COMMERCIAL IN CONFIDENCE

FINAL REPORT

Impact Analysis of CSIRO Cybersecurity Research

Prepared for
CSIRO

August 2020

THE CENTRE FOR INTERNATIONAL ECONOMICS
www.TheCIE.com.au

The Centre for International Economics is a private economic research agency that provides professional, independent and timely analysis of international and domestic events and policies.

The CIE's professional staff arrange, undertake and publish commissioned economic research and analysis for industry, corporations, governments, international agencies and individuals.

CANBERRA
Centre for International Economics
Ground Floor, 11 Lancaster Place
Canberra Airport ACT 2609

Telephone +61 2 6245 7800
Facsimile +61 2 6245 7888
Email cie@TheCIE.com.au
Website www.TheCIE.com.au

SYDNEY
Centre for International Economics
Level 7, 8 Spring Street
Sydney NSW 2000

Telephone +61 2 9250 0800
Email ciesyd@TheCIE.com.au
Website www.TheCIE.com.au

Contents

BOXES, CHARTS AND TABLES

Summary

CSIRO's Data61 (Data61) Cybersecurity represents an exemplar in CSIRO research: clear causal links between research excellence, and meeting the specific needs of government and industry to address large scale challenges and avoid potentially large scale societal and economic costs.

The impact pathway identifies clear links between collaborative, capability, and capacity building activities; new technologies and solutions with immediate and wider application; and an ability to unlock significant digital, data and Artificial Intelligence capabilities to boost productivity and growth.

Addressing problems that otherwise pose significant risks to Australia

Global connectivity poses a major challenge to the protection of privacy and trust, with costly disruptive potential, with US$170 billion[1] spent globally to minimise cybersecurity risks.

At its most severe, cybersecurity incidents cost are estimated to cost the Australian economy up to $1 billion per year.[2] Australian sectors most reliant on cyber connectivity generate annual gross revenue of more than $500 trillion, and account for nearly 670 000 Australian jobs. For these sectors, the loss in GDP from one week of cyber downtime due to cyber invasion is estimated at $5.6 trillion, with a loss of 32 000 jobs.[3]

Levels of risk and cost need to be addressed, as businesses and governments rely on accurate and thorough data to protect their information and digital assets. This is complex, with cyber risk assessment challenged by fast-evolving threats and data limitations, which are difficult to address when organisations are unwilling to share relevant information, and/or are unaware of their vulnerabilities to data loss and privacy-invasive actions.

---

[1] Cybersecurity Ventures, 'Cybersecurity Market Report Q4 2015', *Cybersecurity Ventures*, 2015, <https://cybersecurityventures.com/cybersecurity-market-report-q4-2015/>, accessed 27 July 2020

[2] Actual report cannot be sourced in the public domain. References to the estimate have most recently reported in Australian Criminal Intelligence Commission, 'Cybercrime', *Australian Criminal Intelligence Commission*, 2019, <https://www.acic.gov.au/about-crime/organised-crime-groups/cybercrime>, accessed 3 June 2020.

[3] AustCyber, 'Australia's Digital Trust Report 2020', AustCyber, July 2020, <https://www.austcyber.com/resource/digitaltrustreport2020>, accessed 30 July 2020

Solution: build resilience, shared awareness, and human capacity

Since 2016, CSIRO's Data61 has been undertaking a range of initiatives to boost research, commercialisation and connectivity outcomes across Australia's cyber industry, and drive the development of new cybersecurity architectures. The cybersecurity program now includes over 47 activities across focused cyber themes, including:

- boosting cyber security research and collaboration
- cyber ecosystem activities
- commercialisation of cyber solutions
- improving Cyber Security Skills, and
- deepening connections with international partners.

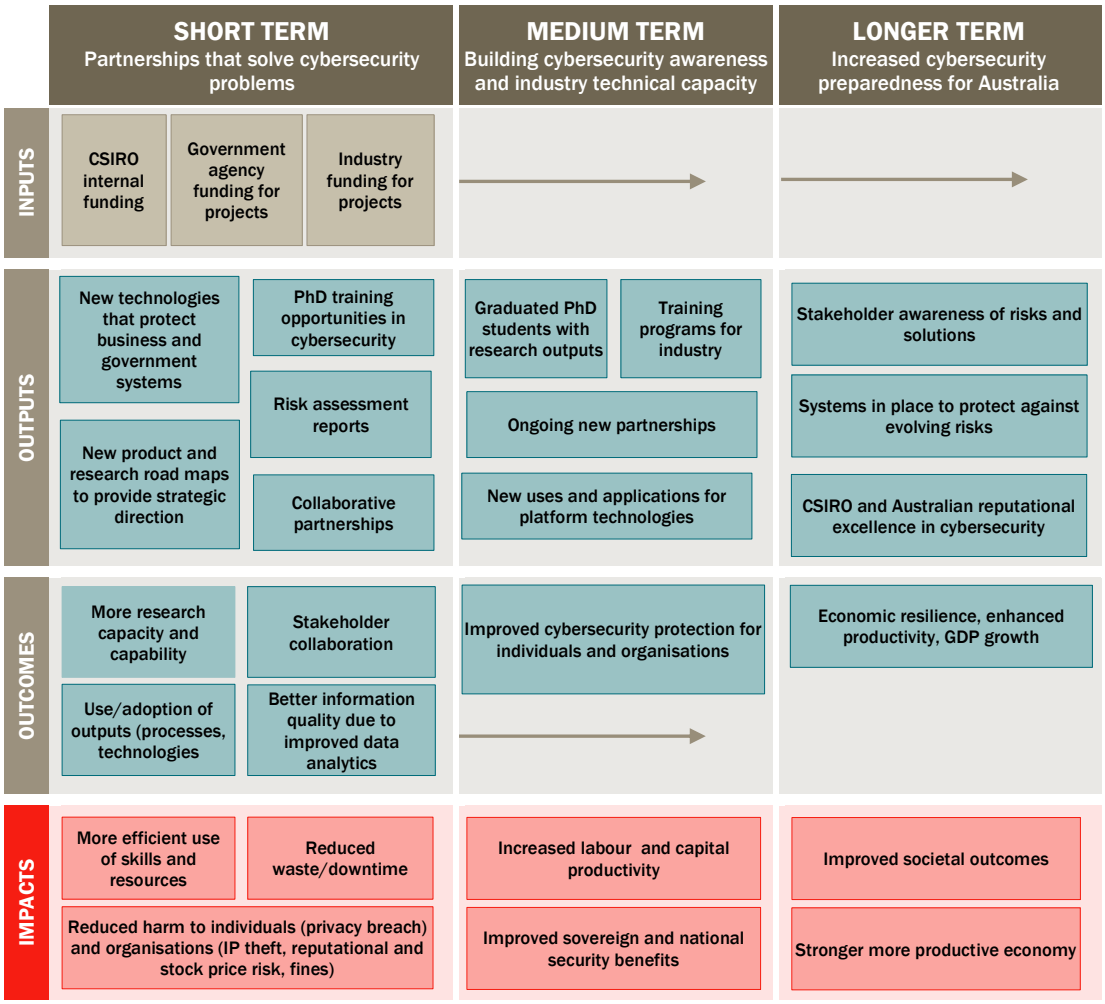
Over 60 cybersecurity researchers and engineers have been funded to support projects to improve cyber research and technology commercialisation over the past three years. Between FY2018 and FY2020, $33.8 million in funding has been invested by CSIRO in its three major cyber security groups within the Software and computational Systems (SCS) research program.[4] These groups have delivered new platform technologies and associated products that are actively being trialled and adopted by researchers, industry, and all levels of government, in Australia and internationally. Key outputs of the team include:

- novel science and technological solutions
- new partnerships and collaborations
- risk assessments for government to improve preparedness and response to cyber attack
- leadership and guidance forums and materials for cyber initiatives
- new training and development opportunities, and
- elevated CSIRO and Australia's international reputation.

The impact pathway for CSIRO Cybersecurity expands from impacts associated with discrete technology partnerships to changes in the cyber security system and capacity in Australia. An overview of its multidimensional nature is illustrated below.

[4] Trustworthy Systems, Distributed Systems Security, and Information Security and Privacy. Includes salary, on-costs and operating costs.

1 Multidimensional impact pathway for CSIRO Cybersecurity



Source: CIE.

Valuing Data61 Cybersecurity

In its short history, Data61 Cybersecurity has enhanced CSIROs contribution to Australia's cybersecurity innovation and protection, leveraged additional government and industry investment, and brought stakeholders together to achieve more through collaboration and dispersion of cybersecurity capacity building than would have been achieved otherwise.

This includes leveraging substantial investment into Australia's cybersecurity preparedness, with numerous contracts with clients to provide commissioned work to address industrial and agency needs. Over 2018-2020, contracted revenue for the three cyber groups has amounted to 27.9 million in nominal terms. With additional cybersecurity-related funding for Data61 from the National Innovation and Science Agenda (NISA) of $19.8 million over three years allocated to the three cyber groups, this results in all cyber groups covering their labour and overhead costs, and generating additional research capacity for CSIRO. Across the three cyber groups, a cost recovery

rate of 178 per cent is achieved, ranging from 115 per cent for Trustworthy Systems to 235 per cent for Distributed Systems Security.

The public dissemination of publications from the research team have been embraced globally, generating an estimated $844 000 annually as works are cited by the cybersecurity research community.[5]

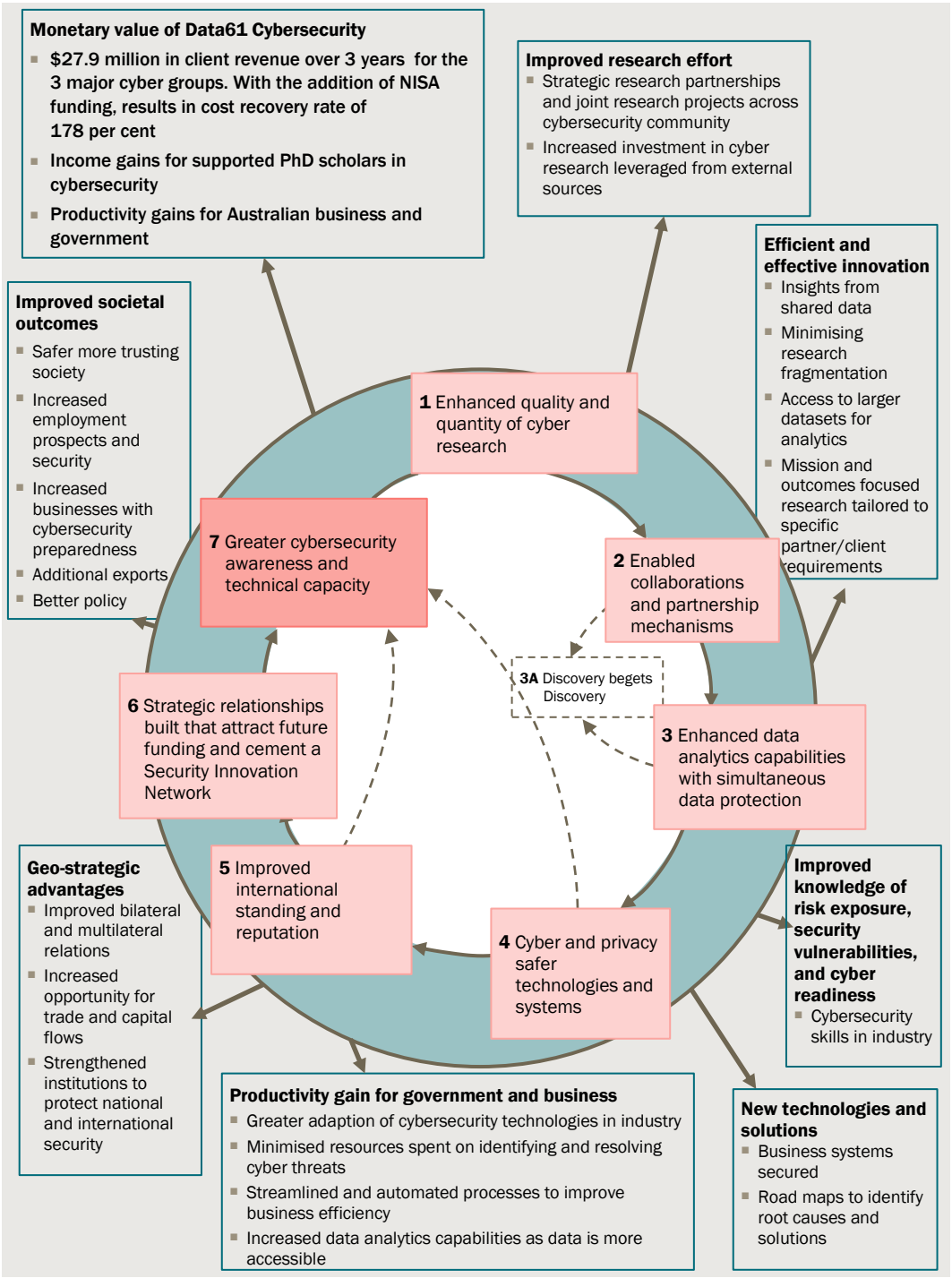
Data61's Cybersecurity groups are still in their infancy, and growing as fast as their staff capacity can sustain. With the PhD scholarships program and upskilling of industry, cybersecurity capacity will grow, and with it, demand from government and industry to improve cybersecurity preparedness across the country.

The rapid uptake of demand for cybersecurity expertise, and the leveraged commitment to substantial funding of research points to a research program that is highly valued on multiple fronts, with the capacity to materially impact on the resilience of the Australian economy.

The logic of the impact creation model for Cybersecurity is illustrated in chart 2.

[5] Calculated by the CIE, as described later in this report.

2 Key outcomes and impacts of Data61's Cybersecurity programs



Data source: CIE.

1 Challenges and risks

Since 2016, CSIRO's Data61 (or Data61) has been a driving catalyst in Australia's cyber research agenda, and is already beginning to realise Australia's potential to be a regional and global leader in cyber research and technology commercialisation.

Its approach is highly collaborative, including partnerships with Australian and international governments, companies, universities, and networks to bring the best minds and mission-driven solutions to Australian needs and challenges, and ensure Australian governments and companies have early access to emerging technologies and capabilities.

Research investments are being made across cyber-aligned fields including trustworthy systems, distribution system security, data security and privacy, AI and cyber security, and human central cyber security to demonstrate at scale the use of new cyber techniques and architectures in the local environment.

What's at stake

Global connectivity facilitated by information and digital technologies brings enormous opportunities for business and society. However, it also represents a major challenge to the protection of privacy and trust, and has the potential to destabilise, disrupt and corrupt information systems and infrastructure at a large economic and social cost.

The 2018 Symantec Security Response estimated that globally there are an average of 5200 Internet of Things attacks per month.[6] In early 2018, Meltdown and Spectre put industry on global alert of an in-built insecure default that allows attackers to bypass security control and steal data if exploited.[7] Data61 had played in integral role in discovering Spectre and Foreshadow, a variant of Meltdown that bypassed Intel's secure vault to expose data.[8]

---

6 Davis, D., 'Internet of Things Cyber Attacks Grow More Diverse', *Symantec-enterprise-blogs*, 2019, <https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/istr-2019-internet-things-cyber-attacks-grow-more-diverse?om_ext_cid=biz_social3_AMS_NAM-IV_twitter_>, accessed 6 June 2020.

7 Australian Cyber Security Centre, 'ACSC statement on reports of Intel Active Management Technology (AMT) security issue', *Australian Signals Directorate*, 2018, <https://www.cyber.gov.au/news/acsc-statement-on-reports-of-intel-active-management-technology-security-issue>, accessed 6 June 2020.

8 Chelvan, C., 'Foreshadowing attacks: cybersecurity researchers save the day', *CSIRO scope*, Aug 2018, <https://blog.csiro.au/foreshadowing-attacks-cybersecurity-researchers-save-the-day/>, accessed 10 Aug 2020

A 2019 report by Dell Computing found that of 307 companies suffered hardware breaches, 52 per cent experienced loss of sensitive data, 39 per cent incurred financial loss due to system downtime, and 32 per cent suffered financial loss due to remediation efforts.[9]

In Australia, the Office of Australian Information Commissioner 2018 report on Australian data breaches found nearly 25 per cent of data breaches occurred in the health sector, which is highly vulnerable to re-identification risk and thereby significant financial and reputational ramifications.[10]

To assess Australia's exposure to health data risks, researchers from the University of Melbourne successfully re-identified the longitudinal medical billing records of 10 per cent of Australians, equivalent to around 2.9 million people to demonstrate the relative ease in re-identifying Australian patient medical data without permission using an undergraduate-computing-level skill set.[11]

Given these challenges, Australian and international demand for cybersecurity solutions is strong, with an estimated US$170 billion spent globally to minimise cybersecurity risks.[12]

Costs of cyber intrusion and risks

Cyber intrusion has a direct deleterious economic impact, typically associated with denial of service assaults and malicious insiders.

The 2019 Australian Cyber Security Review found that cybersecurity incidents cost the Australian economy up to $1 billion per year.[13] In 2020, it was estimated that Australian sectors most reliant on cyber connectivity generate annual gross revenue of more than $500 trillion, and account for nearly 670 000 Australian jobs.[14] For these sectors, the loss

---

9 Forrester Consulting, 'BIOS Security – The Next Frontier for Endpoint Protection Report', *Dell Technologies*, 2019, < https://www.dellemc.com/ja-jp/collaterals/unauth/analyst-reports/solutions/dell-bios-security-the-next-frontier-for-endpoint-protection.pdf>, accessed 6 June 2020.

10 The Office of Australian Information Commissioner, 'Notifiable Data Breaches Statistics Report: 1 January to 31 March 2018', *OAIC Notifiable data breaches*, July 2018, < https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-january-to-31-march-2018/>, accessed 4 June 2020

11 Culnane, C., Rubinstein, B., and Teague, V., 'Health Data in an Open World', *Corenell University arXiv Organisation*, 2017, <https://arxiv.org/ftp/arxiv/papers/1712/1712.05627.pdf>, accessed 6 June 2020.

12 CSIRO Data61 Cyber Security Strategy, 2019, p 1

13 Actual report cannot be sourced in the public domain. References to the estimate have most recently reported in Australian Criminal Intelligence Commission, 'Cybercrime', *Australian Criminal Intelligence Commission*, 2019, <https://www.acic.gov.au/about-crime/organised-crime-groups/cybercrime>, accessed 3 June 2020.

14 AustCyber, 'Australia's Digital Trust Report 2020', AustCyber, July 2020, <https://www.austcyber.com/resource/digitaltrustreport2020>, accessed 30 July 2020

in GDP from one week of cyber downtime due to cyber invasion is estimated at $5.6 trillion, with a loss of 32 000 jobs. Worse still, the rate of losses accelerates as the period of cyber downtime extends (table 1.1).

1.1 Potential economy-wide impact of digital disruptions

Sector	1-week attack		4-week attack	
	GDP ($m)	Jobs	GDP ($m)	Jobs
Digital activity	-4 965	-27 174	-29 788	-163 042
Cyber security	-283	-1 541	-1 700	-9 248
Online retail	-290	-2 690	-2 002	-18 558
Digital health	-27	-189	-174	-1 202
Solar power generation	-10	-43	-63	-281
Space industry	-27	-178	-178	-1 189
Hydrogen manufacturing	-0.16	-1	-1	-5
Total	**-5 602**	**-31 816**	**-33 906**	**-193 525**

Note: Note that the scenarios were designed in terms of timescale only.

Source: AustCyber, 'Australia's Digital Trust Report 2020', AustCyber, July 2020, <https://www.austcyber.com/resource/digitaltrustreport2020>, accessed 30 July 2020

International studies that publish more specific data on cybersecurity costs tend to report lower costs, albeit still substantive, and are of major concern for Australia and internationally. The Ninth Annual Cost of Cybercrime Study estimated that the average annual cost to a country from cyberattacks is US$13 million. The most costly type of attack is from malware (US$2.6 million annually), and the most costly consequence was to business disruption (US$4 million annually), mainly due to denial of service (table 1.2).

1.2 Annual average cost of the consequences of cyberattacks

	Business disruption	Information loss	Revenue loss	Equipment damage	Total cost by attack type
	US$2019	US$2019	US$2019	US$2019	US$2019
Malware	0.5	1.4	0.6	0.1	2.6
Web-based attacks	0.3	1.4	0.6		2.3
Denial of service	1.1	0.2	0.4	0.1	1.7
Malicious insiders	0.6	0.6	0.3	0.1	1.6
Phishing and social engineering	0.4	0.7	0.3		1.4
Malicious code	0.2	0.9	0.2		1.4
Stolen devices	0.4	0.4	0.1	0.1	1.0
Ransomware	0.2	0.3	0.1	0.1	0.7
Botnets	0.1	0.2	0.1		0.4
Total cost by consequence	**4.0**	**5.9**	**2.6**	**0.5**	**13.0**

Note: Numbers may not add due to rounding.

Source: Bissell, K., and Lasalle, R., 'Ninth Annual Cost of Cybercrime Study', *Accenture Security North America*, 2019, <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>, accessed 4 June 2020.

Across all countries, the total value at risk from cybercrime is estimated to be US$5.2 trillion over the next five years, based on value at risk globally from direct and indirect cyberattacks over the 2019-2023 period.

The IBM Security Cost of a Data Breach Report in 2019 found that the probability of experiencing a data breach over two years was 29.6 per cent, which has increased by close to a third over the past five years.

The reported average cost of a data breach is US$3.92 million, with an average breach size of 25 550 records, and the average time to identify and contain a breach being 279 days (314 days when caused by malicious attack).[15]

Average costs are 95 per cent higher in an organisation where there is no security automation deployed, and in Australia (as is the international average) 48 per cent of organisations do not have security automation deployed. A comparison of costs for Australia vis-à-vis the global average are summarised in table 1.3.

Not captured in these estimates are the financial costs associated with risks to assurance of underlying service reliability for life–or mission–critical systems or functions.

For instance, in 2017, the US Food and Drug Administration identified that many medical devices – including St. Jude Medical's implantable cardiac devices – contain configurable embedded computer systems that are unsafe from cyber invasions and exploits. Malfunctions such as battery depletion and incorrect pacing or shocks, due to intrusion into such a life-critical system, can cause devastating injury or even death.[16]

1.3 Summary of data insights from the 2019 Cost of a Data Breach Report

	Australia	Global average
Average cost of a data breach	US$2.13 million	US$3.92 million
Average cost of a data breach that takes more than 200 days to resolve	Not reported	US$4.56 million
Average cost of a data breach that takes less than 200 days to resolve	Not reported	US$3.34 million
Average cost of a megabreach (more than one million records)	Not reported	US$3.92 million
Average cost per record breached	US$110	US$150
Direct expenses	US$50	Not reported
Non cash outlays needed for breach resolution	US$60	Not reported
Cost per health record breached	US$429	US$645

Source: IBM Security, 'IBM Security Cost of a Data Breach Report 2019', *IBM*, 2019, < https://www.ibm.com/security/data-breach>, accessed 5 June 2020

15 IBM Security, 'IBM Security Cost of a Data Breach Report 2019', *IBM*, 2019, < https://www.ibm.com/security/data-breach>, accessed 5 June 2020.

16 U.S. Food & Drug Administration, 'Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication', *2017 Safety Communications*, 2017, <https://www.fda.gov/medical-devices/medical-device-safety/safety-communications>, accessed 3 June 2020.

There are also high potential risks of cyberattacks to embedded systems.

Complex in nature, embedded systems are typically used in automobiles, mobile phones, industrial machines and medical equipment. For example, embedded systems in consumer vehicles entail cruise control, backup sensors, suspension control and airbag systems, hence cyber invasion can have potentially severe consequences.

In 2015, trial research showed vulnerability of the Jeep SUV being hacked via its Sprint cellular network, with attackers able to gain full control of entire vehicles with speedup, slowdown and veer-off.[17]

The immediate adverse impacts of untrustworthy systems include software defects, system failure, leakage of sensitive information, financial costs, and in embedded systems, damage to property, injury, or loss of life.

Immediate financial costs include user incidents and repair costs for bugs, and costs associated with delayed service introduction.

Longer term costs include the development or exacerbation of:

- loss of reputation and future business
- legal actions
- injuries and fatalities
- crime
- loss of employment, and
- loss of public service and essential services.

Need for risk management capability and governance

Faced by emerging cyber threats with evolving scope, scale and sophistication, the 2020 Cyber Security Strategy Industry Advisory Panel outlined key strategic priorities and identified best practice from an industry perspective. The 2020 Cyber Security Strategy is clear-sighted about opportunities and barriers on cyber risk management, development of trustworthy digital market, and shared awareness of cyber treat. In particular, the 2020 Strategy recommends[18]:

- to develop treat-identifiers for a digital technology market where security is built in across the supply chain, leveraging Australia's global leadership in cyber policy development, as well as support by major national agencies – the CSIRO and Defence Science and Technology.
- to increase investment in cyber security research and development

---

17 Bonderud, D., 'Eight Crazy Hacks: The Worst and Weirdest Data Breaches of 2015', *Security Intelligence*, 2015, < https://securityintelligence.com/eight-crazy-hacks-the-worst-and-weirdest-data-breaches-of-2015/>, accessed 3 June 2020.

18 2020 Cyber Security Strategy Industry Advisory Panel, 'Industry Advisory Panel Report for Australia's 2020 Cyber Security Strategy', Department of Home Affairs of Australian Government, July 2020, <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf>, accessed 30 July 2020

- to improve collaboration with the cyber industry to shape cyber security standards and align market-wide practise with a transparent and secure digital supply chains
- to promote partnerships between the institutions and the industry to share real-time treat information for preparedness.

Hence, levels of risk and cost need to be incorporated into a cybersecurity risk management and government framework, as businesses and governments rely on accurate and thorough information to protect their information assets. Despite its importance, a comprehensive cyber risk assessment is challenged by fast-evolving threats and data limitations. One important constraint is the ability to assess the probability and cost of a security incident when organisations are unwilling to share relevant information, and/or are unaware of their vulnerabilities to data loss and privacy-invasive actions.[19]

Part of a successful cyber defence includes human capabilities in recognising risk, provisioning for their mitigation, and devising dynamic solutions that can adapt to changing needs.

Solution: build resilience, shared awareness, and human capacity

Since 2016, Data61 has been undertaking a range of initiatives to boost research, commercialisation and connectivity outcomes across Australia's cyber industry, and drive the development of new cybersecurity architectures. The cybersecurity program now includes over 47 activities across focused cyber themes, including:

- developing new scientific and technological solutions
- boosting cyber security research and collaboration
- cyber ecosystem activities
- commercialisation of cyber solutions
- improving Cyber Security Skills, and
- deepening connections with international partners.

Enhanced research and collaboration

A core strategy of the cyber security program is to boost cyber research capability and collaboration in Australia, including with the Australian Centre for Cyber Security, Australian Cyber Security Growth Network (AustCyber), and CyberSecurity CRC. Key research areas include:

- **Trustworthy Systems** — building on the formally verified seL4 operating system kernel to architect systems with critical components isolated from uncritical, untrusted ones
- **Distributed Systems Security** — designing security for distributed systems, including in areas such as IoT

---

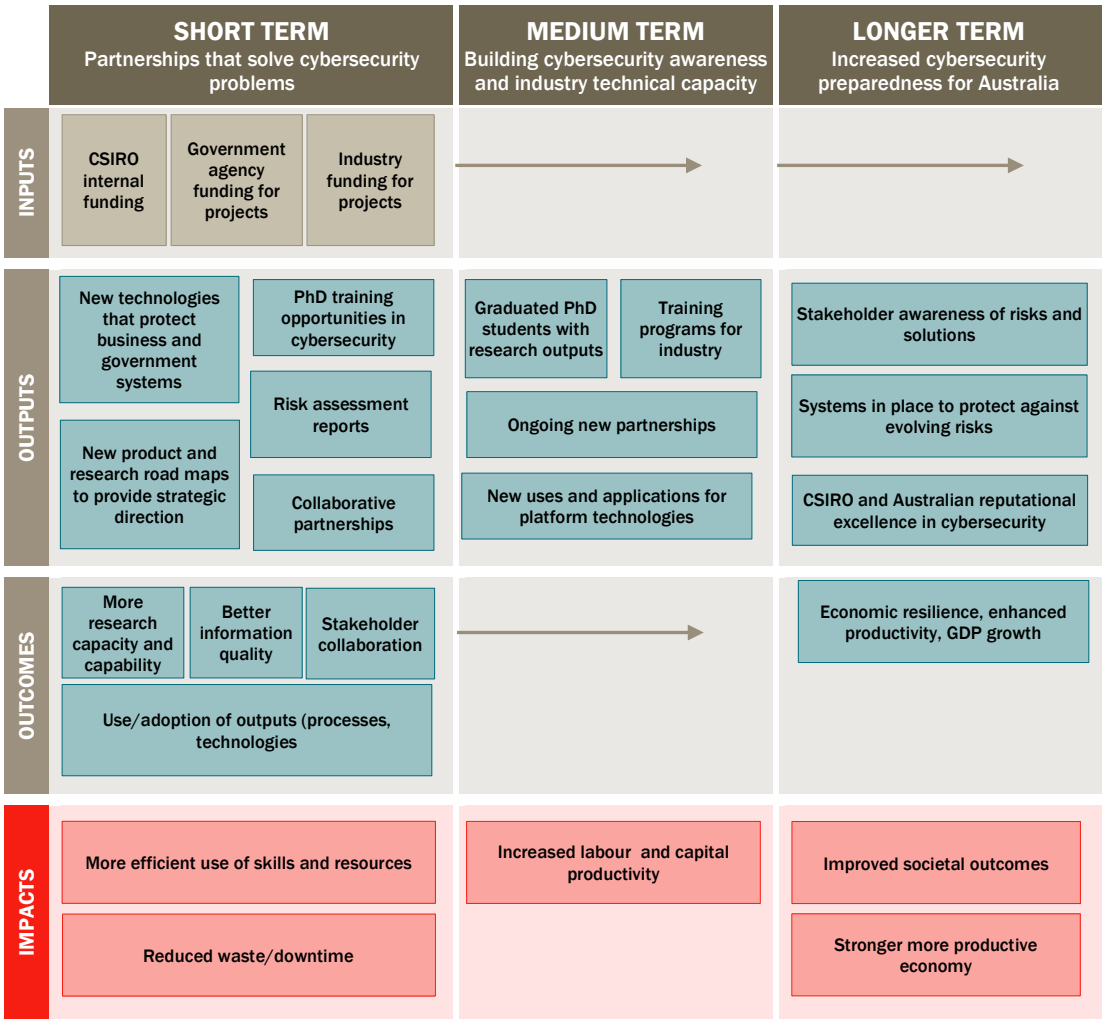
19 Taylor (2015), 'Potential Problems with Information Security Risk Assessments', *Information Security Journal: A Global Perspective*, vol. 24, pp.1-8, 2015.

- **Data Security and Privacy** — identifying and quantifying risks of data privacy and security vulnerabilities and developing privacy-preserving technologies
- **AI and Cyber Security** — using AI to solve cybersecurity problems and designing secure and safe AI systems, and
- **Human Centric Cyber Security** — focusing on vulnerabilities and threats centred around humans: usage, user and usability.

These activities are already increasing collaboration across Australia's cyber ecosystem, and aligning activity around Australia's key cyber challenges and opportunities. Several research outputs and technologies have already been developed, and are being trialled by governments and industry for potential future deployment.

Through NISA's Platforms for Open Data (PfOD) initiative, Data61 is also supporting Commonwealth Government Departments to explore and deploy secure data sharing and analysis technologies. The impact pathway for CSIRO Cybersecurity is multidimensional, ranging from impacts associated with discrete technology partnerships to changes in the cyber security system and capacity in Australia. An overview of its multidimensional nature is illustrated in chart 1.4 and described further in Chapter 2.

1.4 Multidimensional impact pathway for CSIRO Cybersecurity



Source: CIE.

2 Impact pathway for Data61 Cybersecurity

In its short history, Data61 Cybersecurity has enhanced CSIROs contribution to Australia's cybersecurity protection, leveraged additional government and industry investment, and brought stakeholders together to achieve more through collaboration and dispersion of cybersecurity capacity than would have been achieved otherwise. The value of cybersecurity expertise from Data61 is evidenced by high demand for commissioned projects, which for the three cybersecurity groups covers over 189 per cent of all program costs (comprised of $ 47.7 million in direct client revenue and NISA cybersecurity-related funding). The public dissemination of publications from the research team have been embraced globally, generating an estimated $870 000 annually as works are cited by the cybersecurity research community.

Inputs

CSIRO has invested in over 60 full time equivalent (FTE) cybersecurity researchers and engineers to support projects to improve cyber research and technology commercialisation over the past three years. Between FY2018– FY2020, $25.2 million has been invested by CSIRO in its three major cyber security groups (table 2.1).

2.1 CSIRO's investment into major cyber security groups

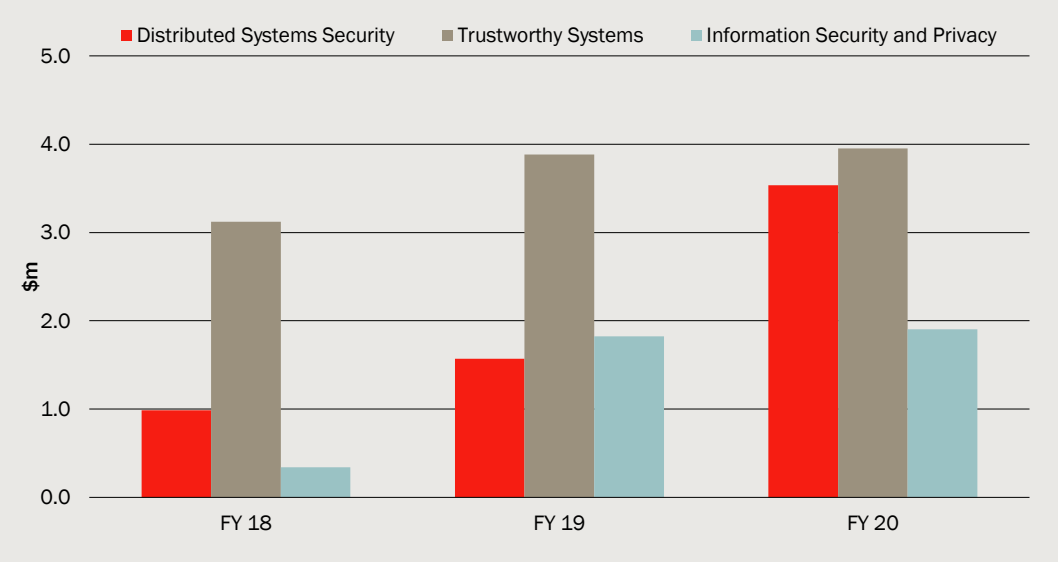
	Distributed Systems Security	Trustworthy Systems	Information Security and Privacy	Total
	$'000	$'000	$'000	$'000
Operating costs				
FY18	594.9	365.0	15.3	975.2
FY19	1 390.6	294.3	24.8	1 709.7
FY20	1 187.6	240.2	54.4	1 482.2
Total operating costs	**3 173.1**	**899.6**	**94.4**	**4 167.1**
Salary cost				
FY18	987.8	3 120.1	339.0	4 446.9
FY19	1 569.8	3 881.3	1 825.3	7 276.4
FY20	3 533.6	3 953.2	1 901.8	9 388.5
Total salary costs	**6 091.1**	**10 954.6**	**4 066.0**	**21 111.7**
TOTAL	**9 264.2**	**11 854.2**	**4 160.4**	**25 278.8**

Source: CSIRO unpublished.

Funding across the portfolio has increased in each year, although the focus on project work and the involvement of external funding sources has seen funding fluctuations at

the group level, with Distributed System Security, then Trustworthy Systems, experiencing the strongest overall growth in funding of all the groups (chart 2.2).

2.2 Increasing funding dominance of key programs over time



Source: CSIRO unpublished

Key non-CSIRO sources of funding comprise:

- **co-investment** funding from Science and Industry Endowment Fund, Defence Science & Technology Group, Cyber Security Research Centre Ltd.,, Department of Transport, Asian Office of Aerospace Research, and Intersective Pty. Ltd.
- **CSIRO strategic** funding to conduct research in broad cyber areas, such as from Department of Finance, Australia Competition & Consumer, The Department of the Prime Minister, Australian Prudential Regulation, and PwC, and
- **service and consulting** commissioned work for Hensoldt Cyber GmbH, HRL Laboratories, LLC, Rockwell Collins Inc, The Boeing Company Inc, Cyber Security Research Centre Ltd, United Technologies Corporation, Department of Customer Service, Department of Foreign, Australian Federal Police, Department of Industry, Science, and US Army International Technology and others.

Outputs: What Data61 cyber delivers

All the programs within the Data61 cyber portfolio have delivered new platform technologies and associated products that are actively being trialled and adopted by researchers, industry, and all levels of government, in Australia and internationally.

Key output domains across the Data61 cyber portfolio include the following:

- new partnerships and collaborations
- risk assessments for government agencies to improve their preparedness and response to cyber attack
- leadership and guidance forums and materials for cyber initiatives
- new training and development opportunities, and
- elevated CSIRO and Australia's international reputation.

New research partnerships

Important partnerships to date include:

- a three year strategic partnership (now extended for an additional three years) with the **Defence Science and Technology Group (DST Group)** for research collaboration in the areas of cyber and electronic warfare. This partnership has resulted in:
  - the commencement of 23 joint research projects with 15 universities in areas including cyber influence and data analytics, sensing to effects, autonomous systems, and system design for resilience
  - a networking forum held between Data61, DST Group and AustCyber in November 2017, attended by 80 participants from a wide range of universities and industries. The networking forum developed into a full-fledged the cybersecurity for defence conference. The first one was planned for March/20 but had to be postponed due to COVID19.
  - two Data61- DST Group Cyber Summer Schools (a third was postponed due to COVID19) providing 150 Australian research and academic leaders with access to international and local thought leaders in defence cyber, and
  - an early exploration of cyber security risk modelling for Australia's maritime ports to assess the convergence of cyber physical and logical cyber threats impacting the industry and national security.
- **partnering with the Attorney General's Department and CERT Australia** to explore a Cyber Threat Information Portal to support government to industry threat intelligence sharing
- **partnering with the NSW Government** to deliver targeted projects in:
  - Cybersecurity governance and management — developing a strategic roadmap for the protection of New South Wales' critical infrastructure
  - Internet-of-Things security — exploring deployment of a lightweight public-key encryption scheme and multi-level authentication protocol
  - cross-agency cybersecurity collaboration — exploring the potential for the use of blockchain to support cross-agency process coordination, and

  - threat intelligence data analytics — using advanced models for threat intelligence analytics, in a NSW context
- **partnering with the ACT Government** to establish the Canberra Cyber Network (CCN) — a collaboration between ACT Government, ANU, UNSW Canberra, UC and CIT, to promote best practice policy and behaviour in government and business
- **working with the Victorian Government** to grow Data61's Victorian Cyber and Innovation Centre in Melbourne and establish it as a focal point for industry to research collaboration and network building
- **working with the Queensland Government** to understand cyber readiness, security vulnerabilities and to explore the establishment of a secure data sharing framework within government, and
- collaborating on projects with States' internal data analytics groups, including the **NSW Data Analytics Centre (DAC)** and **Victorian Centre for Data Insights (VCDI)** and **SA's Office of Data Analytics** to support the sharing of sensitive information across government.

Data61 is also strengthening its international reputation for cyber excellence through partnerships such as:

- collaboration with **DARPA and Rockwell Collins** on a joint "Cyber Assured Systems Engineering (CASE)" project, trialling Data61's mathematically proven seL4 system software and architecture in defence applications
- a multi-million, multi-year collaboration with **a major European cybersecurity company and RISC-V Foundation** on critical system security
- joining various national networks and forums such as **Australia-Israel cybersecurity dialogue, Prime Minister's round table on cybersecurity, working group for Academic Centre of Excellence on cybersecurity and AustCyber**, and
- **Memorandum of Understandings (MOUs)** or other collaboration with various international universities on cybersecurity such as MIT, CMU, Purdue, NIST, University of Pittsburgh, University of Texas at San Antonio, TU Munich, Uni Augsburg, Uni, Chalmers Uni, Cambridge, Imperial College London, Singapore research ecosystems (NUST/NTU/A*Star) and IIT Bombay.

Risk assessments for agencies

In just three years, Data61 has established itself as a trusted advisor on privacy-enhancing and secure data sharing and associated technologies.

Over 30 privacy risk assessment have either been undertaken by Data61 and/or using its technology and tools for diverse data assessment use cases, and more than ten government departments and agencies have been provided with a Re-identification Risk Metric and Privacy and Re-identification Risk assessment.

For instance, Data61 has:

- worked with **Australian Bureau of Statistics** to prototype software enabling public data platforms to interactively access aggregated data, drawn from unit record datasets

- supported the **Department of Social Services (DSS)** in generating a synthetic social security dataset, allowing data to be openly released, whilst maintaining data privacy
- worked with DSS and the **Australian Institute of Health and Welfare** to develop and test software and a user interface to enable auditable data extraction and delivery into a secure environment for policy and research purposes by authorised users
- developed prototype technology for **Department of Industry, Innovation and Science** use in conducting web-based data analytics of BLADE data (business longitudinal), while preventing spontaneous recognition, and
- worked with the Queensland Office of the Information Commissioner, with Data61 acknowledged in the report tabled to the Queensland Parliament, which noted

  'We engaged CSIRO's Data61, the data science and digital specialist arm of the Commonwealth Scientific and Industrial Research Organisation, to assist with this section of the report. Data61 are experts in de-identification and re-identification risk analysis. They have specialised analytic tools that quantify the re-identification risk 'score' of de-identified data. We used these risk scores, and Data61's supporting analysis, to inform our findings in this chapter.' [20]In addition, many sections of its published guideline is directly linked to recommendations provided by Data61.[21]

Leadership and guidance forums and materials for cyber initiatives

Data61 is also actively supporting a number of broader cyber initiatives, including:

- leading as an industry and research provider to the **Cyber Security CRC,** joining 18 industry participants and 6 research partners, and co-leading initial projects for the CRC in security automation and orchestration, example projects include:
  - Cyber Common Operating Picture (CCOP) — A Platform for Gathering, Analysing, and Visualising Cyber Security Data[22]
  - SMART SHIELD Artificial Intelligence Assisted Holistic Anti-Phishing System[23]
  - Deception as a service — apply cutting edge machine learning and artificial intelligence to generate realistic computer systems and assets for the purposes of deceiving intruders who make their way into a system[24]

---

20 The Queensland Office of the Information Commissioner, 'Privacy and Public Data', *Queensland Office of Information Commissioner*, July 2020, p.25 <https://www.oic.qld.gov.au/about/our-organisation/key-functions/compliance-and-audit-reports/privacy-and-public-data-audit-report>, accessed 29 July 2020

21 The Queensland Office of the Information Commissioner, 'Privacy and de-identified data', *Queensland Office of Information Commissioner*, July 2020, < https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/anonymity/privacy-and-de-identification>, accessed 29 July 2020

22 See https://research.csiro.au/distributed-systems-security/cyber-common-operating-picture-ccop/

23 See https://research.csiro.au/distributed-systems-security/artificial/

24 See https://research.csiro.au/distributed-systems-security/deception/

  - Automated Identity and Access Management — development of an intelligent support for identity and access management task within enterprise IT Systems with dynamic business environments,[25] and
  - Automatic Assessment and Protection of Personal Information in Data Sharing — development of an automatic tool to analyse the robustness of Personal Information Factor (PIF) by considering the effects of re-identification attacks.
- having developed and launched **a Cyber Security Industry Roadmap** in collaboration with CSIRO Futures and the AustCyber, aimed at identifying cyber requirements for Australia's growth sectors.

Data61 is also **supporting Australian organisations to grow their cyber awareness and skills**, including through:

- the Cyber for Directors program, developed in conjunction with the Australian Institute of Company Directors (AICD) to lift digital literacy of Australian business leaders. To date, AICD and Data61 have delivered ten courses under the program with 1579 attendees
- two blockchain reports developed for the Department of Treasury and Finance to inform on the opportunities and security and privacy risks of deploying blockchain based technologies and systems and working on a new version with Australian Computer Society (ACS) for an industry and skilling report
- publishing a De-Identification Decision-Making Framework, in partnership with the Office of the Australian Information Commissioner (OAIC) to guide Australian businesses on managing re-identification risk
- partnering with Fintech accelerator Stone & Chalk on a number of cyber focused initiatives including the 2017 Fintech Cyber Summit, and
- partnering with the Silicon Valley Innovators Network (SINET) in the delivery of the 2017 and 2018 SINET61 Summit, with each Summit drawing approximately 250 high level international and local participants.

Training and development opportunities

Data61 has provided new training opportunities for Australian to develop world class skills in cyber security. This includes:

- support for **over 80 Data61 Cyber PhD Scholarships** in collaboration with Australian universities, and
- Over **20 undergraduate and graduate scholarships** and associated supervision effort in relation to the **Cyber Security CRC**.

New technologies

To progress opportunities to **commercialise new cyber technologies and solutions**, Data61 has developed around eleven cyber technologies — six in the pilot phase, two

---

[25] https://research.csiro.au/distributed-systems-security/automated/

undergoing trials, three in pre-commercialisation phase, and some already adopted and in use by clients. Examples include:

- working in collaboration with DST Group to developed and commercialise the Cross Domain Desktop Compositor (CDDC) prototype, which improves productivity in Defence and provides a means to securely access multiple isolated networks. CDDC has won three State iAwards in SA and the National Award for R&D, and has entered into the Defence Innovation Hub to continue the commercialisation process
- discussions with prominent defence industry leaders on the potential to collaborate in the use of formal methods for automated cyber assured systems verification
- working with a large EU-based cyber security organisation to explore commercialisation of anomaly detection techniques and user behaviour analytics for the Enterprise market
- working with a major international airline manufacturer on Secure and Modular Internet of Things (SMIT) technologies, trailing Data61's lightweight authentication protocol and architecture for use the manufacturer's supplier network. SMIT was recently open sourced to benefit Australia SME for global supply chain integration. https://www.smit-project.com/
- working with Australian Federal Police (AFP) on Data Airlock which enables data analytics in secure enclave and protects human investigators from harmful data, and
- partnering with Australian company Kollakorn, to provide biometrc authentication techniques to their CertainID product.

Examples of some of the deliverables Examples of some of the particular technologies produced as a result of the Data61 cyber research program are showcased in boxes 2.3, 2.4, 2.5, and 2.6.

2.3 High-Assurance Cyber Military Systems

The High-Assurance Cyber Military Systems project adopted a fundamentally different, formal methods-based approach to enable semi-automated code synthesis from executable, formal specifications. Its aim was to raise the technical bar and lower the development cost for high-assurance cyber-physical systems. With partners, Defense Advanced Research Projects Agency (DARPA), Rockwell Collins, Galois Inc, University of Minnesota, Boeing, HRL, MIT, University of Illinois, Carnegie Mellon University (CMU), Princeton University, and US Army's TARDEC, CSIRO embedded Data61's world's most verified and fastest operating system kernel, seL4, on a range of unmanned and autonomous systems. It was demonstrated that mathematically assured software does protect against cyber-attacks.[26]

Beyond defence, the project provides core technologies for protecting a wide range of cyber-physical systems from attacks, including civilian aircraft, implanted medical devices, cars and other transport systems, robots and industrial plants. The successful demonstration of the software formally verified that it had reached the maturity to be embedded on real-world systems. This has triggered significant uptake of the technology in a wide range of industries, as demonstrated by the number of presentations on the industry use of seL4 by various companies at the recent seL4 summit in November 2018.[27]

[26] The HACMS project @ Data61, see https://ts.data61.csiro.au//projects/TS/SMACCM

[27] The first annual seL4 Summit was held on November 14-16, 2018 at the Hilton Washington Dulles Airport, Herndon, see https://www.sel4-us.org/summit.

2.4 Trustworthy Systems (TS)

The TS group has achieved significant breakthroughs to resolve untrustworthy systems by well-designed microkernels and successfully delivered tech-transfer projects to deliver software, tools, frameworks and platforms for cost-effective production of trustworthy systems.

The microkernels are engineered to reduce the size of kernel of the operating system (OS) – the most critical part of software systems for codes to run in privileged mode – to the absolute minimum. Restricted privileged execution with less LOC lowers security risk and brings about stability for entire multitasking systems.

The main microkernels – L4 embedded and seL4 microkernels – are engineered and produced to improve the performance and security of software systems.

L4 embedded was early adopted by Qualcomm, a leading manufacturer of wireless communication chips for mobile phone and other devices. The kernel technology was marketed as OKL4 and by 2008, it has achieved a deployment of greater than half a billion units per year. A version of this kernel now protects the secure enclave of all iOS devices.

Building on 15 years of experience with L4 microkernel, a new microkernel called seL4 was developed. It is the first-ever operating system kernel with a machine-checked formal, mathematical proof of absence of implementation defects. A key limitation of traditional combination of testing, code inspection and engineering processes that a critical system has built on for functioning, is an incomplete coverage of all behaviours and inputs of a non-trivial systems. The TS group uses a formal, mathematical model and proof to enable the machine-checked formal verification of a microkernel. It allows the reasoning about all possible behaviours of a system, thereby bringing about guarantees of absence of defects. Complementary to this development are breakthroughs in machine-checked code-level proof of isolation properties for a general-purpose OS kernel, worst-case execution time analysis of multitasking OS kernel, and security disclosure of timing attacking.

The TS group continues to build on the seL4 technology as a secure foundation and implement trustworthy systems. One highlighted effort was through the High-Assurance Cyber Military Systems program, where the TS group collaborated with US companies including Boeing to transition the seL4 technology to cyber-attack resistant autonomous vehicles. Another key project using seL4 technology was performed in Australia where the TS group collaborated with Australia's Defence Science and the Technology (DST) group to develop a device allowing users to visualise information from multiple networks of different classification levels on the same monitor.

The most significant uptake and adoption has been in the United States, with Australia in the early adoption stage of the research and technologies.

2.5 Data Airlock

Protecting sensitive data – such as images and video captured during legal investigations – against illicit data processing and transmission has always been important and led to limitations of R&D in analytics of sensitive data.

To enable safe and reliable use while keeping security of sensitive data under control, Data61 of CSIRO, in collaboration with Australian Federal Police (AFP) and Monash University, has developed a data analytics platform called Data Airlock. The platform keeps sensitive data in secure vaults and allows researchers to develop manually vetted algorithms against the data in isolated environments, the airlocks. Researchers are able to receive updates during executions and vetted outputs for evaluation. The platform also enables partially trusted third parties to host the system securely.

AFP has adopted Data Airlock for better identification and utilisation of sensitive data. Other agencies from various domains such as Department of Home Affairs and NSW Police also show their interest in uptakes of this technology in their context.

Data Airlock will be further developed by additional cryptography and differential-privacy algorithms – especially for healthcare sector – and more adaptivity for analytics of all types of sensitive data.

2.6 R4 – The re-identification risk ready reckoner

Data re-identification poses substantial privacy risks to individuals as well as data owners. R4 is an information theory based risk assessment tool – developed by the Information, Security and Privacy (ISP) group – to assist data custodians with evaluation of levels and origins of re-identification risks for better decision making on data and relevant risk treatments.

At R4 standard techniques including binning and perturbation are directly applied to one or more attributes. Modified versions of these attributes and their risks analyse are also enabled to see potential impact of transformations.

R4 is adopted to conduct privacy risk assessments for agencies such as Transport for NSW, Department of Health and Australian Taxation Office. It is currently under advanced licensing negotiation for commercialisation.

Outcomes

Leveraged investment into Australia's cybersecurity preparedness

Data61 has executed numerous contracts with clients to provide commissioned work to address industrial and agency needs. Over 2018-2020, contracted revenue for three cyber groups has amounted to $27.9 million. In addition, the three cyber groups have received funding from NISA of $19.8 million over three years, given the alignment of research outcomes with the national science agenda.

Key contributors of revenue are displayed in table 2.7. Excluding NISA funding, the top five revenue contributors are Defence Science & Technology Group, Hensoldt Cyber GmbH, Rockwell Collins Inc, United Technologies Corporation, and The Boeing Company Inc. They have contributed more than $20.5 million.

2.7 Major customers for FY 18-20 Revenue

Customers	Revenue	Percent of total
	$	%
Defence Science & Technology Group	11 840 598	42
Hensoldt Cyber GmbH	3 197 985	11
Rockwell Collins Inc	2 165 256	8
United Technologies Corporation	1 822 367	7
The Boeing Company Inc	1 521 279	5
Cyber Security Research Centre Ltd	1 263 709	5
Australian Federal Police	1 123 000	4
Asian Office of Aerospace Research	1 013 953	4
Department of Customer Service	747 000	3
HRL Laboratories, LLC	537 058	2
Other	2 706 098	10
Total	**27 938 302**	**100**

Note: Total Revenue here includes program-level revenue of $12.2 million. Excludes NISA-Data61 funding of $19.8 million. *Source:* CSIRO unpublished

Key revenue generators by program is shown in table 2.8.

With the addition of NISA funding, this level of revenue covers all investment costs in these groups, with a combined cost recovery rate of 178 per cent, ranging from 115 per cent for Trustworthy Systems to 235 per cent for Distributed Systems Security.

2.8 Cost recovery by cybersecurity group

Program	Costs FY18	Revenue FY18	Costs FY19	Revenue FY19	Costs FY20	Revenue FY20	Cost recovery FY18-FY20
	$m	$m	$m	$m	$m	$m	%
Distributed Systems Security	1.58	7.84	2.96	5.55	4.72	8.37	235
Trustworthy Systems	3.49	4.19	4.18	4.90	4.19	4.60	115
Information Security/Privacy	1.85	4.40	1.85	3.33	1.96	4.56	217
Annual total	**6.92**	**16.43**	**8.99**	**13.78**	**10.87**	**17.53**	**178**

Note: Annual total costs include salary and operating costs. Annual total revenues include $27.9 mil generated by the cyber groups and their collaborative program-level revenue, plus NISA-Data61 funding of $19.8 million over three years.

Source: CSIRO unpublished

Strengthened intellectual capital

The CSIRO Data61 cluster of programs has had an immediate and enduring effect on building Australia's intellectual capital in cybersecurity.

This occurs on multiple fronts:

- through the research of key program team members
- PhD opportunities afforded to new researchers, and
- upskilling of industry to understand and manage their risk exposure.

Value of published work

Researchers involved in the Cybersecurity programs have a large volume of published material and associated citations, which is a measure of the value of knowledge output and built intellection capital from the programs.

A substantial amount of researcher time is dedicated to the publication of publicly available materials and keynote speaking addresses in international public forums, which add to the stock of cybersecurity intellectual capital in Australia.

Significant research publications and citations are summarised in tables 2.9 and 2.10. One indicator of the effectiveness of information dissemination by CSIRO Data61 Cybersecurity researchers is the citation of published work. While this is just a subset of the uptake of research findings, it remains indicative of the value of research outputs, nonetheless.

In total, the Cybersecurity team account for over 162 517 citations, or 81 501 in the past five years alone (table 2.10). On average, this is 16 300 citations every year across the group. In line with the approach adopted by Florio, Forte and Sirtori (2015),[28] the value of citations can be deemed equivalent to the value of researcher time and the time taken

28 Florio, M., Forte, S. and Sirtori, E., 2015, 'Cost-benefit analysis of the Large Hadron Collider to 2025 and beyond', arXiv:1507.05638v1, available at: https://arxiv.org/abs/1507.05638

to read citations. Assuming it takes a researcher one hour to read and cite a paper,[29] $844 000 is generated annually through Data61 Cybersecurity-associated citations.

2.9 Significant Cybersecurity publications

Author(s)	Year	Publication
Wu, N., Farokhi,F.,Smith, D.andKaafar, M.A.	2020	The Value of Collaboration in Convex Machine Learning with Differential Privacy. IEEE Symposium on Security and Privacy, San Francisco 2020 (Core A*)
Ahmed, Il-Youp, Huh, Kwak, Oh and Kim	2020	Void: A fast and light voice liveness detection system. Usenix Security 2020, 2685-2703.
Kocher, Horn, Fogh, Genkin, Gruss, Haas, Haburg, Lipp, Mangard, Prescher, Schwartz, Yarom	2019	Spectre attacks: Exploiting speculative execution, IEEE Symposium on Security and Privacy, pp. 19-37, San Francisco, May, 2019 (CORE A*); and InIEEE Symposium on Securityand Privacy, pages 19–37, San Francisco, May 2019. IEEE.
Muhammed F. Esgin, Raymond K. Zhao, Ron Steinfeld, Joseph K. Liu, Dongxi Liu	2019	MatRiCT: Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol. ACM Conference on Computer and Communications Security 2019: 567-584 (CORE A*)
Ikram, M., Masood, R., Tyson, G., Kaafar, M.A., Loizon, N. and Ensafi, R.	2019	The Chain of Implicit Trust: An Analysis of the Web Third-party Resources Loading. Proceedings of the 2019 World Wide Web Conference (WWW '19) (CORE A*)
Esgin, Steinfeld, Liu, J. K., Liu, D.	2019	Lattice-based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications, Crypto, 2019,115-146 (CORE A*).
Ge, Yarom, Chothia, Heiser	2019	Time Protection: The Missing OS Abstraction. EuroSys 2019: 1:1-1:17
Lai, Patranabis, Sakzad, Liu, J. K., Mukhopadhyay, Steinfeld, Sun, Liu, D., Zuo	2018	Result Pattern Hiding Searchable Encryption for Conjunctive Queries. 25th ACM Conference on Computer and Communications Security (CCS) 2018: 745-762. (CORE A*)
Klein, Andronick, Kuz, Murray, Heiser, and Fernandez	2018	Formally verified software in the real world. Communications of the ACM, 61:68–77, October 2018
Sun, Yuan, Liu, Steinfeld, Sakzad, Vo, Nepal	2018	Practical Backward-Secure Searchable Encryption from Symmetric Puncturable Encryption. 25th ACM Conference on Computer and Communications Security (CCS) 2018: 763-780. (CORE A*)
Yan, Sui, Chen, Xue	2018	Spatio-temporal context reduction: a pointer-analysis-based static approach for detecting use-after-free vulnerabilities. 40th International Conference on Software Engineering (ICSE) 2018: 327-337 (ACM SIGSOFT Distinguished Paper Award, CORE A*)
Masood, R., Zhao, B.Z.H., Asghar, H.J. and Kaafar, M.A	2018	Touch and You're Trapp(ck)ed: Quantifying the Uniqueness of Touch Gestures for Tracking. Proceedings on Privacy Enhancing Technologies, pp.122-142.
Masood, R., Vatsalan, D., Ikram, M. and Kaafar, M.A.	2018	Incognito: A Method for Obfuscating Web Data. In Proceedings of the 2018 World Wide Web Conference on World Wide Web, pp. 267-276. (CORE A*)
Lyons, McLeod, Imatary, and Heiser	2018	Scheduling-context capabilities: A principled, light-weight OS mechanism for managing time. In EuroSys Conference, Porto, Portugal, April 2018. ACM
Perrier, V., Asghar, H.J. and Kaafar, D	2018	Private Continual Release of Real-Valued Data Streams. The Network and Distributed System Security Symposium, NDSS 2019 (CORE A*)

Source: Tessellate 2019, Appendix B.

29 Consistent with the assumption in Florio et al. (2015), as discussed by: Schopper, H., 2016, 'Some remarks concerning the cost/benefit analysis applied to LHC at CERN', *Technological Forecasting and Social Change*, available at: http://isidl.com/wp-content/uploads/2017/08/E4668-ISIDL.pdf

2.10 Publication productivity of key team researchers

Author	Program	Citations in past 5 years	h-index in the past 5 years
Liming Zhu		4 271	35
June Andronick	Trustworthy Systems	1 882	14
Gernot Heiser	Trustworthy Systems	6 749	35
Gerwin Klein	Trustworthy Systems	2 976	20
Rob van Glabbeek	Trustworthy Systems	2 214	24
Michael Norrish	Trustworthy Systems	2 243	15
Kevin Elphinstone	Trustworthy Systems	1 985	12
Carroll Morgan	Trustworthy Systems	1 552	20
Tony Hosking	Trustworthy Systems	1 641	14
Yuval Yarom	Trustworthy Systems	5 867	25
Surya Nepal	Distributed Systems Security	5 019	33
Josef Pieprzyk	Distributed Systems Security	2 696	24
Seyit Camtepe	Distributed Systems Security	2 071	21
Shiping Chen	Distributed Systems Security	1 913	19
Dali Kaafar	Information Security Privacy	2 982	31
Brian Anderson	Information Security Privacy	18 540	52
Eliathamby Ambikairajah	Information Security Privacy	2 576	23
David Smith	Information Security Privacy	3 684	25
Julien Epps	Information Security Privacy	5 192	32
Vijay Sivaraman	Information Security Privacy	2 486	28
Sanjay Jha	Information Security Privacy	2 962	27
TOTAL		**81 501**	

Source: The CIE.

This excludes value derived from dissemination of insights through keynote speaking addresses, which have been numerous in the last two years alone (table 2.11).

2.11 Invited keynote and plenary talks (2018–19)

Name	
June Andronick	FM 2019 keynote SecDev 2019 keynote
Surya Nepal	Keynote/Invited Talk, Australasian Conference Information Security and Privacy (2016-18) Keynote Speaker at 11th International Conference On Security Of Information and Networks, September 2018 / Cardiff University, Cardiff UK. Keynote Speaker at the International Workshop on the Internet of Things Cybersecurity and Safety, University of Canterbury, Christchurch, New Zeeland, July 2018. Keynote Speaker. 5th Cyber Security Symposium, International Hotel, Wagga Wagga, July 2018. Organised by Charles Stuart University, Wagga Wagga, Australia Invited Panel Member. 2nd Industrial Internet 4.0 Summit. Harnessing industry 4.0 to advance Australia's manufacturing sector. 21-22 February 2018, SMC conference and function centre. Keynote speaker ASWEC 2019, Adelaide Keynote Speaker, Singapore Cyber Security R&D Conference 2019 (SG-CRC 2019).
Dali Kaafar	Invited Speaker at the Future Data Conference, November 21 2018 Sydney. Invited Speaker at GovInnovate – October 9th-11th 2018 in Canberra. Panelist at the IIT Panel – Sydney September 26 2018. Panelist in the Data61 Live event, Brisbane September 18-19. Panelist at the CIFI Conference Sydney – September 13th 2018. Invited Speaker at the Data Privacy and Protection Conference – September 12th 2018 Sydney. Invited Speaker at the Customer Data Privacy and Protection – September 4th–5th in Melbourne. Panelist at SINET61 – August 1st 2018 in Melbourne. Panelist at the Australia-Israel chamber of Commerce event on Cyber security 2017, Plenary Talk at the Optus Data Breach Notification event 2018. Keynote speaker in the WWW Workshop on Computational Methods for CyberSafety (Cybersafety 2017), "Measuring, Characterising and Detecting Fake Social Activity", April, Perth 2017. Invited Talk in the Global Summit for Future Networks, Security and Privacy of the SDN-NFV Data Plane", April Nanjing 2017. Webinar for the AICD Australian Institute of Company Directors. Data Privacy: What you need to know about privacy preserving technologies and data sharing", March 2017. Invited Talk in the Dagstuhl Seminars series, Online Privacy in the era of Facebook, Dagstuhl 2013. Plenary Invited Talk at the 26th IEEE Annual Computer Communications Workshop (CCW 2012), Invited Talk at the Cyber Security, Forensics and Cyber-Crime Prevention Colloquium, "Geolocalisation of Botnet Mothership Command & Control Servers". Montreal, October 2011. Panelist in the Cyber Security, Forensics and Cyber-Crime Prevention Colloquium, Montreal, 2011. Invited Talk at the Workshop on Social Networks Security, "The 10 rules of Inference Techniques from an information security perspective", KAIST, Seoul 2011. Invited Talk at the Forensics Lerti Seminars, "Peer to peer monitoring from your laptop", June 2010. Invited Seminars at several Prestigious institutes, organisations and universities including Concordia University (2010, 2012, 2014), UC Berkeley (2015, 2016), NYU Polytech (2014), UCL (2015, 2016), Huawei Research Centre (2012, 2013), Tsinghua University (2011, 2012, 2014), CMU (2015).
Liming Zhu	Panelist, "Risk and Security with blockchain and DLTs", ADC Blockchain Summit, Mar/2019 Invited talk, "Distributed AI and Smart Contract: Implications to global financial stability", at Financial Stability Board (FSB)'s Financial Innovation Network (FIN) meeting, Jan/2019, HK. Keynote, "Distributed Trust: How Data-Driven Applications, AI and Blockchain is Impacting Service Oriented Computing", ICSOC, Nov 2018, Hangzhou, China. Panelist, "Best in class regulatory initiatives across the globe", Money 20/20, 2018, Hangzhou Panelist, "Industry 4.0 and Cybersecurity", Industry 4.0 Leaders Summit, HK, Oct 2018 Talk + Panelist, "Staying Relevant in the Analytics Age", Data Analytics Seminar 2018 Panelist, "cybersecurity for medical devices", TGA workshop, Sept 2018 Guest of Honour at private luncheon, How Blockchain can help Industry, Berlin, Sept 2018

Name	
	Invited talk/Panelist: "Blockchain and Cybersecurity", OECD Blockchain Policy Forum, 2018
	Panelist, "The Business of Blockchain", USyd business school Affinity series event, July 2018
	Keynote, "How automation and artificial intelligence can digitally transform the procurement profession", CIPS, July 2018
	"Introducing Cyber-Physical Security Industry Frameworks", ASIS breakfast series, May 2018
	Panelist, "Cyber Resilience: change and adapting as leaders", National Public Sector Managers and Leaders Conference, Mar 2018
	Keynote, "Automating Cybersecurity and Compliance", The Australian Cyber, Fraud and Risk Summit, Mar 2018
	Expert Witness, parliament enquires on "Growing presence of inauthentic Aboriginal and Torres Strait Islander 'style' art and craft products and merchandise for sale across Australia" , 2018
	Keynote, "Data Economy: the Cornerstone of Smart Business", GMIC + Sydney, Dec 2017
	Panelist, "Cybersecurity: is your business prepared for the next unknown threat?", Australia-Israel Chamber of Commerce, Nov 2017
	Keynote, Intersecting fintech and cybersecurity, Nat. Fintech and Cybersecurity Summit, 2017

Source: Tessellate 2019, Appendix C.

Too early to estimate net benefits but the value case is clear

Data61's Cybersecurity programs are still in their infancy, and growing as fast as their staff capacity can sustain. With the PhD scholarships program and upskilling of industry, cybersecurity capacity will grow, and with it, demand from government and industry to improve cybersecurity preparedness across the country.

Data61's Cybersecurity programs are an excellent example of an exemplar in CSIRO research: clear causal links between research excellence and meeting the specific needs of government and industry to address large scale challenges with potentially large scale costs to society and economy when not addressed well.

A case study on the economic value of one of its research groups is showcased in box 2.12.

2.12 Estimated economic returns from Trustworthy Systems

A 2019 research impact evaluation of CSIRO Trustworthy Systems (TS) estimated the triple bottom line impact of TS worldwide, and the benefits provided to Australia by avoiding and minimising the cost of challenges to Trustworthy Systems.

Over the 2018-2028 period, it was estimated that TS research generated benefits between $93.2 million and $275.6 million in net present value terms due to the application of seL4[30] into industry, government and defence, and a reduction in the direct and indirect costs of data breaches in Australia.

This was comprised of:

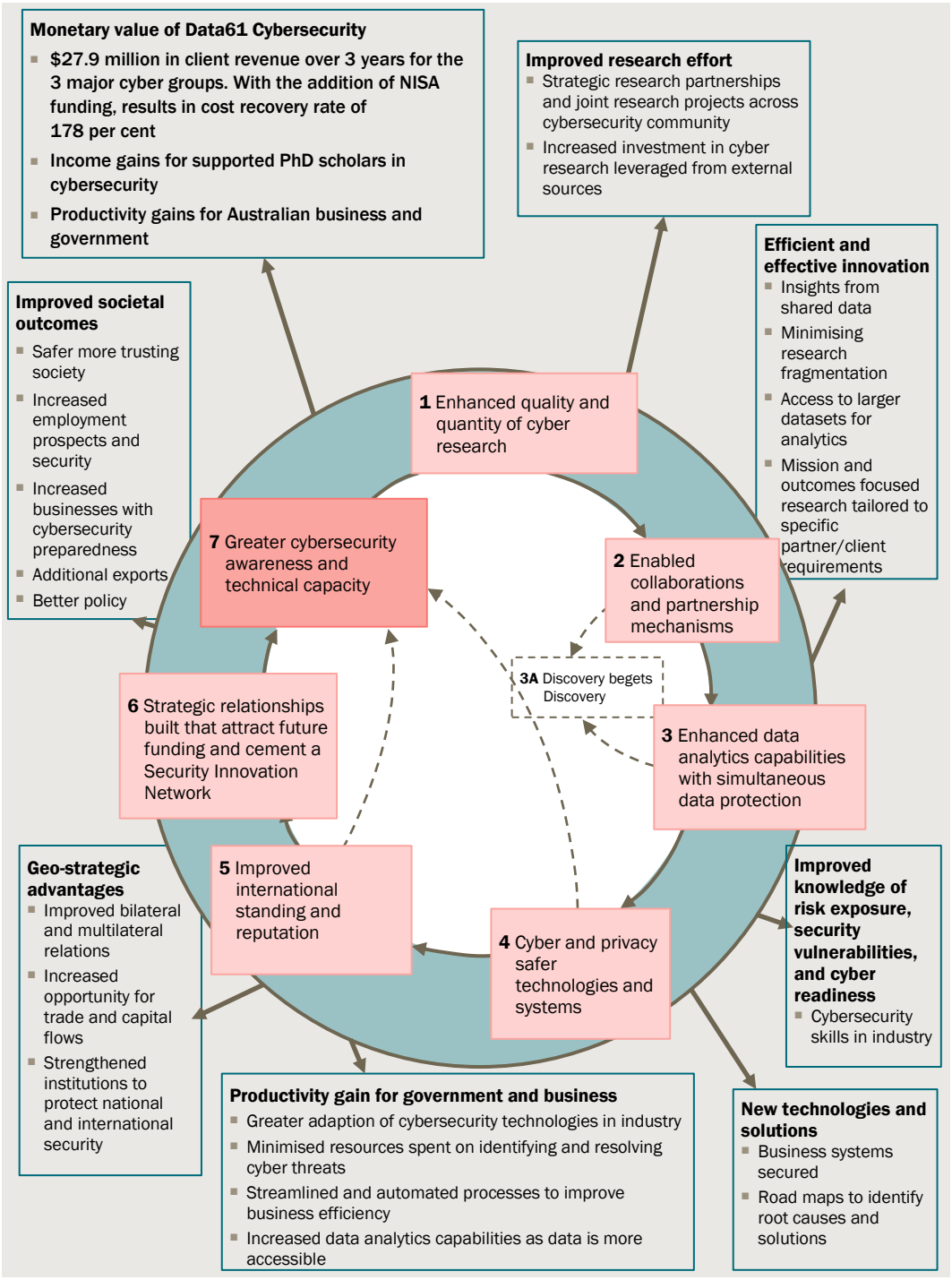
- economic benefits from the commercialisation of the Cross Domain Desktop Compositor (CDDC) technology, which uses the seL4's verified isolation and information security capabilities, worth $8.6 million to $23.6 million in present value terms depending on the level of adoption (no change in demand through to an increase in domestic and international demand), and
- reduced costs for data breaches in Australia, worth $84.6 million to $252.0 million in present value terms, depending on the percent of Australian data breaches that will be subject to adoption of seL4- enabled software systems (10, 20, or 30 per cent)

Source: CSIRO 2019a, Understanding the value and real-world impact of the Trustworthy Systems group's research and technology, Research Impact Evaluation, CSIRO.

The rapid uptake of demand for cybersecurity expertise, and the leveraged commitment to substantial funding of research points to a research program that is highly valued on multiple fronts, with the capacity to materially impact on the resilience of the Australian economy. The logic of the impact creation pathway for Cybersecurity is illustrated in chart 2.13.

30 The seL4 microkernel platform and tools include the CAmkES component platform, which protects critical systems from software failures and cyber-attacks.

2.13 Key outcomes and impacts of Data61's Cybersecurity program



Data source: CIE.

References

Ahmed, M. E., Youp, I., Huh, J. H., Kwak, I. K. (2020), Taekkyung Oh and Hyoungshick Kim. Void: A fast and light voice liveness detection system. Usenix Security 2020, 2685-2703.

AustCyber (2020), 'Australia's Digital Trust Report 2020', AustCyber, July 2020, <https://www.austcyber.com/resource/digitaltrustreport2020>, accessed 30 July 2020

Australian Criminal Intelligence Commission (2019), 'Cybercrime', *Australian Criminal Intelligence Commission*, 2019, <https://www.acic.gov.au/about-crime/organised-crime-groups/cybercrime>, accessed 3 June 2020

Australian Cyber Security Centre (2018), 'ACSC statement on reports of Intel Active Management Technology (AMT) security issue', *Australian Signals Directorate*, 2018, <https://www.cyber.gov.au/news/acsc-statement-on-reports-of-intel-active-management-technology-security-issue>, accessed 6 June 2020.

Australian Government (2016), Cost-Benefit Analysis; Guidance Note, Department of the Prime Minister and Cabinet – Office of Best Practice Regulation, https://www.pmc.gov.au/sites/default/files/publications/006-Cost-benefit-analysis.pdf.

Bissell, K., and Lasalle, R., (2019), 'Ninth Annual Cost of Cybercrime Study', *Accenture Security North America*, 2019, <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>, accessed 4 June 2020.

Bonderud, D., (2015), 'Eight Crazy Hacks: The Worst and Weirdest Data Breaches of 2015', *Security Intelligence*, 2015, < https://securityintelligence.com/eight-crazy-hacks-the-worst-and-weirdest-data-breaches-of-2015/>, accessed 3 June 2020.

Chelvan, C., (2018) 'Foreshadowing attacks: cybersecurity researchers save the day', *CSIRO scope*, Aug 2018, <https://blog.csiro.au/foreshadowing-attacks-cybersecurity-researchers-save-the-day/>, accessed 10 Aug 2020.

CSIRO Data61 (2019), Cyber Security Strategy.

CSIRO (2019a), Understanding the value and real-world impact of the Trustworthy Systems group's research and technology, Research Impact Evaluation, CSIRO.

Culnane, C., Rubinstein, B., and Teague, V., (2017) 'Health Data in an Open World', *Corenell University arXiv Organisation*, 2017, <https://arxiv.org/ftp/arxiv/papers/1712/1712.05627.pdf>, accessed 6 June 2020.

Davis, D., 'Internet of Things Cyber Attacks Grow More Diverse' (2019), *Symantec-enterprise-blogs*, 2019, <https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/istr-2019-internet-things-cyber-attacks-grow-more-diverse?om_ext_cid=biz_social3_AMS_NAM-IV_twitter_>, accessed 6 June 2020.

Chelvan, C. (2018), 'Foreshadowing attacks: cybersecurity researchers save the day', *CSIRO scope*, Aug 2018, <https://blog.csiro.au/foreshadowing-attacks-cybersecurity-researchers-save-the-day/>, accessed 10 Aug 2020.

Florio, M., Forte, S. and Sirtori, E., (2015), 'Cost-benefit analysis of the Large Hadron Collider to 2025 and beyond', arXiv:1507.05638v1, https://arxiv.org/abs/1507.05638.

Forrester Consulting (2019), 'BIOS Security – The Next Frontier for Endpoint Protection Report', *Dell Technologies*, 2019, < https://www.dellemc.com/ja-jp/collaterals/unauth/analyst-

reports/solutions/dell-bios-security-the-next-frontier-for-endpoint-protection.pdf>, accessed 6 June 2020.

Ge, Q., Yarom, Y., Chothia, T., Heiser, G. (2019), Time Protection: The Missing OS Abstraction. EuroSys 2019: 1:1-1:17.

IBM Security (2019), 'IBM Security Cost of a Data Breach Report 2019', *IBM*, 2019, < https://www.ibm.com/security/data-breach>, accessed 5 June 2020.

Ikram, M., Masood, R., Tyson, G., Kaafar, M.A., Loizon, N. and Ensafi, R. (2019). The Chain of Implicit Trust: An Analysis of the Web Third-party Resources Loading. Proceedings of the 2019 World Wide Web Conference (WWW '19) (CORE A*).

Klein, G., Andronick, J., Kuz, I., Murray, T., Heiser, G., Fernandez, M., (2018), Formally verified software in the real world. Communications of the ACM, 61:68–77, October 2018.

Lai, S., Patranabis, S., Sakzad, A., Liu, J. K., Mukhopadhyay, D., Steinfeld, R., Sun, S., Liu, D., Zuo, C., (2019), Result Pattern Hiding Searchable Encryption for Conjunctive Queries. 25th ACM Conference on Computer and Communications Security (CCS) 2018: 745-762. (CORE A*).

Lyons, A., McLeod, K., Almatary, H., Heiser, G. (2018), Scheduling-context capabilities: A principled, light-weight OS mechanism for managing time. In EuroSys Conference, Porto, Portugal, April 2018. ACM.

Muhammed F. Esgin, Raymond K. Zhao, Ron Steinfeld, Joseph K. Liu, Dongxi Liu (2019a), MatRiCT: Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol. ACM Conference on Computer and Communications Security 2019: 567-584 (CORE A*).

Muhammed F. Esgin, Raymond K. Zhao, Ron Steinfeld, Joseph K. Liu, Dongxi Liu (2019b), MatRiCT: Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol. ACM Conference on Computer and Communications Security 2019: 567-584 (CORE A*).

Muhammed F. Esgin, Raymond K. Zhao, Ron Steinfeld, Joseph K. Liu, Dongxi Liu (2019c), Lattice-based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications, Crypto, 2019,115-146 (CORE A*).

Perrier, V., Asghar, H.J. and Kaafar, D. (2018). Private Continual Release of Real-Valued Data Streams. The Network and Distributed System Security Symposium, NDSS 2019 (CORE A*).

Schopper, H (2016), 'Some remarks concerning the cost/benefit analysis applied to LHC at CERN', *Technological Forecasting and Social Change*, http://isidl.com/wp-content/uploads/2017/08/E4668-ISIDL.pdf.

Taylor, R. (2015), 'Potential Problems with Information Security Risk Assessments', *Information Security Journal: A Global Perspective*, vol. 24, pp.1-8, 2015, <https://www.researchgate.net/publication/283784852_Potential_Problems_with_Information_Security_Risk_Assessments>, accessed 6 June 2020.

Tessellate Communication (2019), 'Data61 Cybersecurity industry Development Program: Evaluation Report, Commercial-in-Confidence, July 2019.

The HACMS project @ Data61, see https://ts.data61.csiro.au//projects/TS/SMACCM

The Office of Australian Information Commissioner (2018), 'Notifiable Data Breaches Statistics Report: 1 January to 31 March 2018', *OAIC Notifiable data breaches*, July 2018, < https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-january-to-31-march-2018/>, accessed 4 June 2020.

U.S. Food & Drug Administration (2017), 'Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication', *2017 Safety Communications*, 2017, <https://www.fda.gov/medical-devices/medical-device-safety/safety-communications>, accessed 3 June 2020.

Wu, N., Farokhi,F.,Smith, D.and Kaafar, M.A. (2020), The Value of Collaboration in Convex Machine Learning with Differential Privacy. IEEE Symposium on Security and Privacy, San Francisco 2020 (Core A*).

THE CENTRE FOR INTERNATIONAL ECONOMICS
www.TheCIE.com.au