NSW Cyber Security Network Cyber Vouchers

Cyber Voucher Illustrative Use Cases

Please note: all Use Cases are fictional and merely illustrative of the types of projects that may be considered.

Use Case 1

Voice hacking

A two person startup based in the Sydney Startup Hub believes that home-based 'voice activated' devices, such as Amazon's Alexa, Google's Assistant and Apple's Siri, are subject to possible 'white noise' attacks and they have developed an early stage algorithm to possibly address this cybersecurity concern. A 'white noise' attack is where would be intruders and hackers can use crafted non-speech noise to activate and command these devices to "open front door" or "purchase $1,000 of goods".

The start-up would benefit from a rigorous, independent and credible test of their algorithm in different deployment and device configurations. A NSW CSN Cyber Voucher can be used to connect with a leading research team in a Member NSW University to design and conduct such a test and provide a documented report on the results. The report would assist the startup with refining its product development and solution strategy, define leading use cases and build trust with potential investors and strategic partners.

https://nypost.com/2018/05/11/hackers-can-use-white-noise-to-break-into-your-alexa/

Use Case 2

Documented Consents

A NSW provider of medical General Practice (GP) practice management software (PMS), which includes an Electronic Patient Record (EPR) component, understands that even basic analysis of EPR information across all of their GP subscribers would add considerable benefit to their GPs and to patients. For example, GPs could provide 'patient to their peer group' ratings to individual patients and gain insights about treatments and progress. However, to provide such information, all patients would need to provide appropriate consents and the analysis would need to be undertaken utilising an appropriate privacy protected method. The GP PMS provider wishes to better understand the Australian landscape for how best to construct and implement patients 'consents' (mostly a legal question) and what are the most suited Provable Privacy approaches available (mostly an Information Security question). The company can utilise a NSW CSN Cyber Voucher to engage with one or more NSW CSN University Member Law Schools (on the consent question) and Computer Science Departments (on the Differential Privacy question) to better understand the general state and suitability of available approaches.

Use Case 3

Video tracking

A spin-out from CSIRO's Data61 Redfern, Sydney facility claims world leading face recognition expertise, allowing for close to real-time identification of individuals across a database potentially numbering in the millions of subjects. It is a maxim of cyber security that it starts with strong physical security boundaries, particularly around human movements (eg 'ghosting' through access-controlled entries). The startup intends to target larger corporate customers in commercially sensitive sectors with its system. Facial recognition systems can be used as a defensive (denial of entry), as well as an operational (alerting & tracking) and forensic (what happened) mechanism. However, both the false positive and false negative rates can be too high in various circumstances (eg lighting, crowds, occlusions) to have required trust in the systems. The company can utilise a NSW CSN Cyber Voucher to engage with one or more NSW CSN University Members to fully benchmark global best practice of publicly available face recognition algorithms to seek improvements in its own system.

https://www.abacusnews.com/who-what/skynet-chinas-massive-video-surveillance-network/article/2166938

https://www.news.com.au/technology/online/big-brother-chinas-chilling-dictatorship-moves-to-introduce-scorecards-to-control-everyone/news-story/6c821cbf15378ab0d3eeb3ec3dc98abf

https://www.forbes.com/sites/zakdoffman/2019/01/13/chinese-media-claims-nypd-is-using-beijing-controlled-facial-recognition-is-it-true/#1d1bb91a592a

https://www.smh.com.au/business/companies/do-whatever-you-have-to-woolworths-staff-rewarded-for-spying-on-pokie-players-20180227-p4z1zw.html

Use Case 4

Social Engineering Attacks

Context variables

An existing Wollongong based cyber-threat assessment services agency intends to use its expertise in machine learning and cognitive psychology to develop a deployable model of how company employees' present mental state (eg tired or stressed vs fresh and relaxed) and their work context (eg high / low pressure, repetitive) might affect their likelihood of being drawn into a phishing attack. More than 40% of cyber-security related incidents in business are still via phishing. The startup believes an 'early warning' system may significantly reduce the cases of phishing. A key part of their intended solution is developing a method for 'bootstrapping' an enterprise wide "Alert Algorithm" for each potentially vulnerable employee within each of their client companies. Via a NSW CSN Cyber Voucher the Wollongong services agency can engage with a Member NSW University to develop a 'playbook' of the mechanics involved in the design and implementation of such an approach.

https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00691/full

Use Case 5

5G & IoT Security for 'Connected Automated Vehicles' (CAVs) around busy campuses, as transit vehicles, or on golf courses

A NSW company currently servicing the electronic golf cart market believes that these vehicles will morph into being fully autonomous, but always network connected, and be used in an increasingly wide range of circumstances (not only for golf courses movement, but for aged care facilities, retirement and holiday villages, resorts, company campuses, universities, and as short range transit options to public transport stations). Meanwhile, 5G is emerging as a global cellular technology which may be utilised as a network infrastructure component to connect these CAVs for real-time traffic management purposes. Being connected devices, these CAVs are vulnerable to cyber security concerns. At this point, however, the security properties of 5G are not well understood but need to be in order for CAVs relying on 5G to build security into their operation. This NSW company can utilise a NSW CSN SME Cyber Voucher to engage with a Member NSW University to provide an up to date assessment of where 5G currently stands, its likely development path, and options for how the company's own product strategy might evolve in light of 5G.

https://www.automotiveworld.com/webinars/automotive-cyber-security-protecting-the-car-from-the-cloud/

https://www.continental-automotive.com/en-gl/Cyber-Security

Use Case 6

Addressing Wine Fraud via Provenance Tracking

A Hunter Valley based wine storage and logistics company is seeking to expand its business into wine provenance tracking for fine wines that are intended for longer term drinking and for wine collectors that typically access and trade wine on active online auction sites. The counterfeiting of wine, including Australian wine, is a growing concern affecting the wine economy via these secondary electronic markets. The company believes that by combining innovative 'hidden watermark' labelling and sealing, machine vision and IoT based device (bottle) tracking they can help secure the provenance of high value wines. The company also wishes to explore the use of, or development of their own, blockchain-based platform to provide transparent, real-time, enquiry of the provenance history of tracked wines to their target subscriber base. The company can utilise a NSW CSN Cyber Voucher to engage with a Member NSW University to provide an assessment of the technical and economic merits and limitations of the various existing blockchain technologies for their intended purpose.

https://www.profitablehospitality.com.au/blog/wine-fraud-is-here-in-australia-and-it-could-happen-to-you/

https://www.abc.net.au/news/2018-08-04/australian-lookalike-wines-big-sellers-on-chinese-online-giant/10064836

https://www.everledger.io/industry-applications

Use Case 7

Building Automation Systems

A Lane Cove based company, XYZ Pty Ltd, has been a local leader in the building automation market for over thirty years. With clients including major airports, commercial property developers and managers, and financial institutions, XYZ has steadily grown its portfolio of services and products from third-party international vendor representation through to local design, manufacture, installation and on-going operation of increasingly integrated, and cloud based, building automation systems. Security is now looming as a key attribute of these systems, especially as connected devices and sensors proliferate, new network types are added, and remote cloud operation becomes prevalent. XYZ would like to use a NSW CSN Voucher to have a NSW Member University provide a first-pass Security Scan of one if its existing client sites (with the client's approval) to gain an in-house 'vulnerability view' of potential weak spots. The results will assist guide XYZ in its further product and service development and improve the security aspect of its offering to NSW businesses.

Use Case 8

GDPR & Open Banking in Australia

A Sydney Startup Hub based Fintech startup is working on a data sharing platform that straddles the fine line between GDPR and Open Banking. While GDPR is a European centric data privacy standard its ramifications are being felt worldwide. Meanwhile, Open Banking initiatives, such as those in the UK and those being proposed in Australia, increase opportunities for FinTech companies to gain access to – and potentially share -- customer related data between themselves to gain better customer insights to improve overall customer offerings and experience. Open Banking is an opportunity, while the evolving legal (and moral) standards around data ownership, control and use - which GDPR represents - presents a real challenge. The startup wishes to use a NSW CSN Cyber Voucher to prepare a White Paper, co-authored with a NSW Member University, on the present unresolved state of data privacy and sharing issues and how approaches such as Differential Privacy can provide certain 'guarantees' to alleviate many concerns.

Use Case 9

Satellite communications security

A small Maitland based company has partnered with a more experienced Sydney and Colorado company specialising in Ground Station User Interfaces to add terrestrial communications security 'health' as a component to the console's monitoring. The team intends to collaborate and build a relationship with a NSW Member University to prepare a tender response for a recent Geoscience Australia Request for Information (RFI). Geoscience Australia has commenced a RFI process in a market research exercise to progress the identification of high-level cybersecurity risks associated with the proposed Australian Satellite -Based Augmentation System (SBAS) architecture, which may aid in the development of an operational Cybersecurity Strategy. The Maitland company will use a NSW CSN Cyber Voucher to build its relationships and augment its expertise around communications network security and draft an RFI Response for the tender.

https://australiancybersecuritymagazine.com.au/cyber-security-strategy-satellite-based-augmentation-system-sbas/