AustCyber
Australian Cyber Security Growth Network

SUBMISSION

TECHNOLOGY INVESTMENT ROADMAP FOR A FRAMEWORK TO ACCELERATE LOW EMISSIONS TECHNOLOGIES

DEPARTMENT OF INDUSTRY, SCIENCE, ENERGY AND RESOURCES

JUNE 2020

Cyber security: the enabler for success

Strong cyber security embedded in digital infrastructure and business practices are part of a low carbon energy technology roadmap

Cyber security as an industry offers a new source of economic growth to Australia. It is also an enabler of growth through digital transformation in every sector of the economy – including the energy sector.

The energy sector's development and uptake of low emissions technologies, combined with broader digitization and digitalization through Industry 4.0 models, are driving greater efficiency and global competitiveness. It is also increasing the sectors' dependency on technology being trusted and resilient to malicious cyber activity and other digital forms of interruption.

These trends illustrate that digital technologies, connectivity and automation are having a profound impact on the way organisations operate. These trends are not discrete and exert an influence on an evolving cyber security threat landscape, with diverse and unanticipated cyber security risks now affecting businesses, governments and people.

The increased complexity of the cyber threat landscape is globally recognised. This is in part due to the responsiveness and resourcefulness of malicious actors taking advantage of unsecured rapid digitalization, as well as legacy in ICT infrastructure and human behaviours, human and technological capability gaps. This, combined with improving but comparatively still low awareness in broader society, outdated and siloed legislation and regulation, rapidly evolving geopolitical and cultural dynamics and human bandwidth overload.

In our cyber-physical world, developing an efficient low emissions ecosystem, including with new technologies discussed in the *Technology Investment Roadmap Discussion Paper*, requires all components of energy production, distribution and consumption technologies to be connected, integrated and, where appropriate, automated.

Regardless of the nature and form of new and existing technologies that drive lower emissions, they are being integrated in increasingly online environments across energy networks. So too are the data sets and business intelligence to, for example:

- manage and control the various low emissions and other technologies to make sure they are providing energy when and where it is needed;
- integrate customer demand with energy supply and create opportunities for customers to use the low carbon energy and reduce demand for energy when supplies are low;
- ensure the energy is stored when it not being used, and available for later use; and
- measure and monitor energy generation, supply and network performance.

Digital capability is the key underpinning infrastructure that brings all the sources of energy and customers together. They ensure new low emissions and existing legacy technologies work together and perform effectively and drive not only more efficient networks, but make sure the low carbon technologies are available when they are needed.

Without this digital infrastructure, it is much more challenging to orchestrate energy networks to manage customer demand effectively and deliver energy efficiently, and ensure the promise of low emissions technologies are delivered.

Cyber security risks – and opportunity

Cyber security risk manifests throughout the energy system as well as in the value chains supporting these complex processes, including pricing mechanisms and regulatory controls. The risks are not limited to larger organisations or processes, though the more complex and interconnected these are, the higher the consequences of a security breach or compromise.

Malicious cyber activity is a growing challenge for organisations worldwide. It can be in the form of online fraud through to sophisticated cyber espionage and calculated cybercrime. Malicious cyber activities have the potential to seriously harm not just an organisation's business and reputation, but also to compromise a nation's security, stability and prosperity.

With the number of malicious incidents spiking in recent years, as perpetrators aggressively exploit flaws in digital infrastructure, cyber security is increasingly becoming front of mind for business leaders and regulators who are anxious to shore-up defences and improve resilience.

The risks are real and pervasive as shown by the example of an attack on a power plant in India late last year, where its digital networks were comprised using malicious software (malware) designed for data extraction.

> *…"Critical national infrastructure is a lucrative target for cyber hackers," said Stuart Reed, VP Cyber at Nominet. "Not only can an attack disrupt services that have a nation-wide impact but data is often highly sensitive and valuable."*
>
> *"The attack on India's nuclear power plant is particularly worrying given it should have had the newest and most secure network," said Reed. "It is fundamental that those responsible for the provision of critical infrastructure are taking the necessary steps to defend themselves from attackers."*
>
> *"They need a layered approach to cybersecurity, all the way down to a network level," he added. "By tapping into the ubiquitous DNS layer for network detection and response, for example, security teams can use their existing infrastructure to identify malicious traffic entering and leaving their network early, allowing them to quickly take steps to mitigate the impact of an attack before damage is done."*[i]

Cyber adversaries are constantly devising new ways to exploit vulnerable systems and networks. This is forcing organisations – including energy network operators, generators and customer focused smart energy devices to strengthen their cyber defences.

Smart and sophisticated uptake of cyber capabilities in the energy sector to better manage cyber risk represents a significant opportunity to underwrite the success of the sector's future. Assuring trust in energy systems and developing cyber resilience improves competitiveness and contributes to improved productivity.

How to embed cyber security into low emissions technologies

With many energy networks becoming increasingly digital and incorporating a larger number of external parties into the network ecosystem, there are key principles that can underpin the way these ecosystems are developed and operated to assure cyber resilience. These include as follows, taken from AustCyber and Data61's Cyber Security Industry Roadmap, reflecting areas of focus for the energy sector's uplift in cyber security (among other priority sectors).

1. **Secure by design** – ensuring new products (including novel technologies), services, platforms, processes, facilities and devices are designed with cyber security as a key consideration through:
    - assurance of secure products using guidelines to establish a baseline for built-in cyber security in products and services that harmonises with local and international standards, allowing for improved exportability[ii]
    - ensuring secure by design skills in workplaces are strong, so companies involved in the development and commercialisation of new technologies embed strong cyber security early in the design process
    - security is embedded in ICT training with the gap between cyber security and ICT education bridged by embedding more cyber security aspects into all tertiary information technology courses. Research and industry collaboration between Australia's cyber security sector and the research community to help Australian industry underpin innovation with strong cyber security[iii]
    - ensuring secure trade and supply chains through contractual negotiations and agreements that clearly integrate cyber security measures in the development phase, leading to much greater security across energy supply chains.
2. **Robust and resilient** – building greater cyber maturity and resilience in the Australian energy sector and communities by developing a robust security culture.
    - Awareness in the energy sector and community about the importance of cyber security is strong, supported by a targeted, high-profile education campaign.
    - Workforce cyber awareness skills are strong throughout all levels of staff, with companies adopting appropriate risk-based cyber security practices.
    - Frameworks for cyber security with improved governance enables more innovation, while ensuring cyber resilience is prioritised.
    - Strong leadership at Executive and Board levels through cyber security literacy and education initiatives that are supported right at the top and well attended, leading to improved cyber security awareness within company leadership structures.
    - Australia's energy sector continues to build global reputation through collaboration with the cyber security sector, leveraging strengths of the research community.
3. Building **secure, robust and resilient networks** for legacy and low emissions energy, includes developing a trusted digital ecosystem which allows the rapid exchange of information and providing a stronger environment for network integration of all the key network players:

- Trusted partners that engage in trusted sharing of information within value and supply chains, with third parties and with customers.
- Threat intelligence sharing within industry efficiently, allowing credible threats and risks to be quickly understood, mitigated and dealt with.
- Collaborative cyber security demonstration projects to illustrate how a trusted secure ecosystem may be established to create and preserve commercial value within Australia's nationally important energy sector.
- Resources and best practice guidelines with tailored cyber security assessment resources, customised to Australia's energy sector and adaptable to the unique circumstances of businesses.
- Onshore cyber security capability nurtured and encouraged by judicious procurement of locally developed cyber security solutions that helps to maintain a critical mass of onshore cyber capabilities.

Delivering these principles and actions requires strong cross-sector collaborative action. Many of the immediate actions described here are already in process in cyber literate sectors such as finance and defence, however, we are seeing a need for greater focus for them to be implemented across the broader Australian industry, including in the energy sector.

With the energy sector undergoing profound transformation, which will accelerate in coming years as the shift to lower emmissions technologies gathers pace, AustCyber welcomes further discussion about actions that can be undertaken to ensure energy networks are secure, robust and resilient as our economy and lives are dependent on them.

About AustCyber

As the Australian Cyber Security Growth Network Limited, AustCyber is a publicly funded, private entity which commenced on 1 January 2017. Our mission is to grow Australia's cyber security sector, to support the development of a vibrant and globally competitive Australian cyber security sector. In doing so, our activities will enhance Australia's future economic growth in a digitally enabled global economy and improve the sovereign cyber capabilities available to protect our nation's economy and community.

We form a part of:

- the Australian Government's Industry Growth Centres Initiative, established through the 2015 National Innovation and Science Agenda. Like our sister Industry Growth Centres NERA and METS Ignited, we are one of six centres that have been set up in sectors of competitive strength and strategic priority to boost innovation and science in Australia; and
- Australia's current Cyber Security Strategy, released in 2016. It was through the industry consultation and development of this strategy that the concept for AustCyber was first conceived.

Our funding comes from majority Federal Government grants – funding for operations and programs, and for the $15 million AustCyber Projects Fund which provides grants to projects that deliver national benefit. We also receive funding under contracts with the governments of the ACT, NSW, QLD, SA, TAS, WA and the Sunshine Coast Regional Council and Townsville City Council, which we match, to deliver AustCyber's national network of Cyber Security Innovation Nodes – with the NT and VIC soon to join.

We work to align and scale Australian cyber security research and innovation related activities across the private sector, research communities, academia and within Australian governments. We are responsible for maintaining a strong supply of innovative Australian cyber security solutions and capability and have established ourselves as an independent advocate for the competitive and comparative advantages of Australian technical and non-technical cyber security capabilities.

Beyond our shores, we work with partners across many countries to develop export pathways for Australian solutions and capability. This helps the rapidly growing Australian cyber security sector tap into market 'hot spots' around the world.

---

[i] https://www.silicon.co.uk/security/cyberwar/indian-nuclear-power-station-hack-301447

[ii] Note that AustCyber in partnership with Standards Australia and the NSW Government is currently developing a comprehensive national framework for cyber security standards and guidance to streamline the existing fragmented landscape of technical standards and business practices. This work includes the energy sector, with industry representation across traditional and renewable energy sources.

[iii] AustCyber in partnership with the national TAFE network have developed nationally consistent Certificate and Advanced Diploma qualifications in cyber security. Further, many of Australia's universities now deliver cyber security courses and microcredentials mapped to the internationally recognised Cybersecurity Workforce Development Framework produced by the US National Initiative for Cybersecurity Education, with Australian input led by AustCyber. Refer to AustCyber's website for more information.