and reliable access to networks and network services.
- MailGuard, a cloud-based security provider, has a proprietary platform that addresses the evolving threat landscape by blocking email threats, enabling immediate protection for users across the globe.

- Nuix provides leading technology for solving complex real-world data challenges including investigation, cyber security, insider threats, intelligence, litigation, regulation, privacy and risk management.
- Wontok addresses security architecture from the ground up, by assuming malware is already present on the PC desktop and mobile device and creating a barricade around sensitive transactions. Wontok identifies gaps in security left behind by off-the-shelf antivirus software.

Wontok, Quintessence Labs (see case study page 12), Nuix (see case study page 13) and Stratokey (see case study page 14) are some of the companies that feature on the Cybersecurity 500, the definitive list of the world's leading and most innovative companies in the cyber security industry.

[cybersecurityventures.com/
cybersecurity-500/](https://cybersecurityventures.com/cybersecurity-500/)

QuintessenceLabs

QuintessenceLabs delivers advanced cyber security solutions. One of their leading solutions is the highly secure Trusted Security Foundation (TSF), which combines the security of a FIPS 140-2 Level 3 hardware security module (HSM) with an advanced key and policy manager and high-speed quantum random number generator.

One customer utilising this solution is a leader in cloud-based document and email management, with hundreds of thousands of users around the globe. They operate an expanding network of data centres in the US, Europe and the Asia-Pacific and they aim to provide the highest level of protection for digital assets. All data is encrypted to the highest standards, with one or more levels of encryption delivered at a customer level. The customer needed to expand their data centres, while continuing to enhance data protection through an additional encryption layer. They wanted scalability and speed, unbeatable security and redundancy, as well as interoperability to integrate seamlessly with existing infrastructure.

QuintessenceLabs successfully partnered with them to develop a targeted, integrated solution. Multiple redundant TSF solutions were deployed to all the customer's data centres. The customer's application servers provide the user interface and business logic for the service. Their users' documents are encrypted with unique keys generated by the TSF solution, and then wrapped using master keys to ensure isolation between customers. This provides scalability as well as enabling dual control of the documents by the end user and cloud document provider.

Key services included fully synchronous replication assurance allowing both logical and physical segregation to meet multi-level, regulatory, and operational security needs. In addition, the 1Gb/s quantum random number generator has ample throughput to meet the master key needs for each data centre with room for expansion.

The TSF solution is also deployed in other industries including financial services, government and defence.

quintessencelabs.com

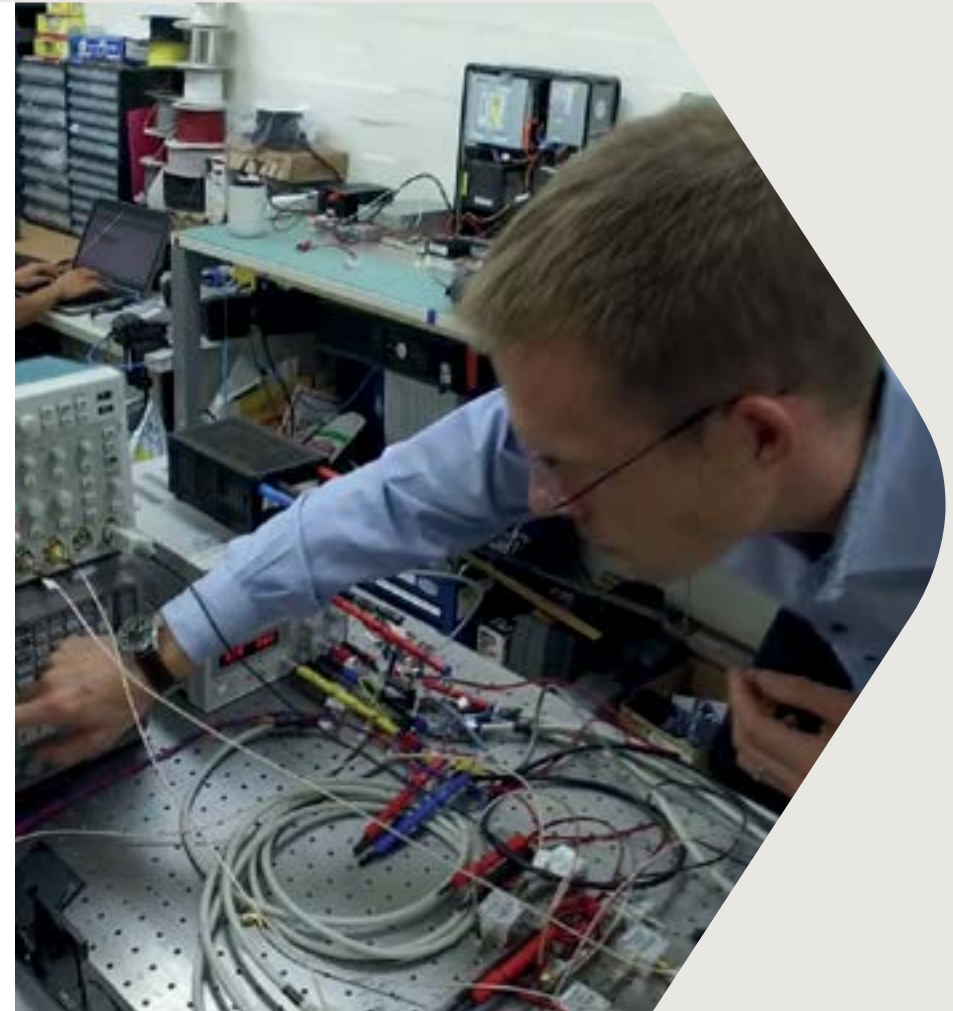


Image courtesy of QuintessenceLabs

Nuix

Nuix supplied document processing and investigation technology that was essential to the Panama Papers investigation conducted by German newspaper *Süddeutsche Zeitung* and the International Consortium of Investigative Journalists (ICIJ).

Süddeutsche Zeitung received an anonymous leak of approximately 11.5 million documents, totalling 2.6 terabytes of data, detailing the activities of Panamanian law firm Mossack Fonseca, which helped clients set up anonymous offshore companies. While these offshore entities are generally legal in the jurisdictions in which they are registered, the investigation revealed that some were allegedly used for unlawful purposes including sovereign and individual fraud, drug trafficking, and tax evasion.

Süddeutsche Zeitung and ICIJ used Nuix software to process, index, and analyse the data. More than 400 journalists in 80 countries around the world then investigated the data, before publishing the first set of results on April 4, 2016.

Investigators used Nuix's optical character recognition to make millions of scanned documents text-searchable. They used Nuix's named entity extraction and other analytical tools to identify and cross-reference the names of Mossack Fonseca clients through millions of documents.

Nuix donated the software to *Süddeutsche Zeitung* and ICIJ for the purposes of the investigation. A Nuix consultant also advised the investigators on hardware configurations and workflows. Nuix employees never saw or handled any of the leaked data, that task was undertaken by the journalists involved in the investigation.

[nuix.com](https://www.nuix.com)



Eddie Sheehy, CEO Nuix. Image courtesy of Nuix.

Stratokey

StratoKey is a single point (gateway) for enterprises to secure an entire suite of cloud and SaaS applications.

As a cloud access security broker, StratoKey performs a number of tasks including access control, in-app encryption, monitoring (including audit capabilities), and behavioural analysis, and can institute defensive countermeasures as required. StratoKey can be deployed either on premise or in the cloud.

StratoKey delivers four distinct capabilities:

1. Encryption – both in-application field and attachment encryption. This encryption utilises either AES (256bit) or format preserving encryption. StratoKey also supports hybrid tokenisation and data masking.
2. Monitoring – providing real-time visibility into users' activities within cloud and SaaS applications. StratoKey compiles security profiles on each user passing through the StratoKey gateway and logs the user's access in its entirety.
3. Analytics – detecting security conditions triggered by robots, account hijacks, hackers and insider threats. The analysis engine also incorporates user behavioural analysis. This is designed to detect anomalies, outliers and security conditions and provides a strong foundation to defend against user credential theft.
4. Countermeasures – delivering an automated threat response engine with different rule sets for 'how' to respond to threats. StratoKey's countermeasures are flexible and can respond depending on threat severity, from blocking connections, through to dispatching second factor challenges.

StratoKey provides cloud encryption that automatically encrypts user data before it is transmitted to the cloud. This is in addition to user-level encryption and other compelling distinct technological capabilities, such as advanced user behaviour analytics, system visibility, breach detection and automated countermeasures to automatically thwart a breach.

StratoKey services a broad range of industries such as finance, healthcare, education and technology and is deployed in both small and large enterprise environments around the world.

stratokey.com



Image courtesy of Stratokey

Senetas

Senetas is a leading developer and manufacturer of high-assurance network encryption hardware. Senetas multi-certified encryptors provide maximum network security without compromising high-speed data networks' performance. They are trusted by the world's most security conscious organisations and leading global brands.

Senetas 'all-Australian' developed and built encryptors are supported and distributed globally by Gemalto – the world's leading data security company. They are used by governments and defence forces, commercial and industrial enterprises, and cloud, data centre and service providers in 30 countries. Customer support includes 24/7 high response service levels.

Certified by leading independent testing authorities - Common Criteria, FIPS, CAPS and NATO - Senetas encryptors are certified 'suitable for government and defence use'.

Senetas encryptors provide advanced high-assurance network encryption. They are used to protect cloud and data centre services; big data; government information; commercially sensitive intellectual property; citizen identity and privacy; defence and military secrets; business, financial data and banking transactions; data centre traffic and CCTV networks ; and critical industrial and infrastructure systems.

In the past, network encryption was important. Today those that take data security seriously demand high-assurance encryption. This ensures that a successful network breach only results in meaningless data reaching criminals' hands.

The critical elements of Senetas high-assurance network encryption are:

- secure and tamper-proof dedicated encryption hardware
- end-to-end 'gapless' network encryption
- state-of-the-art 'client-side' Encryption Key Management
- standards based and authenticated encryption.

Senetas high-assurance network encryption has recently been chosen to protect:

- European energy distribution from cyber-terrorists – attacks on the SCADA control systems that disrupt energy supplies
- global cloud computing services for national governments – protecting citizen privacy and government information
- international data center and cloud service provider networks - ensuring global customers' and stakeholders' Big Data protection
- national 'Digital City' networking of government agencies – protecting citizen privacy and data integrity.

senetas.com

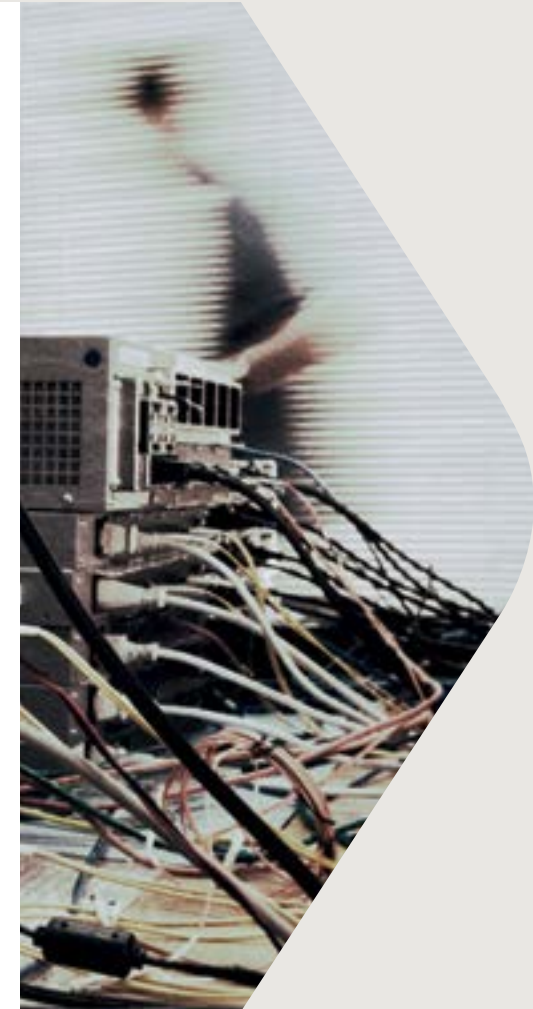


Image courtesy of Senetas

INTRODUCTION

> INDUSTRY OVERVIEW

INDUSTRY STRENGTHS

FURTHER INFORMATION

CONSULTING SERVICES

Australia has expertise in providing advice on cyber security, from large-scale consulting firms down to sole operators who possess deep knowledge of specific technical hardware or software systems. The focus is not only technical aspects such as network testing, security and penetration testing and security architecture, but also on protecting business assets such as reputation, IP, employees and customers.

For example:

- Acurus builds and integrates innovative products and services which are fully customised to an organisation's brand and service offering, providing clients with additional revenue streams.
- Bugcrowd uses an evolutionary approach to cyber security to bring together the world's largest crowd of independent security researchers with the most innovative companies.
- IDCARE, a national identity support service, assists individuals who believe their personal information has been put at risk. IDCARE also works with government and industry to independently assess their capacity to respond to contemporary and emerging identity theft and misuse risks.



Hivint

Hivint is a cyber security consulting firm. Growth is being driven by the Security Colony portal that provides tested security resources to help businesses combat the threat of hackers. The concept is simple; if a problem is discovered and solved in one organisation, it makes sense to make the answer available to other organisations so they can take immediate steps to protect their businesses from the same threat.

Information security is different to many facets of business competition - consumers don't want more secure and less secure businesses, they want every organisation to be sufficiently secure to protect their information and their assets. Consumers can then focus on price, quality, customer service and other more relevant attributes. SecurityColony.com is an Australian-first cyber security collaboration portal that specifically addresses this problem.

Such a 'shared challenge' arose within the Australian health insurance industry in response to changes to prudential regulation of the industry in 2015. All funds needed to refresh their Information Security Management Systems to align with the new

requirements, and needed tools and support to understand their gaps.

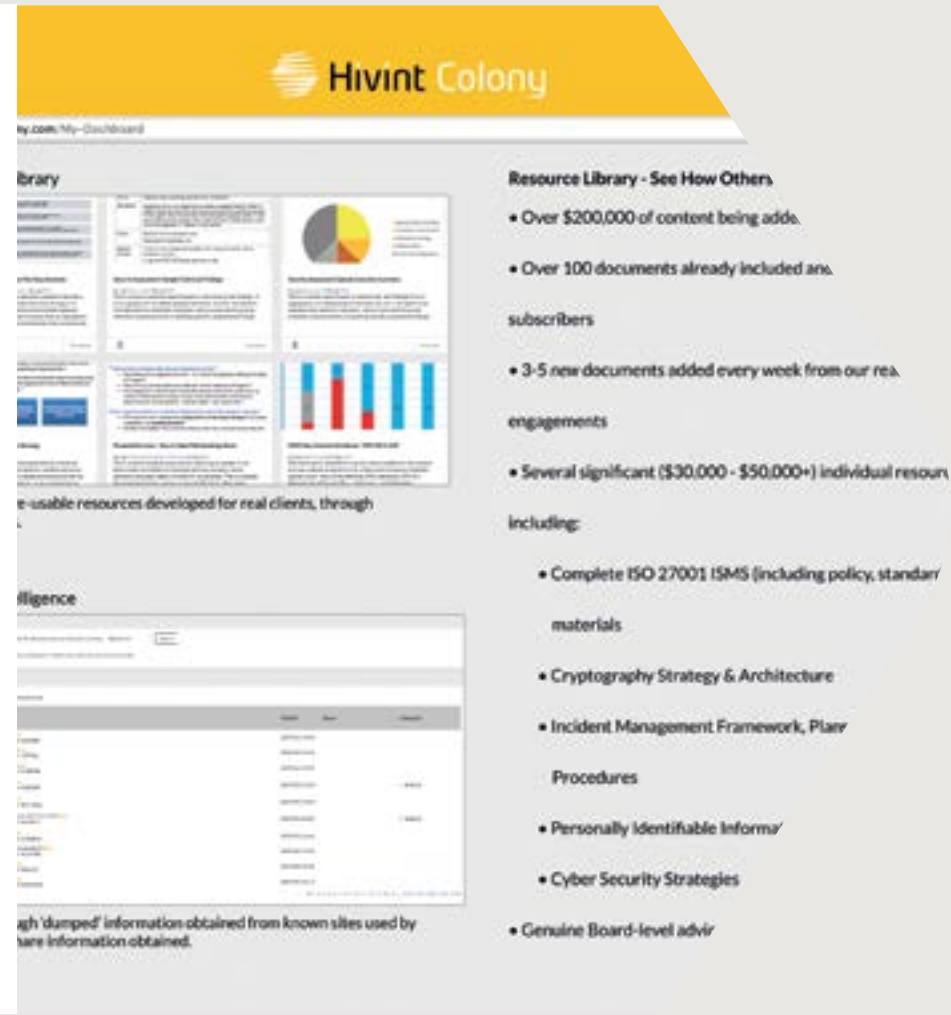
One of the largest health funds in Australia engaged Hivint to complete a series of gap analysis projects, which included the development of APRA-regulation-specific checklists and tools.

Another organisation engaged Hivint to complete the development of a full ISO 27001-based Information Security Management System incorporating APRA-specific requirements.

In each of these cases, the resulting material was made available via SecurityColony.com and a number of additional health funds then used these resources to fast track their own compliance programs, saving time and tens of thousands of dollars in consulting spend.

Improvements made by those organisations were then fed back to the original clients, so they too obtained a significant benefit from this process.

hivint.com



The screenshot displays the Hivint Colony website interface. At the top, there is a yellow header with the Hivint Colony logo. Below the header, the main content area is divided into several sections. On the left, there is a 'Resource Library' section with a list of documents and a pie chart. In the center, there is a 'Dashboard' section with a bar chart and a table of data. On the right, there is a 'Resource Library - See How Others' section with a list of resources and a table of data. The website is designed to provide a comprehensive overview of the security resources available to its members.

Image courtesy of Hivint

TriskeleLabs

As ongoing security breaches occur on a near daily basis, many organisations see an obvious need to conduct a penetration test. Many senior IT executives take this approach, the path of least resistance, as it delivers immediate reporting results. Unfortunately, this point-in-time exercise does not always meet the needs of technical staff, nor does it resolve the majority of risk.

Triskele Labs has worked with a number of organisations that are required to conduct penetration testing, and assisted them to incorporate additional security considerations.

One particular instance involved Triskele Labs working with a global building security provider to conduct penetration testing that not only identified issues, but ensured these were reviewed and remediated prior to testing being completed. This was achieved through a collaborative and ongoing partnership, rather than a one-off piece of work.

The teams came together to:

- conduct architecture reviews prior to penetration testing commencing
- keep in constant communication during testing
- conduct rolling iterative testing, as opposed to re-testing at completion
- reduce reporting by producing an executive summary.

This methodology provided the ideal outcome for the client, and all work fell under the banner of penetration testing. The project also expanded to include ongoing consulting and architecture reviews. This met the technical team's needs, while also providing a penetration testing report and outcome that was suitable for management.

The risk to the organisation was significantly reduced during testing, and Triskele Labs have since successfully rolled this methodology out to other clients.

triskelelabs.com



INTRODUCTION

> INDUSTRY OVERVIEW

INDUSTRY STRENGTHS

FURTHER INFORMATION

EDUCATION AND TRAINING SERVICES

Australian providers of cyber security education and training span the higher education sector, the vocational sector and private providers. Many Australian universities rank in the top 100 of global higher education indices, and are known for their teaching and research excellence. There is a wide range of coursework and research degrees, ranging from technical courses to those focussed on the environmental aspects of cyber security.

- Commonwealth Bank, Australia's largest provider of financial services, and the University of New South Wales (UNSW) have formed a partnership that aims to dramatically increase the number of Australian university students graduating with industry-relevant cyber security skills. Over the next five years, UNSW will roll out additional undergraduate subjects as a dedicated stream within Computer Science. The university has agreed to release the courses under Creative Commons licensing as massive open online courses (MOOCs). The partnership also funds the development of a cyber security teaching and research lab on UNSW's Sydney campus.

- Edith Cowan University offers a range of under-graduate and post-graduate cyber security degrees designed to meet the demand for cyber security professionals within government, law enforcement and industry.
- Optus Business and Macquarie University have joined forces to establish a multi-disciplinary Cyber Security Hub to help businesses and government recognise and protect themselves from increasing cyber threats. The new Optus Macquarie University Cyber Security Hub will provide research, courses and consultancy services to the private sector and government agencies.

It represents a \$10 million investment that will draw on the expertise of Optus, leading Macquarie University academics and industry experts to cover three areas; computing and IT, business and economics and security studies and criminology. It will focus on providing a holistic approach to cybercrime, how it is perpetrated, how it affects the economy and how it impacts policy.

The partnership includes degree programs, executive and business short courses, professional recruiting opportunities, thought leadership through cyber awareness events, and international engagement in areas such as intelligence, technology, criminology, finance and governance.

- IT Security Training Australia focuses on meeting the training needs of information security professionals. They use either leading providers of education in specialist areas or use their own experienced team of experts to develop the most current content.
- Box Hill Institute provides vocational training specialising in cyber security, designed to develop skills and knowledge for a career as a cyber security technician.

Centre for Internet Safety – University of Canberra

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security.

The Centre delivers actionable insights for governments, businesses and individuals. For example, the Centre recently undertook in-depth research and analysis on behalf of a global credit card scheme, evaluating various trust and safety issues for new products.

With a primary focus on training and education, the flagship product is the Graduate Certificate in Cyber Law and Policy, delivered through the Faculty of Business, Government and Law. Realising a deficiency in the global market for cyber security training and education focused at the executive level, this Graduate Certificate is very popular with students seeking to learn about the environmental aspects of the internet. Open to a broad range of national and international students, the Graduate Certificate allows students

to research strategic issues such as cyber security law, digital evidence, intelligence management and cybercrime investigations.

The Centre also provides a broad range of vocational training and education focused on cyber security, investigations, prosecutions and intelligence development for individuals, corporations and governments. For example, programs tailor-made for the banking and finance sector are delivered by experts and focus on:

- the impact of cybercrime on e-commerce, m-commerce and business viability
- the interaction between governments, businesses and consumers to reduce cybercrime and threats to cyber security
- policy and legal questions stemming from cybercrime and threats to cyber security.

canberra.edu.au/cis



Australian Centre for Cyber Security – University of NSW

The Australian Centre for Cyber Security (ACCS) at the University of New South Wales is a unique interdisciplinary research and teaching centre.

The ACCS operates across the full breadth of cyber security research and teaching (software, hardware, networks, payload, people, policy, law and the information ecosystem). It was created to capitalise on world class research in different aspects of the field involving some 60 scholars across the University of New South Wales. The Centre has working relationships with partners as diverse as Oxford University, Northrop Grumman, Cisco, (ISC)², the EastWest Institute, the Australian Army and the United States Navy.

One project underway, led by Dr Benjamin Turnbull, will increase the efficiency and ability of the Tor Network, a worldwide privacy network enabling legitimate anonymous communication. Tor has millions of daily users across the world and is used by diverse groups such as people seeking to evade government censorship, journalist sources, people evading geoblocking restrictions and anonymous online commerce systems. Dr

Turnbull recently received a significant grant from the US Naval Research Laboratory to address challenges for Tor Hidden Services.

The ACCS has developed both theoretical and practical responses to the unmet and rapidly developing education needs in cyber security. It delivers three Masters degrees embracing offensive cyber war and diplomacy, critical infrastructure dependencies, cyber adversary tradecraft and cyber terrorism.

Headquartered on the Australian Defence Force Academy Campus, the ACCS is taking a lead role in research on the future skills base for Australia's military forces. This includes development work on the idea of a National Cyber Security College, as well as working with international colleagues, through (ISC)², on worldwide curriculum development. ACCS also undertakes commissioned research for external clients, including development of serious games for cyber security.

unsw.adfa.edu.au/australian-centre-for-cyber-security



Image courtesy of University of New South Wales

INTRODUCTION

INDUSTRY OVERVIEW

> INDUSTRY STRENGTHS

FURTHER INFORMATION

ATTRACTIVE INVESTMENT LOCATION

A number of international cyber security organisations have made significant investments recently in Australia.

They are leveraging the investment-friendly environment, the world-class talent and expertise, the national approach to strategy, research and Government support and Australia's proximity to Asia. Australia has also become home to a broad range of global IT organisations who recognise the attractiveness of Australia as an investment destination.

For example:

- CSC has acquired the Dalmatian Group, a Canberra-based information and security consultancy, in a move the company says will strengthen its leadership position in the cyber security market for the Australian Government.
- Cylance, a US-based IT security company, has opened an office in Australia to tackle the Asian market, promising a radical new approach to endpoint security.
- Zscaler, a cloud-based security vendor, has made a significant investment into the Asia Pacific and Japan, using Australia as its anchor market.
- Singtel Optus, a telecommunications provider, has teamed up with Sydney's Macquarie University to establish the Cyber Security Hub to support the public and private sector.
- NEC Corporation, together with NEC Australia, has announced plans to establish a Global Security Intel Centre (GSIC) in Adelaide, Australia to address growing global demand for cyber security. The GSIC will aim to enable the adoption of more efficient business models that translate into new opportunities. In addition, NEC Australia and the University of Adelaide have agreed to collaborate on a Smart Cities project that will help accelerate smart, dynamic, secure and sustainable cities.
- IBM has unveiled plans for a new Australian National Cyber Security Centre in Canberra. The new Centre will connect Australia with IBM's global network of over one dozen security operations centres, providing on-the-ground access for the government and private sectors to IBM's security technology and expertise.
- Dimension Data and Deakin University, with support from LaunchVic, will set up a cyber security incubator in order to accelerate the development of unique cyber security solutions and intellectual property.



INTRODUCTION

INDUSTRY OVERVIEW

› INDUSTRY STRENGTHS

FURTHER INFORMATION

MATURE NATIONWIDE APPROACH TO CYBER DEFENCE

The establishment of what is now the Australian Cyber Security Growth Network (ACSGN) was announced in December 2015, as part of the Government's National Innovation and Science Agenda. The ACSGN will provide strategic coordination of a national cyber security innovation network (see box).

In addition, the Australian Prudential Regulation Authority ensures Australia's financial institutions are well-educated and well-informed about the risks of cyber attacks. The regulator seeks confirmation that institutions have strategies and plans to address evolving forms of cyber risk, through a systematic approach to managing and securing operating systems and software.

Industry, academia, universities and research organisations also play a vital role in development within the sector. For example CSIRO's Data61, the largest data innovation group in Australia, and the Australian Institute of Company Directors have announced a joint commitment to focus on the digital and cyber literacy of directors and boards across Australia.

GOVERNMENT SUPPORT AND INITIATIVES

Australian Cyber Security Growth Network (ACSGN)

In recognition of cyber security's importance, the Australian Government's A\$1.1 billion National Innovation and Science Agenda (NISA) has allocated A\$30.5 million to an industry-led Australian Cyber Security Growth Network, in order to help grow and strengthen Australia's cyber security industry.

The ACSGN will support the development of a vibrant and globally competitive Australian cyber security industry aimed at enhancing Australia's future economic growth. To achieve this, the ACSGN will bring together industry, researchers

and governments to work together to identify industry priorities and coordinate cyber security research and innovation.

Specifically, the ACSGN will:

- demonstrate leadership and coherence in cyber security
- drive collaboration and coordination in the industry
- accelerate commercialisation of cyber security technologies
- facilitate talent growth
- pursue policy advocacy and reform as it relates to cyber security.

innovation.gov.au/page/cyber-security-growth-centre

Cyber Security Strategy

The Australian Government's Cyber Security Strategy establishes five themes of action for Australia's cyber security to 2020²:

- a national cyber partnership
- strong cyber defences
- global responsibility and influence
- growth and innovation
- a cyber smart nation.

Each theme is supported by actions the Government will take to improve cyber security. Recognising that cyberspace is dynamic, the Strategy's initiatives will be reviewed and updated annually and the Strategy reviewed and updated every four years.

cybersecuritystrategy.dpmc.gov.au



INTRODUCTION

INDUSTRY OVERVIEW

> INDUSTRY STRENGTHS

FURTHER INFORMATION

Department of Defence

The Department of Defence has announced a Next Generation Technologies Fund³ of around A\$730 million (over the decade to FY 2025–26) to be invested in strategic next generation technologies that have the potential to deliver game-changing capabilities, such as cyber and quantum technologies. Defence will build collaborative programs with academia, publicly funded research agencies, industry (particularly small to medium enterprises), and Australian allies to create a vibrant and interlocking research and innovation capability that is focused on driving defence outcomes.

Examples of priority areas of work for the Fund, as identified in the Integrated Investment Program, include integrated intelligence, surveillance and reconnaissance; space capabilities; multidisciplinary material sciences; quantum technologies; trusted autonomous systems; cyber; and advanced sensors.

R&D Tax Concession

Businesses can take advantage of Commonwealth Government schemes such as the Research and Development (R&D) Tax Incentive – providing broad-based, market-driven assistance for all industries. It provides a targeted tax offset to encourage more companies to engage in R&D⁴

WORLD-CLASS RESEARCH BASE

The work of Australian cyber security researchers is internationally respected, and research focuses on new technologies and approaches which support the nation's cyber security. This includes discovery and understanding of vulnerabilities, threats and their impacts, enabling improved risk-based decision making, resilience and effective responses to cyber intrusions and attacks. Australia ranks fourth globally in patent filings in cyber security research and development, with activity including distributed computing and packet switching technology.⁵

A research team at the University of Sydney has made a major breakthrough in generating single photons (light particles) as carriers of quantum information in security systems. The team developed secure passwords which can only be broken by violating the laws of physics. The ability to generate single photons, which form the backbone of technology used in laptops and the internet, will drive the development of local secure communications systems.

CSIRO's Data61 is utilising advanced capabilities in software systems, machine learning, networks and optimisation to develop software systems that are inherently more robust, trustworthy and resilient to emergent

cyber threats (see case study on page 7). Other examples include the Australian Cyber Security Research Institute, which brings together a collaborative network of researchers, universities, government and industry partners nationwide. Also, Federation University is creating knowledge and tools for the development of simple, safe and secure environments to support the continued uptake of internet commerce and identity management.



INTRODUCTION

INDUSTRY OVERVIEW

> INDUSTRY STRENGTHS

FURTHER INFORMATION

INTERNATIONAL COLLABORATIONS

Australia is an influencer and driver of change at the international level. The Commonwealth Government participates in relevant United Nations and regional forums and partners with a number of countries on cyber issues and reforms. Australia's national Computer Emergency Response Team (CERT) currently chairs the steering committee of the Asia Pacific Computer Emergency Response Team (comprising 28 teams from 20 economies across the region) and shares threat information with other response teams around the world.

The Australian Strategic Policy Institute – International Cyber Policy Centre brings together the various Australian Government departments with a responsibility for cyber issues, along with a range of private sector partners and creative thinkers, to help create constructive cyber policies both at home and abroad. The Centre aims to facilitate conversations between government, private sector and academia across

the Asia Pacific to increase dialogue on cyber issues and create a common understanding of the issues and possible solutions in cyberspace.

Flinders University has established an academy with Cisco to benefit students studying for ICT degrees. Cisco Networking Academy is a global IT skills and career building program for learning institutions and individuals. More than 5.5 million people have joined the Networking Academy since 1997. Cisco staff will train Flinders students to work with new technologies and digital innovations, including cyber security. Students can undertake the training while still studying their ICT degrees.

CSIRO's Data61 is partnering with Cyber London (CyLon), Europe's first cyber security accelerator and business incubator, to strengthen cyber collaboration between Australia and the United Kingdom. A Memorandum of Understanding signed by the two parties aims to accelerate cyber innovation in both Australia and the UK by providing expertise, resources and capital to enhance the growth of this sector.

The Defence Science and Technology Group has a joint action plan with the United States Department of Homeland Security for the cyber security of critical infrastructure. The joint action plan is part of a Science and Technology Treaty and includes distribution of IMPACT resources (Information Marketplace for Policy and Analysis of Cyber-risk and Trust dhs.gov/csd-impact) for cyber security researchers.



INTRODUCTION

INDUSTRY OVERVIEW

> INDUSTRY STRENGTHS

FURTHER INFORMATION

WORLD-CLASS TECHNICAL SKILLS AND EXPERTISE

Many of Australia's cyber security professionals are active members of key international associations, such as the Information Systems Audit and Control Association (ISACA), the SANS Institute, the International Information Security Systems Certification Consortium (ISC)², the Open Web Application Security Project (OWASP) and the Council of Registered Ethical Security Testers (CREST). These associations hold training and education as well as conducting certifications in the Australian market.

Global security companies who have set up technical operations in Australia to access a skilled workforce include:

- Akamai Technologies, a cloud services provider, that has opened a data center as part of its global expansion strategy. The company's 'scrubbing centre' leverages a cloud-based approach to mitigate threats without causing significant business disruption

- Context Information Security, a company that provides holistic and product-agnostic security services based on the technical skills, professionalism, independence and integrity of their consultants
- iSight Partners, a cyber threat intelligence organisation. iSight Partners have launched a threat intelligence centre to better serve customers in the Asia-Pacific region
- NCC Group, a global information assurance specialist, provides organisations worldwide with expert escrow, verification, security consulting, website performance, software testing and domain services
- Ping Identity, a global identity vendor, has opened a data centre in Australia to meet growing demand in the Asia-Pacific region from government and enterprise clients. This data centre adds to existing facilities in Germany and the United States.



INTRODUCTION

INDUSTRY OVERVIEW

INDUSTRY STRENGTHS

> FURTHER INFORMATION

Australian Information Industry Association (AIIA)

The AIIA is Australia's peak representative body and advocacy group for those in the digital ecosystem.

Since 1978 the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for its members and to contribute to Australia's economic prosperity.

The AIIA do this by providing a strong voice of influence; building a sense of community through events and education; enabling a network for collaboration and inspiration; and developing compelling content and relevant information.

aiaa.com.au

Australian Computer Society (ACS)

The ACS is the association for Australia's information and communications technology (ICT) profession. The ACS represents all ICT practitioners in business, government and education.

Its role is to help members realise their professional ambitions, making the most of an era of extraordinary possibility. The ACS is passionate about recognising professionalism, developing ICT skills and creating a community with a true sense of belonging.

It is committed to advancing the ICT industry as a whole and upholding the highest standards of professional conduct through its Code of Ethics.

acs.org.au

Australian Information Security Association (AISA)

As a nationally recognised not-for-profit organisation and charity, the AISA champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the public as well as businesses and governments in Australia.

Established in 1999, AISA has become the recognised authority on information security in Australia with a membership of over 3,000 individuals across the country. AISA caters to all domains of the information security industry with a particular focus on sharing expertise from the field at meetings, focus groups and networking opportunities around Australia.

AISA's vision is a world where all people, businesses and governments are educated about the risks and dangers of cyber attack and data theft, and to enable them to take all reasonable precautions to protect themselves. AISA's strategic plan calls for continued work in the areas of advocacy, diversity, education, and organisational excellence.

aiaa.org.au

CREST Australia New Zealand Ltd

A not-for-profit company limited by guarantee, CREST Australia New Zealand runs the Council of Registered Ethical Security Testers on behalf of member companies. It provides assessment, accreditation, certification, education and training in cyber and information security for individuals and corporate entities, and promotes the provision of high quality, best practice information security services according to its company constitution.

A CREST approved organisation ensures work will be carried out by qualified individuals with up-to-date knowledge of the latest vulnerabilities and techniques used by real attackers, backed up by appropriate methodologies for the secure storage and protection of data.

The CREST scheme is comprised of two tracks: company accreditation and individual tester certification. This provides two layers of assurance that the penetration tester is capable of understanding each unique security posture, leading to the best recommendations on security improvements.

crestaustralia.org

REFERENCES

1. Australian Government. Cybersecurity – Capability Statement
science.gov.au/scienceGov/ScienceAndResearchPriorities/Pages/Cybersecurity.aspx
2. Australian Government. Australia's Cyber Security Strategy – enabling innovation, growth & prosperity
cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
3. Australian Government. 2016 Defence Industry Policy Statement
defence.gov.au/whitepaper/Docs/2016-Defence-Industry-Policy-Statement.pdf
4. Australian Government. Research and Development Tax Incentive
business.gov.au/assistance/internal-assistance/research-and-development-tax-incentive
5. LexInnova. Network Security - Overview of patent out-licensing opportunities
lex-innova.com/wp-content/uploads/2016/02/LexInnova-Network-Security-616-1.pdf





The Australian Trade and Investment Commission – Austrade – contributes to Australia’s economic prosperity by helping Australian businesses, education institutions, tourism operators, governments and citizens as they:

- develop international markets
- win productive foreign direct investment
- promote international education
- strengthen Australia’s tourism industry
- seek consular and passport services.

Austrade helps companies around the world to identify and take up investment opportunities in Australia as well as to source Australian goods and services.

Our assistance includes:

- providing insight on Australian capabilities
- identifying potential investment projects and strategic alliance partners
- helping you to identify and contact Australian suppliers.

W austrade.gov.au

E info@austrade.gov.au



austrade.gov.au



Australian Government
Australian Trade and Investment Commission

