ACDA response to
Cyber Secure Queensland Strategic Plan 2023

Feb 2023

Active Cyber Defence Alliance

Overview

We are seeking your input

Q1. Do you think the cyber threat environment is getting worse or better? What areas are you most concerned about?

The Australian Cyber Security Centre (ACSC) received approximately 76 thousand cybercrime reports in the financial year 2022. The number of reports has increased in comparison to previous years, with approximately 67 thousand cybercrime reports filed in financial year.

Things are getting worse. The current passive approach to cyber security has created an environment where the consequences of crime and the risk of retribution are minimal, while the crime itself is highly profitable, thus the prevalence of cybercrime is escalating. The practice of some foreign governments of sheltering cyber criminals who undertake state espionage objectives while pursuing their criminal activities give them a further layer of immunity and consequence boldness. As we see increasing attacks on critical infrastructure and industrial control systems, we must assume that some criminal information theft and extortion attacks are also masking infections of sleeper malware laid as a contingency in preparation for future conflict between nation states.

Q2. Are there any significant gaps or other activities we should be acknowledging? Are there activities that you were not previously aware of that need to be communicated more?

Rather than comment on specific Queensland programmes we will address the wider gap in approach that flows from the universal focus on passive cyber defence. The Cyber Secure Queensland Strategic Plan provides an opportunity to address this by expanding the range of Queensland's cyber defence activities to change the balance of power in the cyber realm in favour of the defender thus reversing the current asymmetric advantage of the attacker which is creating so much loss and risk for legitimate organisations.

Cyber security should be understood from the perspective of risk. We need to understand the threat actor, threat vector, asset and vulnerability to properly understand the cyber risk. The passive cyber security approach of protecting the assets and removing the vulnerabilities should be coupled with the intelligence gathering about the threat actor and threat vector of active defence to fully understand the cyber risks, and then define the controls required to mitigate the risk.

Q3. Have you had any experience with any of these activities and resources? What were the positives? What could have been done better?

In dealing with Qld government cyber stakeholders the ACDA has encountered a lively interest in exploring active cyber defence approaches and in testing and

evaluating these in proof-of-concept exercises to understand how they would work and where value is delivered. Unfortunately, lack of available human resources has prevented realisation of a concrete program of works. We see the current consultation as a valuable opportunity to prioritise resources to this important activity.

Theme 1 – Securing Queensland

Q4. What do you think about this theme?

We would add to the Opportunities: The forward leaning mindset of Qld Gov cyber leadership and the timing of this consultation present. An opportunity for Qld to provide leadership in the evolution of active cyber defence to compliment passive cyber defences, or, to use the language of the MITRE Corporation, the movement to enhance a controls-based defence with a defence based on adversary engagement

Q5. What should the strategic objectives be, and how could we measure success?

Qld strategic objective should be to make its digital environments hostile to malicious activity and its intelligence structured such that it sees adversaries coming and has detailed awareness of their activities through the reconnaissance, active compromise and aftermath phases of any incident. Towards this objective, Qld needs adopt what ACDA calls “Active Cyber Defence” and MITRE Corporation calls “Adversary Engagement”.

ACDA defines Active Cyber Defence as the employment of cyber intelligence, deception, active threat hunting and lawful countermeasures to expose, elicit and affect malicious actors more effectively than is possible with "Passive Cyber Defence" which relies on conventional cyber security practices such as network hygiene, firewalls, virus filters, identity & access controls and good user behaviour etc. By itself, "Passive Cyber Defence" has proven to be ineffective against sophisticated attacks. "Active Cyber Defence" excludes "Offensive Cyber" actions which are the sole domain of authorised government agencies, although it could include mechanisms to coordinate potential responses by such agencies.

MITRE defines adversary engagement as the “combination of denial and deception to increase the cost and decrease the value of your adversary’s cyber operations. Adversary engagement goals can be any combination of the following: to detect adversaries on the network, to elicit intelligence to learn about adversaries, or to affect an adversary by raising the cost, while lowering the value of their cyber operations.”

As stated in the theme’s associated challenges “The exponential increases in data volume and variety, with high expectations regarding protection, privacy and appropriate access and use of data, make security more difficult to achieve.” This trend is likely to continue and demands a change in approach to make our rapidly evolving information ecosystems sustainably defensible. Our present cyber posture positions us like a blind and deaf boxer in a boxing ring. The adversary can pick off the boxer and ultimately defeat them. They might learn the occasional lucky punch

while defending but are destined for failure as they never have the initiative and will usually react to attacks too slowly to mount an effective defence.
Simply attempting to improve cyber hygiene and protective systems is not working well and cannot be expected to be effective. Our posture needs to change with the objective of taking and holding the initiative in the cyber conflict rather that to only react after our adversary has made their move.
Success can be measured by:

1. Efficacy –
    a. What is the ratio of false to true positives? Effective detection systems produce a modest number of positive alerts with few false positives.
    b.
2. Timeliness –
    a. Do we have foreknowledge of attacks?
    b. Do we detect attacks during early reconnaissance or later after a foothold has been established?
    c. What is the average days to detection of major breaches?
    d. What is the average time from detection to effective mitigation?
3. Initiative –
    a. During what proportion of incidents do we hold the initiative or are we continually reacting to our adversary's initiatives?

Q6. What activities should we undertake to achieve our objectives?

1. Invest in acquiring competencies in Qld agencies for active cyber defence eg.; training on implementation of MITRE Frameworks: ATT&CK, ENGAGE & Caldera
2. Participate in and contribute to the ACDA working groups:

    - **ACDA Frameworks Working Group**

    Current cybersecurity control frameworks (such as the NIST Cybersecurity Framework) do not accommodate easily the capabilities identified in MITRE ATT&CK, Engage and Caldera. Further, built into the philosophy of these frameworks, is the concept of a static and passive defence.
    The proposed working group seeks to:
    Prepare a submission to MITRE to augment the MITRE Engage framework and potentially propose an integrated framework encompassing MITRE ATT&CK, Engage and Caldera.
    Identify what changes are required in a framework such as the NIST CSF to enable a tactical shift from passive to active defence. It would also seek to embed threat intelligence and tactics based on the MITRE frameworks into the controls design and capabilities of the organisation.
    Augment the MITRE Engage framework and potentially create an integrated framework encompassing MITRE ATT&CK, Engage and Caldera.

Qld government participation in this working group will contribute to redefining security standards to explicitly incorporate active defence/adversary engagement techniques. Government involvement will bring invaluable perspectives to this process and signal to industry and the community at large the value of these acceptable and necessary techniques and approaches.

- **ACDA Lawful Countermeasures Working Group**

The ACDA has established a working group to clarify the legal guidelines on what counter measures are lawful for civilian organisations to undertake in defending themselves from cyber-attack. Recent events are forcing Australia to take a more active cyber defensive posture but just how far can we lawfully go? "For thousands of years laws in many jurisdictions around the world have recognised that actions that normally result in damage and harm will not lead to legal liability where those actions result from:

(i) - Self-Defence

(ii) - Intervening conduct or event

(iii) - Sudden or extraordinary emergency

(iv) - Duress

This right has been excluded from the cyber realm and it should not be excluded."
The ACDA working group will select common cyber defence scenarios and seek to answer the question: What freedom do we have to act and what are the consequences when we don't act?
The working group will:

(v) Identify a set of typical scenarios that occur in cyber incidents from theft of personal private information, intellectual property and from threats to human safety and operational reliability

(vi) Map out guidelines for lawful countermeasures in Cyber Defence for each scenario by answering the questions.

1. What actions are available?
2. Risks if we act
3. Risks if we don’t act

(vii) Consider the context of Australian State and Federal law but potentially also selected international jurisdictions.

Qld government participation in this ACDA working group will contribute to defining the lawful countermeasures in the context of Qld law and empower government and private sector critical infrastructure operators to mount a more proactive, effective and robust cyber defence.

Government involvement will bring invaluable perspectives to this process and signal to industry and the community at large the value of these acceptable and necessary techniques and approaches.

Key benefits to Qld – This work will provide an extra tool to help lift Australia's and Queensland's cyber resiliency. It will make Australian organisations less attractive targets, while reducing the burden on Government, Law Enforcement, and the ACSC to undertake remediation activities.

Q7. What role should government, industry and academia play in this theme? Are there other players?

Q8. What additional activities could we put in place to enhance security of critical infrastructure in Queensland?

Proactive detection - Industrial control systems breaches (Critical Infrastructure)

- Adopt cyber deception/Adversary engagement techniques across government critical infrastructure operations to create synthetic/deceptive assets that will enable early detection of adversary reconnaissance and early evidence of compromise before a serious breach occurs.
- Develop whole of state adversary engagement/deception rolling campaigns to detect adversary reconnaissance and early malicious activities against the Qld's critical infrastructure and on to deceive, study, disrupt, misinform and misdirect attackers

Protection of Olympic Venues

- Upgrading and standardising legacy systems across the 84% of Olympic venues which are existing or temporary to may prove unfeasible. In the case, Qld Government should develop an integrated cyber deception/adversary engagement campaign across the Olympic venues. This will enable early detection of adversary reconnaissance and early evidence of compromise before a serious breach occurs and provide the tools, deceive, study, disrupt, misinform and misdirect attackers.

Threat Intelligence Sharing

- Support community-based Threat Intelligence Sharing initiatives like CI-ISAC https://www.ci-isac.com.au

Q9. What additional activities could be put in place to enhance the security of personal information by government and business?

Proactive detection/Quality assurance Confidential information

Rather than assume confidential information stores remain confidential Qld government should take a proactive approach that assumes data is leaking. This can be done by implementing data loss intelligence using active and passive tracers embedded in synthetic and authentic files to trace and track actual data loss across the government agencies. This approach will enable government to continuously

track and quantify data leakage and highlight leakage hotspots making possible an evidence-based approach to risk mitigation priorities. Contrast this with the current assumption that nothing us leaking until a government data trove in the dark web is exposed by the press.

Theme 2 – Combating cyber threats

Q10. What do you think about this theme?

Q11. What should the strategic objectives be, and how could we measure success?

The Draft strategic objectives T2.1-3 are worthwhile, and hold promise if well executed.

Measures of success:

- Substantively reduce the average number of days to detect a major breach in Queensland
- Measures of early detection
- Measures of false positives versus true positives

Q12. What activities should we undertake to achieve our objectives?

T2.1 Proactively generate and distribute threat intelligence and increase forensic capability.

We refer to our answer to questions 6 & 9 above. Adoption of these recommendations will materially enhance proactive generation of cyber threat intelligence and forensic capability.

T2.2 Enhancing the ability to respond and recover from cyber incidents

Proof of concept cyber exercises to validate the value of active cyber defence

Over the past several years, several Queensland government agencies (Cytec, QGCIO, Electoral Commission & Qld Rail) have attempted to launch proof of concept exercises in the use of cyber deception and active cyber defence-effects with the ACDA and industry partners. Unfortunately, due to lack of resources and funding, none of these exercises proceeded. This strategy process presents an opportunity to allocate resources to this important work. A properly crafted proof of concept exercise will give great confidence to Queensland government practitioners in the effectiveness of the active cyber defensive tools and techniques while fostering awareness and adoption by the community. It will also expand the options available in responding and recovering from cyber incidents.

T2.3 Strengthening the consequences and penalties for cybercriminals

Determining Adversary identity

Aside from discovering TTPs, Adversary engagement and cyber deception enables the defenders to move up the value chain from initial detection towards understanding adversary mission and identity. Once identity is reliably established the way is open for potential third party sanctions to be applied.

Reducing the value of data theft through misinformation

Salting data with fake records so that adversaries cannot distinguish real data from fake data and allowing adversaries to steal fake data sets are examples of active defensive techniques that increase costs for our attackers and reduce the benefit of

their operations when they are successful. Widely deployed, these techniques have potential to undermine the business case for criminal actors to steal data.

Lawful countermeasures

As detailed in our answer to question 7 above, countermeasures that normally result in damage and harm will not lead to legal liability where those actions result from:

(a) - Self-Defence

(b) - Intervening conduct or event

(c) - Sudden or extraordinary emergency

(d) - Duress

This right also applies in the cyber realm, and it should not be excluded. An ACDA working group is studying the boundaries of what actions are lawful for to(?) civil organisation when under attack. Taking down adversary command and control infrastructure may be permissible in appropriate circumstances. Choosing not to act may be criminal in some circumstances. For example, Microsoft has led the way in using existing law to undertake botnet takedowns and materially damage the capacity of criminal groups to undertake cybercrime. Adoption of the findings of the ACDA Lawful Countermeasures working group…..(?)

Benefits to Qld. Participation by Qld Government in this working group would clarify the boundaries of what countermeasures can be undertaken lawfully under Qld law standing to materially increase the costs and risks to malicious actors when they attack Qld organisations.

Q13. What role should government, industry and academia play in this theme? Are there other players?

Government has a role to play in funding and resourcing initiatives to develop active cyber defence capability and to foster awareness and adoption. As we develop this discipline, there will be significant contributions required from the legal profession, academia, cyber practitioners and development of new competencies in the areas of intelligence and counterintelligence and adversary engagement. Other key players who can contribute to this:

The Active Cyber Defence Alliance Inc (ACDA) is a special interest group whose aim is to foster awareness, adoption and capability in Active Cyber Defence practices across Australia with the goal of lifting Australia's cyber resilience. Our intention is to draw together professionals from both supply and demand side along with academic, legal and regulatory stakeholders who will jointly act to support active cyber defence initiatives and to influence policy and practices for the benefit of our community rather than the explicit interests of their organisation.

What we mean by "Active Cyber Defence"

Active Cyber Defence employs cyber intelligence, deception, active threat hunting and lawful countermeasures to expose, elicit and affect malicious actors

more effectively than is possible with "Passive Cyber Defence" which relies on conventional cyber security practices such as network hygiene, firewalls, virus filters, identity & access controls and good user behaviour etc. By itself, "Passive Cyber Defence" has proven to be ineffective against sophisticated attacks.
"Active Cyber Defence" excludes "Offensive Cyber" actions which are the sole domain of authorised government agencies, although it could include mechanisms to coordinate potential responses by such agencies.

Q14. Do you feel you have the skills to detect and avoid malicious cyber-attacks?

Yes. Effective adversary engagement and cyber deception practices produce a very low number of false positives and provide enriched contextual information about imminent and ongoing attacks. This greatly reduces the on forensic analysts as they are no longer searching for a needle in a haystack of needles when searching for indications of compromise.

There is also the potential to design campaigns to elicit further intelligence from the adversary so that while they think they are compromising your valuable assets they are in fact providing your defenders with detailed intelligence of their tools, techniques and procedures (TTPs).

Q15. How can we encourage cybercrime reporting?

Q16. What are your expectations when you report a cybercrime?

Q17. What more could be done to find cybercriminals and hold them to account?

Determining Adversary identity

Aside from discovering TTPs, Adversary engagement and cyber deception enables the defenders to move up the value chain from initial detection towards understanding adversary mission, advanced tools, techniques, procedures and potentially identity. Once identity is established the way is opened for third party sanctions.

Lawful countermeasures

Microsoft has led the way in using existing law to undertake botnet takedowns and materially damage the capacity of criminal groups to undertake cybercrime. It is the ACDA view that existing law has not been sufficiently applied in the cyber realm and that it may be lawful undertake a wider range of countermeasures certain circumstances. The ACDA Lawful Countermeasures working group is exploring and clarifying what countermeasures are lawful, under what circumstances so that defenders have a clear decision process to understand the consequences of acting or not acting during an incident.

Theme 3 – Growing cyber talent

Q18. What do you think about this theme?

Q19. What should the strategic objectives be, and how could we measure success?

Create an intelligence competency stream in Queensland's secondary and tertiary education programs. Enclosed is a link to a draft ACDA document outlining the skills and

competencies required to equip cyber intelligence and adversary engagement operatives.
Analysts training outline.docx

Q20. What activities should we undertake to achieve our objectives?
Study Israel's secondary and tertiary programmes to identify and nurture vocations in intelligence, counterintelligence and cyber defence more generally
Explore programs like the MITRE Engage desktop game. This kit is a helpful tool to enable teaching and collaboration on cyber denial, deception, and adversary engagement. You will definitely want one of these kits if you work in this cyber mission area.
https://www.linkedin.com/feed/update/urn:li:activity:7022620192186736640?updateEntityUrn=urn%3Ali%3Afs_feedUpdate%3A%28V2%2Curn%3Ali%3Aactivity%3A7022620192186736640%29

Q21. What role should government, industry and academia play in this theme? Are there other players?
Q22. How can we make cyber security an attractive career path?
Q23. What do you see as the priority areas where we have current and future skills gaps?

Theme 4 – Innovating and industry growth

Q24. What do you think about this theme?
Q25. What should the strategic objectives be, and how could we measure success?
Q26. What activities should we undertake to achieve our objectives?
Q27. What role should government, industry and academia play in this theme? Are there other players?
Q28. Are there existing security research/innovation programs which could be leveraged, and stronger partnerships created?

Ref Draft strategic objective 4.2

The ACDA believes that the working group initiatives detailed in our answer to Q6 above embody, in themselves, significant innovations and provide a platform for Qld to leadership in both innovation and research in the rapidly emerging field of active cyber defence.

Q29. What Queensland industry sectors would you like to see prioritised for cyber security innovation and research?
Q30. What features would you like to see in a Queensland Government cyber security marketplace?

Theme 5 – Promoting cyber excellence

Q31. What do you think about this theme?
Q32. What should the strategic objectives be, and how could we measure success?
Q33. What activities should we undertake to achieve our objectives?

Q34. What role should government, industry and academia play in this theme? Are there other players?
Q35. For organisations, what cyber security maturity models have you adopted and what challenges did you face?
Q36. What should the priority areas be for collaboration between government and industry for cyber maturity uplift?
Draft object T5.3 suggests the development of a Queensland Government Cyber Defence Centre to facilitate proactive defences and effective response to improve Queensland Government resilience and preparedness. Both sides of the cyber defence coin should be considered in this objective. The passive cyber defence approach, or the "just in case" defence and the active cyber defence or the "just in time" defence.
The intelligence that could be generated by engaging with an adversary who is acting against one Queensland government department or agency could be made immediately available to other departments and agencies so that they can adjust or uplift their passive defences. With the shortage of skilled talent, running a public/private joint venture Cyber Defence Centre, the Queensland Government can get the best cyber intelligence analysts and experts from private enterprise working with public sector analysts to uplift their capability as part of the joint venture.
Q37. For cyber security service providers, have there been any barriers to offering cyber security services to government or other businesses? If yes, what are those barriers?
Theme 6 – Raising cyber resilience
Q38. What do you think about this theme?
Q39. What should the strategic objectives be, and how could we measure success?
Q40. What activities should we undertake to achieve our objectives?
Q41. What role should government, industry and academia play in this theme? Are there other players?
Q42. What gaps and opportunities do you see in awareness and education of cyber security?
Q43. What would help improve the basic skills of your colleagues and customers so they can operate in a digitally secure way?
Q44. How do we help differentiate and inform purchasing decisions for products and services to allow security risks to be taken into account?
Theme reflection
Q45.Do you think there are any major areas missing?
Q46. Do you think we should re-shape or consolidate any of the themes? If so, what would that look like?
Our vision
Q47. Which option for our vision do you like the most?
Q48. Do you have an alternative vision statement to put forward?