2023 HUNTERNET FUTURE LEADERS PROGRAM

Newcastle Airport

# NEWCASTLE AIRPORT CYBER SECURITY STRATEGY

Cyber Air Consultancy

# Who is Cyber Air?

## BRYCE WOOD - BUSINESS DEVELOPMENT MANAGER

Bryce is currently the Purchasing Officer for DSI Underground APAC and holds a Certificate III in Business, Certificate IV in Purchasing, and a Certificate III in Technical Engineering.

## ADAM SNEDDEN - OT CYBERSECURITY SPECIALIST

Adam is a Chartered Professional Engineer with Engineers Australia. He currently works as a Lead IT/OT Engineer at Alliance Automation and specialises in cyber security of industrial control systems.

## BRITTNEY NASH - PEOPLE ENABLEMENT MANAGER

Brittney is a Consultant at Aon and holds a Certificate IV in Work Health and Safety, Diploma of Human Resources, and is studying towards a Diploma of Law.

## HIREN PATEL - BUSINESS IMPROVEMENT SPECIALIST

Hiren is a Business Intelligence Manager at Port of Newcastle. He has worked across different business sector in data analytics, business analysis, and process improvement.

## DAMON VANDERMAAT - DEVELOPMENT MANAGER

Damon has a PhD. in Engineering and currently works as a Product Development Manager at ResTech, based at the University of Newcastle.

> *“Our vision is to help the Hunter Region respond to the cyber threats exacerbated by our world's shifting geopolitical landscape”*
>
> *Cyber Air Team*

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

Global geopolitical shifts are trending the world towards a more uncertain future as evident by mounting tensions in Eastern Europe and the Asia-Pacific regions. Warfare is no longer limited to physical engagement and a new era of global conflict is unfolding in cyber space. The tools and weapons developed for cyber warfare are increasingly spilling over and affecting civilian institutions.

Cyber Air has partnered with Newcastle Airport to deliver a strategy to address the evolving cyber threat landscape caused by geopolitical shifts. This strategy focuses on leveraging the opportunities created by this megatrend for the economic and social benefit of the entire Hunter Region, while also increasing the Airport's preparedness and adaptability to the threats posed by it. Cyber Air recommends that Newcastle Airport explores the following key strategic objectives:

- Develop and implement a Cyber Security Management System tailored to address the distinct operational technology cyber security challenges at Newcastle Airport. This system aims to unlock the potential of online, data-driven operations while upholding security standards and mitigating exposure to cyber threats.

- Engage, support, and facilitate their key Astra Aerolab Precinct defence tenants to meet their DISP membership requirements. This will ensure the secure operation of their tenants and cement Astra as a precinct-of-choice for the defence industry, driving economic growth for the region.

- Partner with key educational institutions to develop a Cyber Security Education Hub in the Astra Aerolab Precinct. This will help address the national skill shortage and position Hunter businesses at the forefront of cyber security readiness and resilience supporting further economic activity in the region.

# CYBER SECURITY - THEATS AND OPPORTUNITIES

In today's digital environment, our data and assets are increasingly being stored in computer systems and networks. The digital environment has flattened our global geography and threats are no longer limited to the physical world.

Cyberattacks are a growing geopolitical risk, becoming larger, more sophisticated, and more persistent. They are a significant threat to individual organisations and national security. Cyberspace is becoming the new battleground for states to jostle for control over critical technologies and to set the agenda for technical standards globally [1].

The repercussions of persistent cyberattacks could have a wide-reaching impact on financial markets and the economy. Government networks, private sector networks and infrastructure are all susceptible to hacking and espionage.

International cooperation to effectively address cyberattacks is challenging given the complex geopolitical relationships between many countries.

It's likely that cyberthreats will continue at least as long as physical conflict does. While the impacts of individual attacks will vary, the broader effects of a heightened threat landscape will be felt by organisations worldwide.

## STUXNET

*Stuxnet is a virus, thought to be developed by the US and Israel, that targeted and substantially damaged the nuclear program of Iran. The virus crossed the air gap to infect Iran's offline OT system. It reported normal operation to the control system while systematically destroying the equipment [2].*

## MAERSK

*In 2017, Maersk was affected by the NotPetya virus. NotPetya was originally developed by Russia to target Ukrainian tax software. Maersk, having operations in Ukraine, became collateral damage in global cyber conflict when its network became infected. The virus encrypted the computers responsible for operating 76 ports and 800 vessels, rendering them completely inoperable for 10 days resulting in losses of USD $250-$300M [3].*

## AUSTRALIA AS A GLOBAL LEADER

*In December 2022, the Federal Government released its 2023-2030 cyber security strategy highlighting the Government's desire for Australia to be a global leader in cyber security. To that end, the Government has launched the Cyber Sec. Skills Partnership & Innovation Fund to upskill Australian workers and businesses [4].*

# BUSINESS IMPACTS OF A CYBER ATTACK

The companies that will be successful in the future are those that disrupt and transform. Cyber resilience is a competitive advantage and needs to be discussed at the highest levels of management. The costs of getting cyber resilience wrong are numerous as per 14 business impacts of cyber-Incidents [32]

**Above** the surface

- Technical investigation costs.
- Customer breach notifications.
- Regulatory compliance.
- Legal fees and litigation.
- Post breach customer protection.
- Public relations breakdown.
- Cyber security remediation.

**Below** the surface

- Insurance premium increases.
- Increased cost to raise debt.
- Impact of operation disruption or destruction.
- Value of lost contract revenue
- Reputational damage.
- Loss of IP.
- Lost value of customer relationships.

Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching USD $10.5 T annually by 2025 [5]. 76,000 cybercrimes were reported in Australia in 2022-23 [6]. For Newcastle Airport, these impacts may include:

- Operational Disruptions - leading to flight delays, cancellations, or grounding of fleets.
- Legal Action - from passengers and partners.
- Safety Risks - to passengers and other physical assets.
- National Security Implications - a coordinated cyberattack on the aviation sector could disrupt military.
- Logistics - impede emergency response capabilities or serve as a prelude to physical terrorist attacks.

**Losses**

Globally, cybercrime costs USD $6 T per year. [30]
The cost of cybercrime to Australia's economy is AUD $29 B per year. [33]

**Incidents**

76,000 cybercrimes were reported in Australia in 2022-23. [6]
In Europe, 61% of all cyber-attacks in 2020 targeted airlines [7].
Cybercrime has increased by 600% since COVID-19. [29]

**Requirements**

Nearly 17,000 more cyber security workers needed in Australia by 2026-27 [8].
Current growth is not sufficient to meet medium-term shortfall [8].

# NEWCASTLE AIRPORT

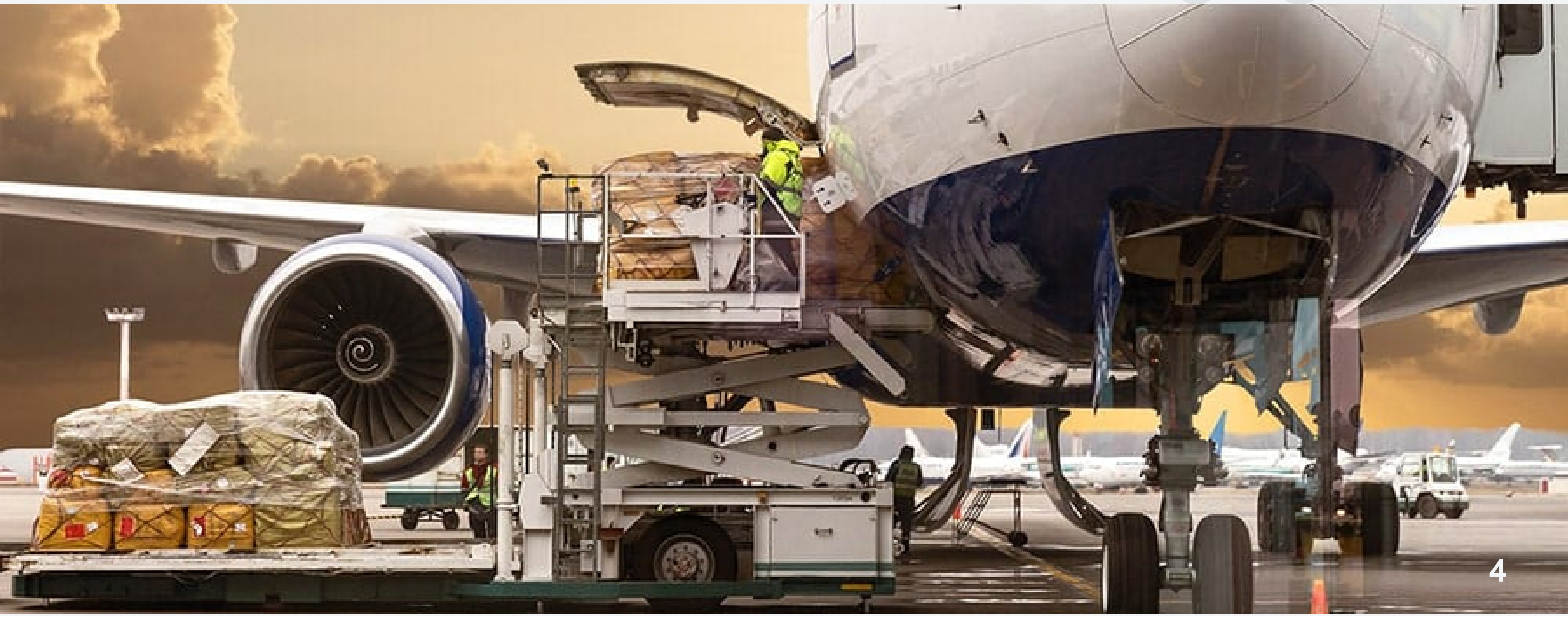
Newcastle Airport Pty Limited (NAPL) is jointly owned by The City of Newcastle and Port Stephens Council. Newcastle Airport is situated in Williamtown, NSW, 15km from Newcastle, 22km from Nelson Bay, and 175km north of Sydney.

Australia's sixth largest regional airport, Newcastle Airport serves a catchment area of 1.1 million people.

Offering 12 direct routes to destinations within Australia, with the ability to also service international destinations. Newcastle Airport currently has the ability to depart 8 planes every hour and handled a record 1.3 million passengers in 2017.

Newcastle Airport operates under a direct lease agreement from the Department of Defence, making it unique in that it sits outside the provisions of the Commonwealth Airport Act 1996.

> *“The Airport’s Board of Directors are focused on the Airport being a driver of economic activity in the Hunter Region”*
>
> *Shane Murray - Property Planning & Development Manager at Newcastle Airport*



In March 2018, Newcastle Airport released its 2036 Newcastle Airport Vision outlining their expansion plans and proposed developments.

One of the key components of the vision is the development of the Astra Aerolab. The Astra Aerolab will provide collaborative space for advanced manufacturing, defence, and aerospace technology, empowering nationally significant research, innovation, and education opportunities.

Cyber Air and the team at Newcastle Airport identified the growing threat of cyberattacks, and the potentials risks to Newcastle Airport and Astra Aerolab as it continues to develop and grow its business in these geopolitically unstable times.

Through the process of exploring the threats, risks and opportunities in this rapidly evolving space, Cyber Air identified that Newcastle Airport should explore three major strategic opportunities:

## OT SECURITY

*Is Newcastle Airport's Operational Technology (OT) secure? Would they know if their baggage handling or passenger screening systems were compromised?*

## DEFENCE NEEDS

*Newcastle Airport will host defence partners in the Astra Aerolab. What are the cyber security requirements for these tenants, and how can Newcastle Airport support them as facility owners and managers?*

## EDUCATION

*Australia is facing a shortage of skilled cyber security professionals. How can Newcastle Airport help address this and inspire school students to pursue a career in cyber security or aviation?*

## ENGAGEMENT TIMELINE

### First Contact

9 Aug

Cyber Air contacted Shane Murray to assist Newcastle Airport respond to the CSIRO 'Global Megatrends'.

### Discovery

16 Aug

Cyber Air engaged in a half-day discovery session with Newcastle Airport. This identified Geopolitical Shifts as an area of interest for the airport.

### Scope Confirmed

4 Sept

A follow-up meeting confirmed the project scope was to explore the threats and opportunities relating to cyber security.

### Data Gathering

13 Sept

Cyber Air hosted a short workshop to explore NAPL's knowledge of cyber security in OT systems.

# OPERATIONAL TECHNOLOGY CYBER SECURITY

### What is Operational Technology?

Operational Technology (OT) is the use of hardware and software to monitor and control physical processes, devices, and infrastructure. [9]

The internationally recognised and accepted standard in OT cyber security is ISA/IEC 62443.

ISA/IEC 62443 recommends against approaching cyber security from a project perspective with a start and end date. Security level will often decline over time using a project approach as cyber security risk is constantly evolving. The standard recommends developing and implementing an organisation-wide cyber security management system (CSMS) that includes elements to reassess risk and take corrective action over time. The chief information security officer (CISO) becomes responsible for managing and maintaining the CSMS. The objective of the CSMS is to meet Newcastle Airport's current and future needs [10].

Disruption to Newcastle Airport's operational technology systems could cause flight delays, loss of revenue, or enable prohibited items to board aircraft. Air gapping is not 100% secure as demonstrated by the Stuxnet virus. It is imperative to not only consider the cyber security of existing systems but to plan for potential future systems in an increasingly connected world.

### Benefits

An effective Cyber Security Management System will mitigate the effects of a cyber security incident, and enable faster response and remediation in the event of an attack. It will give Newcastle Airport confidence to securely integrating OT & IT systems to realise valuable business data. Furthermore, it aids in meeting regulatory requirements, such as the Security of Critical Infrastructure Act 2018.

## Newcastle Airport's OT Systems

Baggage Handling

Building Access Management

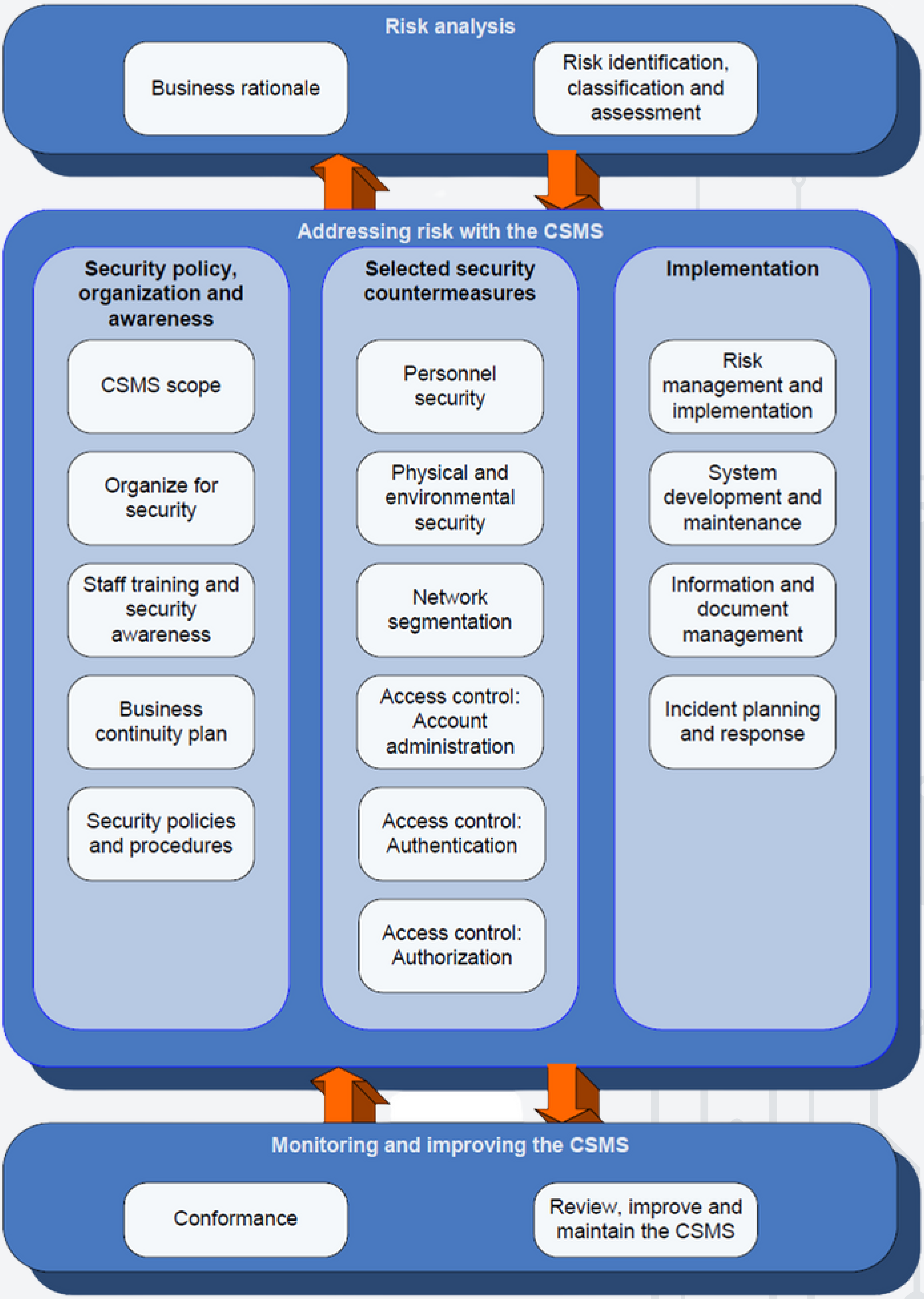
Carpark Management

Passenger Screening

CCTV Systems

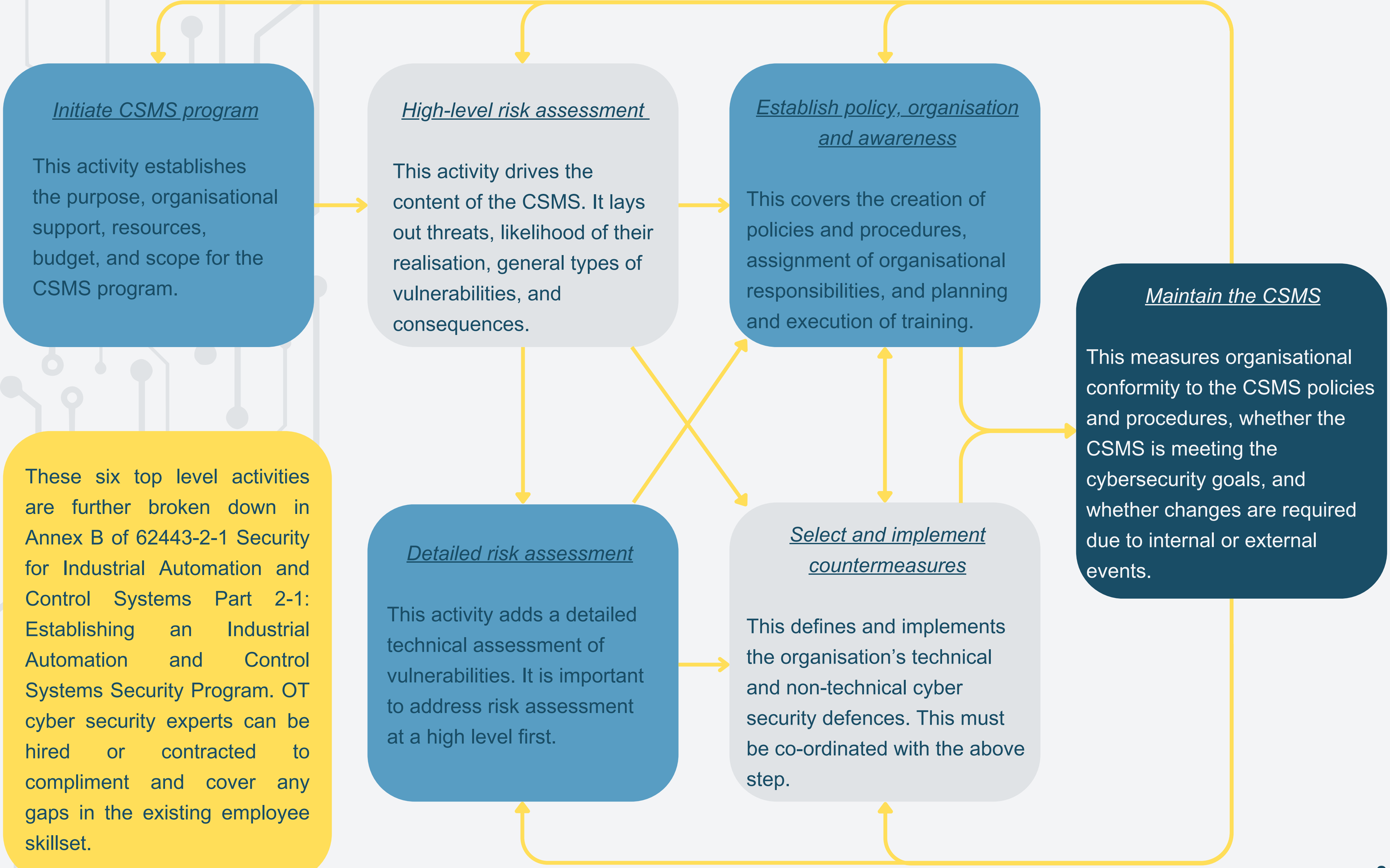
# CYBER SECURITY MANAGEMENT SYSTEM

The elements of a Cyber Security Management System (CSMS) are presented in three main categories: Risk analysis, Addressing risk with the CSMS, and Monitoring and improving the CSMS. Developing a functioning CSMS is a journey that can take months or years to achieve. The process to develop a CSMS can be broken down into six top level interconnected activities [11].


Risk analysis
Business rationale
Risk identification, classification and assessment
Addressing risk with the CSMS
Security policy, organization and awareness
CSMS scope
Organize for security
Staff training and security awareness
Business continuity plan
Security policies and procedures
Selected security countermeasures
Personnel security
Physical and environmental security
Network segmentation
Access control: Account administration
Access control: Authentication
Access control: Authorization
Implementation
Risk management and implementation
System development and maintenance
Information and document management
Incident planning and response
Monitoring and improving the CSMS
Conformance
Review, improve and maintain the CSMS

Elements of a Cyber Security Management System (CSMS) [11]

## Process to develop a Cyber Security Management System (CSMS) [11]



*Initiate CSMS program*

This activity establishes the purpose, organisational support, resources, budget, and scope for the CSMS program.

*High-level risk assessment*

This activity drives the content of the CSMS. It lays out threats, likelihood of their realisation, general types of vulnerabilities, and consequences.

*Establish policy, organisation and awareness*

This covers the creation of policies and procedures, assignment of organisational responsibilities, and planning and execution of training.

*Maintain the CSMS*

This measures organisational conformity to the CSMS policies and procedures, whether the CSMS is meeting the cybersecurity goals, and whether changes are required due to internal or external events.

*Detailed risk assessment*

This activity adds a detailed technical assessment of vulnerabilities. It is important to address risk assessment at a high level first.

*Select and implement countermeasures*

This defines and implements the organisation's technical and non-technical cyber security defences. This must be co-ordinated with the above step.

These six top level activities are further broken down in Annex B of 62443-2-1 Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program. OT cyber security experts can be hired or contracted to compliment and cover any gaps in the existing employee skillset.

## FIVE CRITICAL CONTROLS FOR CYBER SECURITY

Cybersecurity is not a one-size-fits-all and any CSMS developed will need to be bespoke for Newcastle Airport. Cyber Air recommends seeking the advice a dedicated OT cyber security consultant to build a CSMS. However, there are five critical controls that Newcastle Airport can implement, alongside development of their CSMS, to begin their OT cyber security journey [31].

| Critical Control | Description |
|---|---|
| **OT Incident Response Plan** | This plan is distinct from IT's. It involves different device types, communication protocols, different types of tactics, techniques, and procedures (TTPs) specific to the industrial threat groups. Cyber Air recommends creating a dedicated plan that includes the right points of contact, including 3rd parties that manage your systems, as well as thought-out next steps for specific scenarios. Consider table-top exercises to test and improve response plans. |
| **A Defensible Architecture** | OT security strategies often start with hardening the environment. Removing extraneous OT network access points, maintaining strong policy control at IT/OT interface points. Cyber Air recommends that Newcastle Airport implements a demilitarised zone (DMZ) to control all ingress and egress traffic with tools such as firewall whitelisting, secure proxies, and data diodes. |
| **Visibility and Monitoring** | It is important to maintain an asset inventory that encompasses vulnerabilities and mitigation plans. Cyber Air recommends passive network monitoring at key interface points. These monitor for threats and contribute to an up-to-date asset inventory. Some dedicated OT monitoring tools are Dragos, Claroty, and Nozomi. |
| **Secure Remote Access** | Implement multi-factor authentication where possible. Utilise Newcastle Airport's existing IT systems, such as VPNs and jump hosts. Avoid 'backdoors', such as 4G routers, that allow unmonitored remote access. |
| **Risk-Based Vulnerability Management** | Knowing the vulnerabilities and having a plan to manage them. Cyber Air recommends subscribing to vendor alerts to stay updated on emerging vulnerabilities. |

# MEETING THE NEEDS OF DEFENCE TENANTS

The Astra Aerolab precinct is being developed as a campus dedicated to housing aeronautical and Defence industry companies. The precinct is being developed on freehold land owned and developed by Newcastle Airport. The Airport intends to lease the building space to these companies. To do this effectively, Newcastle Airport needs to understand and respond to the physical and cyber security requirements of these companies.

Companies that work in the Defence industry are required to be members of the Defence Industry Security Program (DISP). Being a member of the DISP requires that the company comply with specific rules around governance, personnel vetting and technical requirements for building access and information storage. Compliance with these rules is assessed by the Defence Security and Vetting Service (DS&VS). [12]

As building service providers, it is critical that the Property Development Team at Newcastle Airport understands the requirements of the DISP so that they can offer their tenants the infrastructure they need to work securely. This will greatly benefit their tenants and build the reputation of the Astra Aerolab as a precinct-of-choice for the Defence industry.

## NEED

- *Defence tenants must operate within a strict framework to work securely.*
- *Building requirements feed heavily into this framework.*

## STRATEGY

- *Newcastle Airport identifies and understands the needs of their tenants.*
- *Newcastle Airport provides the required building security campus-wide.*

## BENEFIT

- *DISP Member tenants satisfy their obligations.*
- *Astra Aerolab established as 'precinct-of-choice' for Defence industry companies.*
- *The Hunter benefits from sustainable economic development.*

## WHAT IS THE DISP MEMBERSHIP PROGRAM

The DISP program is stratified into multiple membership levels depending on the sensitivity of the information being handled by the organisation. These levels are [12]:

Entry Level: Makes use of OFFICIAL and OFFICIAL: Sensitive material.
Level 1: Makes use of PROTECTED material.
Level 2: Makes use of SECRET material.
Level 3: Makes use of TOP SECRET material.

The level of information being handled by the company directly links to the controls put in place to maintain protection of the material used by the company. These controls are defined by the Defence Security Principles Framework (DSPF) [13].

The Defence Security Principles Framework defines 4 facets of security compliance and controls that must be adhered to. Each facet has its own requirements to achieve each of the security levels. I.E, in order to operate a DISP Level 2, a company must comply with the level 2 requirements for all of governance, personnel, physical and information security.

**Governance:** The DSPF requires that the applying company appoint a Chief Security Officer (CSO) and a Chief Information Security Officer (CISO). These positions are empowered and responsible for developing security plans and policies, maintain risk registers and incident reports for the business.

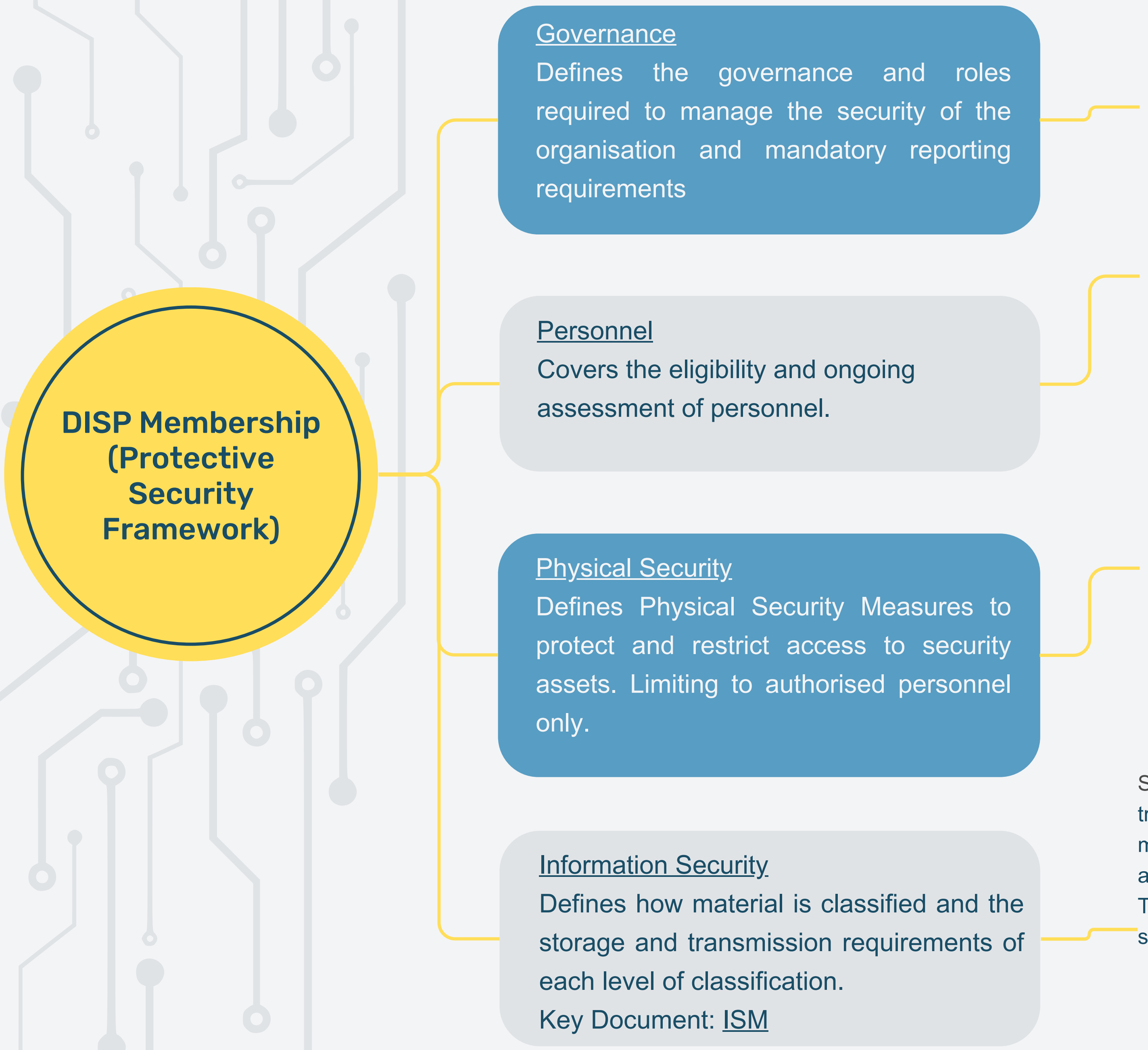
**Personnel:** This facet defines the level of vetting required for personnel to work with secure material. It also defines the ongoing training and vetting requirements to maintain their security clearance.

**Physical Security:** Each of the security levels have corresponding requirements for how buildings need to be constructed to provide an appropriate level of security. The 'zones', that define the level of protected material that can be used and stored, must be accredited by DS&VS.

**Information Security:** Similar to physical security, but for Information and Communications Technology (ICT) systems. The Information Security Manual (ISM) [14] defines the details requirements for each DISP level.

## Framework Areas

## Strategic Relevance



**DISP Membership (Protective Security Framework)**

Governance
Defines the governance and roles required to manage the security of the organisation and mandatory reporting requirements

- Identifies the key stakeholders to engage with and determines the needs of tenants. They will be able to provide critical guidance on what level of building security is required.
- CSO - Chief Security Officer
- CISO - Chief Information Security Officer

Personnel
Covers the eligibility and ongoing assessment of personnel.

- Provides awareness of DISP vetting requirements.

Physical Security
Defines Physical Security Measures to protect and restrict access to security assets. Limiting to authorised personnel only.

- Specifies building layout requirements for handling secure information. Understanding what level of material the Airport's defence tenants handle will affect the zoning requirements when designing buildings.
- Zone 1 - Entries and Foyers
- Zone 2 - General office space
- Zone 3 - Restricted Area. Access to PROTECTED material.
- Zone 4 - Restricted Area. Access to SECRET material.
- Zone 5 - Restricted Area. Access to TOP SECRET material.

Information Security
Defines how material is classified and the storage and transmission requirements of each level of classification.
Key Document: ISM

Specifies how sensitive information must be stored and transmitted within buildings. Understanding what level of material the Airports defence tenants handle will affect the allowances that are needed for networking in building design. The Information Security Manual (ISM) details requirements such as:

- Cabling Type
- Cable Registers
- Security Layering

# DEFENCE TENANT ACTION PLAN

The role of the Property Development Team will be critical to ensuring that the needs of their defence tenants are met. Close engagement with the company CSO and CISO is crucial. The Property Development Team is recommended to adopt the following approach.

## WORK WITH KEY DEFENCE TENANTS

- Engage with tenant company CSO and CISO.
- Determine what DISP membership level they hold.
- Understand the type of assets they need to protect (physical, digital etc.)

## ENGAGE WITH AN EXPERIENCED DESIGN CONTRACTOR

- Work with DS&VS to identify a suitable design and build contractor.
- Review plans with company CSO and CISO.
- Certify plans with DS&VS.

## SUPPORT AND FACILITATE CONSTRUCTION

- Manage relationship with building contractor(s).
- Maintain engagement with tenant CSO and CISO.
- Undertake collaborative inspections when critical infrastructure is close to completion.

## SUPPORT CERTIFICATION PROCESS

- When construction is complete, facilitate inspection and certification with DS&VS.

## PROVIDE ONGOING SUPPORT

- Help the defence tenants maintain their physical security accreditation.
- Appoint a CSO and CISO for the Airport and maintain a risk and incident register for the whole Astra Aerolab precinct.

# EDUCATING THE REGION

Newcastle Airport is facing the challenges of a shortage of skilled cyber security professionals in Australia and limited aviation industry specific cyber security training. To address these issues, Cyber Air proposes a series of initiatives including inspiring school students, creating a dedicated aviation cyber security course, and establishing an education hub.

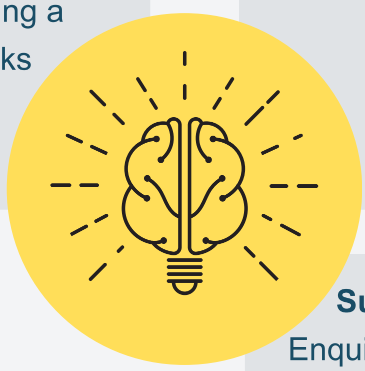
## INSPIRING SCHOOL STUDENTS OF THE HUNTER REGION

A crucial element of addressing the skills shortage is ensuring that there is strong and accessible higher and vocational education. This will support school aged students develop skills in this rapidly growing industry.

Newcastle Airport can help to promote the importance and relevance of STEM opportunities and pathways, which encompasses cyber security, by becoming involved in a STEM Industry Partnership [15]. There are various ways that Newcastle Airport can provide support including:

**Provide real-world learning experiences**
Partner with a school to facilitate a real-world STEM project. This could encompass a student visit to Newcastle Airport for exposure to real world contexts and challenges, and students completing a group project on cyber security risks specific to the aviation industry thereafter.

**Connect with students as role models**
Utilise experienced STEM professionals, such as IT Manager Michael Rae, to host talks with students. Additionally, have employees act as mentors for students, providing guidance about STEM opportunities / pathways.



**Support school to work pathways**
Enquire about Newcastle Airport joining the existing partnership network with Hunter River High School, to take part of an innovative skills-based program that focuses on aeronautical and related aerospace industries [16]. The existing partnership includes the University of Newcastle, and HunterNet members, Varley Group, and Ampcontrol. Newcastle Airport to review whether they partake in this program with the view of expanding the pathway to include Certificate IV in Cyber Security.

# PROPOSING A CYBER SECURITY COURSE SPECIFIC TO THE AVIATION INDUSTRY

With the Astra Aerolab positioning itself as a world leading aerospace and innovation precinct, Cyber Air proposes that Newcastle Airport cements its status as an industry leader and pioneer in Aviation Regulatory Training. Newcastle Airport should utilise its strong ties with HunterNet, University of Newcastle, and other industry partners to apply for a course accreditation of 'Aviation Cyber Security' to the Australian Skills Quality Authority (ASQA). This would be a first of its kind offering in Australia [17].

## NEED

- The Australian Government wants to be 'the most cyber secure nation by 2030' however, there is no cyber security training that is specific to the aviation industry in Australia [4].
- Countries such as Germany, United States, Singapore, and United Kingdom already offer aviation cyber security training.
- Australia's AVI20118 - Certificate II in Transport Security Protection [18] and Air Cargo Security Awareness Training [19] offered by the Cyber and Infrastructure Security Centre make no mention of cyber security.

**What are other countries offering?**

- 'Aviation Cyber Oversight' course offered by UK Civil Aviation Authority International [20].
- 'Aviation Cyber Security' offered by The International Air Transport Association (IATA) whose members include Qantas and Virgin [21].
- 'Foundations of Aviation Cybersecurity Leadership and Technical Management' offered by the International Civil Aviation Organization [22].
- 'Aviation Cyber Security' course offered by Joint Aviation Authorities [23].

## BENEFIT

- Showcase your strong ties with HunterNet, University of Newcastle and other industry partners.
- The proposed 'Aviation Cyber Security' training will be the first offering of its kind in Australia.
- The world leading aerospace and innovation precinct, Astra Aerolab, will have its own training course.
- Newcastle Airport cements its status as an industry leader and pioneer in Aviation Regulatory Training.
- Generate income by engaging in a licence or franchise agreement for other Registered Training Organisations to utilise the course [24].

# AVIATION CYBER SECURITY COURSE DEVELOPMENT ACTION PLAN

| STEP | PROCESS |
|---|---|
| **Step 1 - Propose VET course concept** | • Newcastle Airport to utilise its existing partnership with HunterNet, and other industry partners to form an industry working group.<br>• The industry working group will be responsible for collecting and collating the required information to complete the VET course application concept form, including providing evidence there is a real industry need for your course. |
| **Step 2 – Course development** | • The industry working group is to collaborate with the University of Newcastle to develop and submit the national course document, ensuring it meets the Standards for VET Accredited Courses 2021 and Australian Qualification Framework [25].<br>• The industry working group is to consult with Jobs and Skills Councils (JSCs) i.e., Future Skills Organisation who cover the cyber security and Industry Skills Australia who cover the aviation industry.<br>• For additional assistance with this step review similar courses offered outside of Australia (refer to prior page for examples). |
| **Step 3 – Course submission** | • The industry working group is to submit the application as a collective as they will own the accredited course. |
| **Step 4 – Application assessment** | • One of ASQA's assessors will be assigned to assess the application.<br>• If a notice of non-compliance is provided the industry working group will have to address and re-submit the application within 20 days. |
| **Step 5 – Decision** | • If approved, ASQA will advise course owner number and course code, any conditions on the accreditation, and any duties to manage and monitor your course.<br>• ASQA will add the course details to the national register along with your details as the course owner.<br>• Should one of the members of the industry working group be a recognised Registered Training Organisation (RTO) and wish to deliver this training they will need to add it to their scope of registration.<br>• Alternatively, the industry working group can engage in a licence or franchise agreement with an RTO to utilise the course. |

# DESIGNING A DEDICATED CYBER SECURITY EDUCATION HUB

Collaboration

STEM Partnership

Aviation Cyber Security Course

Cyber Security Focused Living Laboratory

Industry Leading

**What is a ‘Living Labratory’?**

The ‘living laboratory’ is an innovative partnership with the University of Newcastle. Students work in the ‘living laboratory’ to solve unique challenges facing Newcastle Airport, such as with the baggage handling systems [26].

One of the many benefits of the Astra Aerolab Precinct is that it enables collaboration between world leading researchers and educational institutions, all of whom would be at risk of a cyber attack. It is recommended that the Astra Aerolab has an area dedicated to cyber security education.

Newcastle Airport could use this space to expand on their current partnership with the University of Newcastle, to develop a cyber security focused ‘living laboratory’.

Additionally, the space could be used in partnership with a Registered Training Organisation to facilitate the proposed aviation specific cyber security course.

**Grants**

The Australian Government recognises the need for further education in this space and frequently offer grants, such as the $70.3M offered through The Cyber Security Skills Partnership Innovation Fund [27]. The Fund provided industry and education providers with funding to deliver innovative projects that met local requirements, to quickly improve the quality or availability of cyber security professionals in Australia.

In the 2023-24 budget, the Federal Government has allocated a total of $101.6M over five years “to support and uplift cyber security in Australia”. Cyber Air recommends that Newcastle Airport should monitor for future grants that could be utilised towards developing the cyber security lab [28].

**Venue for iSTEM**

A dedicated Cyber Security Hub would be an ideal location for students to complete the 10 week iSTEM cyber security training and provide students exposure to what specialist equipment or cyber security facilities look like.

# CONCLUSION

The ever-evolving landscape of cybersecurity, driven by geopolitical shifts, presents a multifaceted challenge that demands continuous adaptation and vigilance. As nations jockey for supremacy in the digital realm, the vulnerabilities and threats associated with cyber warfare have escalated to unprecedented levels. It is evident that the interplay between geopolitics and cybersecurity is inextricable, and the ramifications of this dynamic are far-reaching. To navigate this complex terrain successfully, Newcastle Airport must prioritize cybersecurity as a foundational element of their security and strategic agenda.

Newcastle Airport is recommended to adopt proactive measures, including the development of resilient cyber infrastructure and securing of their operational technology. These are crucial components of a comprehensive cybersecurity strategy. Moreover, fostering a culture of cybersecurity awareness and education at all levels of society is imperative to **reduce and mitigate the threat of cyber-attacks.**

Working securely is fundamental for companies who partner with the Department of Defence. The rules and regulations that govern how Defence partners operate are in place to ensure that they are protected from geopolitical risks and nefarious actors. Newcastle Airport is recommended to actively engage with their defence tenants to help them operate securely. This will help to establish the Astra Aerolab brand as a preeminent Defence precinct, attracting more Defence contractors to the area helping to build **sustainable, long term economic benefit for the Hunter Region.**

The shortage of skilled cyber professionals is not a problem that is unique to one organisation or region, however Newcastle Airport is well positioned to utilise its strong relationship with other Hunter organisations to help address this. Through a partnership with STEM, Newcastle Airport can inspire the region’s next generation of cyber security professionals. Whilst the proposed ‘Aviation Cyber Security Training’ will **attract more people to the Hunter region**.

As we move forward, it is essential that we remain agile, adaptable, and forward-thinking in our approach to cybersecurity. Geopolitical shifts will continue to shape the threat landscape, but by embracing innovation, and embracing a holistic approach to cybersecurity, we can better defend against cyber threats and safeguard the integrity and security of our digital world. In doing so, we can strive for a future where geopolitical conflicts do not compromise the integrity and resilience of our digital infrastructure, ensuring **a safer and more secure cyber environment for all.**

# REFERENCES

[1] Naughtin C, et al. “Our Future World: Global megatrends impacting the way we live over coming decades,” CSIRO, Brisbane, 2022

[2] J. Rysider, “Stuxnet,” Darknet Diaries, 02 01 2019. [Online]. Available: https://darknetdiaries.com/episode/29/. [Accessed 2023].

[3] J. Rysider, “NotPetya,” Darknet Diaries, 24 12 2019. [Online]. Available: https://darknetdiaries.com/transcript/54/. [Accessed 2023].

[4] A. M. (. M. H. A. D. R. F. Andrew Penn AO (Chair), “2023-2030 Australian Cyber Security Strategy”.

[5] S. Morgan, “Cybercrime To Cost The World $10.5 Trillion Annually By 2025,” Cybercrime Magazine, vol. 2, no. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/, 2020.

[6] N. Dekker, “Critical Cyber Crime Statistics in Australia 2023,” Eftsure, no. https://eftsure.com/en-au/statistics/cyber-crime-statistics/#:~:text=1.-,In%20the%20Annual%20Cyber%20Threat%20Report%202022%2C%20the%20ACSC%20received,%2C%20corporate%20espionage%2C%20and%20fraud., 07 February 2023.

[7] W. B. III, “New Eurocontrol Data Shows Airlines Increasingly Becoming Targets for Cyber Attacks,” no. https://www.aviationtoday.com/2021/07/12/new-eurocontrol-data-shows-airlines-increasingly-becoming-targets-cyber-attacks/#:~:text=Commercial%20airlines%20accounted%20for%2061%20percent%20of%20all,the%20industry%20from%20criminals%2C%20hackers%20and%20stat, 2021.

[8] “Tackling the cyber security skills shortage,” AustCyber, no. https://www.austcyber.com/resources/sector-competitiveness-plan-2019/executive-summary, 2017.

[9] Fortinet, “What is OT Security? An Operational Technology Security Primer,” 14 September 2023. [Online]. Available: https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security.

[10] ISA, “ISA/IEC 62443 Series of Standards - ISA,” 14 September 2023. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[11] ISA, “Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program,” 2009.

[12] Ai Group, “Working Securely With Defence,” August 2023. [Online]. Available: https://www.aigroup.com.au/globalassets/working_securely_with_defence_guide-1.pdf.

[13] S. K, “Defence Security Principle Framework,” 2020. [Online]. Available: https://www.defence.gov.au/sites/default/files/2023-07/Defence-Security-Principles-Framework-Redacted-OFFICIAL-14JUL2023.pdf.

[14] ACSC, “Information Security Manual,” 22 June 2023. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism.

[15] A. G. Department of Education, “How can schools and businesses partner for STEM education?,” [Online]. Available: https://www.education.gov.au/australian-curriculum/national-stem-education-resources-toolkit/i-want-know-about-stem-education/how-can-schools-and-businesses-partner-stem-education.

[16] N. D. o. Education, “P-TECH,” [Online]. Available: https://hunterriv-h.schools.nsw.gov.au/about-our-school/p-tech.html.

[17] “Apply for course accreditation,” [Online]. Available: https://www.asqa.gov.au/course-accreditation/apply.

[18] “Certificate II in Transport Security Protection (International Airport Screening Officer),” [Online]. Available: https://www.tafensw.edu.au/course-areas/aviation-and-aircraft-maintenance/courses/certificate-ii-in-transport-security-protection-international-airport-screening-officer--AVI20118-03#courseUnits.

[19] “Security awareness training,” [Online]. Available: https://www.cisc.gov.au/compliance-and-reporting/air-cargo-and-aviation/security-awareness-training#:~:text=A%20free%20online%20training%20module,and%20Known%20Consignor%20Security%20Programs.

[20] “Aviation Cybersecurity Oversight,” [Online]. Available: https://caainternational.com/course/icao-aviation-cybersecurity-oversight/.

[21] “Aviation Cyber Security,” [Online]. Available: https://www.iata.org/en/programs/security/cyber-security/.

[22] “Foundations of Aviation Cybersecurity Leadership and Technical Management,” [Online]. Available: https://igat.icao.int/ated/TrainingCatalogue/Course/5131.

[23] “Aviation Cyber Security,” [Online]. Available: https://jaato.com/courses/1012/aviation-cyber-security/.

[24] A. S. Q. Authority, “Users’ guide to the Standards for VET Accredited Courses,” [Online]. Available: https://www.asqa.gov.au/sites/default/files/2023-07/Users_guide_to_the_standards_for_VET_accredited_courses.pdf.

[25] “Jobs and Skills Councils,” [Online]. Available: https://www.dewr.gov.au/skills-reform/jobs-and-skills-councils.

[26] “Innovative ‘Living Laboratory’ sees students solve real problems at Newcastle Airport,” [Online]. Available: https://www.newcastle.edu.au/newsroom/featured/innovative-living-laboratory-sees-students-solve-real-problems-at-newcastle-airport.

[27] “Securing our economic prosperity by strengthening cyber security,” [Online]. Available: https://minister.homeaffairs.gov.au/KarenAndrews/Pages/securing-our-economic-prosperity-by-strengthening-cyber-security-13-07-2021.aspx.

[28] “Budget 2023: The Industry Responds to Labor's Cyber Security Plans,” [Online]. Available: https://www.cybersecurityconnect.com.au/industry/9033-budget-2023-the-industry-responds-to-labor-s-cyber-security-plans.

[29] "Critical Cyber Crime Statistics in Australia 2023" - https://eftsure.com/en-au/statistics/cyber-crime-statistics/#

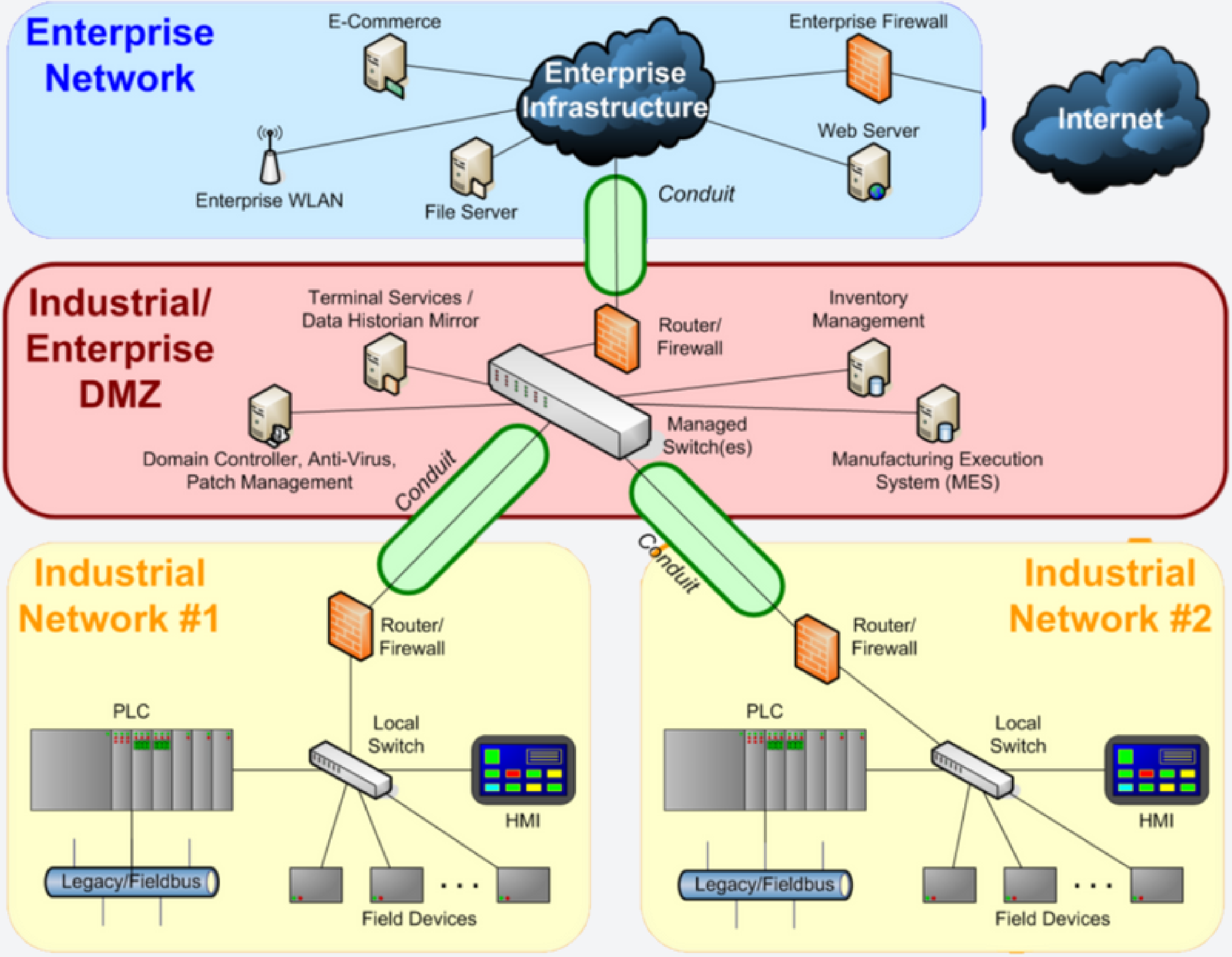
[30] "Cybercrime costs" - https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[31] “5 Critical Controls for World-Class OT Cybersecurity | Dragos” - https://www.dragos.com/resource/5-critical-controls-for-world-class-ot-cybersecurity-infographic/

[32] "14 business impacts of a cyber incident" - https://www.prnewswire.com/news-releases/deloitte-identifies-14-business-impacts-of-a-cyberattack-300284852.html

[33] " A Frost & Sullivan study commissioned by Microsoft - Cost of Cybercrimes to Australia Economy" - https://news.microsoft.com/en-au/features/direct-costs-associated-with-cybersecurity-incidents-costs-australian-businesses-29-billion-per-annum/#:~:text=Sydney%2C%20Australia%2C%2026%20June%202018,1.9%25)%20of%20Australia's%20GDP.

# APPENDIX



**High-level manufacturing example of a defensible architecture [11]**

# THE COST OF CYBERCRIME TO AUSTRALIA

## DIRECT COST TO BUSINESS

**33% = 693,053 businesses** experienced a cybercrime

**11,703** reported a cyber incident → **153** reports of critical infrastructure

energy utilities finance

**60% OF ALL TARGETED ATTACKS STRUCK SMALL AND MEDIUM BUSINESSES**

**$276,323**
Average cost of a cyber crime attack to a business

**53% of the cost** is on detection and recovery

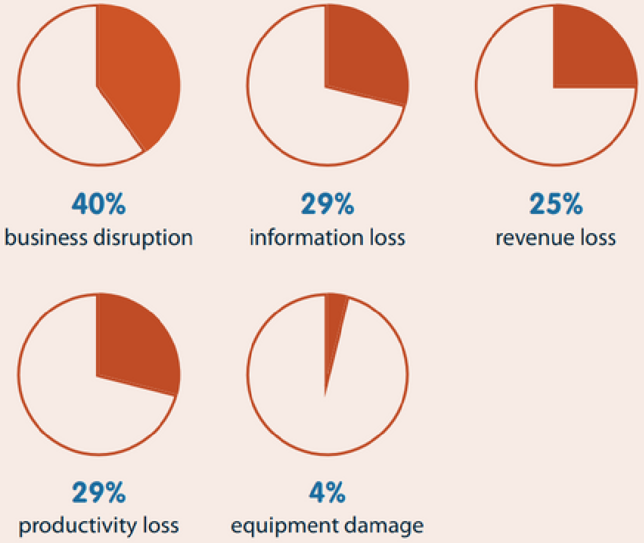
### Average cost per attack

| | |
|---|---|
| Denial of service | $180,458 |
| Web-based attacks | $79,380 |
| Malicious insider | $177,834 |
| Malicious code | $105,223 |
| Phishing and social engineering | $23,209 |
| Malware | $458 |
| Stolen devices | $13,044 |
| Virus, worm or trojan | $421 |
| Botnet | $867 |

**50%** of the costs are caused by web-based attacks and insiders

## INDIRECT COST TO BUSINESS

### Effect of a cyber attack on business



Average time to resolve an attack is **23 days**

**Increase to 51 days** if the attack was a malicious insider, employee or contractor.

Australian Government Initiative
Stay Smart Online

STAY SMART ONLINE

FOR MORE TIPS VISIT
STAYSMARTONLINE.GOV.AU

Data sources: PWC – Global Economic Crime Survey 2014; ABS – Count of Australian Businesses 2014; ABS – Business use of Information Technology – 2014; Ponemon Institute – Cyber Security Report 2014; Symantec – Internet Security Threat Report 2014