SECURING CRITICAL INFRASTRUCTURE
CREATING A STRONG AND RESILIENT CRITICAL INFRASTRUCTURE COMMUNITY
Creating a Secure and Resilient Critical Infrastructure Community

In our increasingly unstable global security environment, great power competition is enacted in digital realms rather than conventional battlefields.

It’s an ambiguous space where businesses and industry are the front line, the Field Marshalls are Captains of Industry, and the first sign of an attack is a sudden and inexplicable failure of an element of critical infrastructure rather than troop movements across a border. As critical infrastructure moves to digital or online options for operations, it increasingly becomes a more accessible target for foreign interference. Critical infrastructure boards and executives must take rapid and effective steps to enhance risk practices to address this threat. However, initial Accenture research has indicated that many companies are unfamiliar with the threat environment, are understaffed to meet the challenge and underprepared to respond.

The strength of Australian national security is contingent on the secure operating practices of critical infrastructure owners and operators. Companies are now ‘fair game’ for aggressive moves in global great power competition and must enhance their risk practices to address this threat. To ensure the creation of a secure and resilient critical infrastructure community implementation and enforcement of legislation as well as close engagement and information sharing will be necessary. To prepare critical infrastructure to become an effective front line, Government and utilities must together create an environment of compliance and a readiness for co-ordinated response.

Implementing a new regulatory environment to support a community committed to risk managed, compliant infrastructure will require specialist security and risk management skills, rare experience in countering foreign interference operations and reliable delivery of technological support and insights.
The Challenge and the Opportunity for Australia

The World Economic Forum’s Network Readiness Index ranks Australia as 18th in the world for digital maturity. This positive finding also exposes Australian vulnerability to cyber-attack. Figures from 2017 show that Australia’s digital environment is trending up—becoming more networked and integrated and increasing opportunities for cyber attackers. Australia is 2nd in the world for providing digitally enabled Government and public-sector services. This network maturity has enabled businesses and Government to drive efficiency and create a closely integrated digital citizenry—it has also expanded Australia’s surface area for attack.

The Australian economy, and particularly the utilities sector, has capitalised on technology to squeeze performance and profit in a challenging political, regulatory and operational environment characterised by new competitors and a swathe of market disruptors. Additional regulatory and commercial pressures will further squeeze margins for utilities and continue to drive this trend as customers and Government require greater granularity on performance and usage and continue to expect the highest standards of supply. This trend has seen an increased use of digital interfaces for companies seeking to exploit efficiencies through digitisation and especially Internet of Things connections.

Internet of Things means that we have more connections and interfaces with the internet than ever before. Australia, as a digital nation is more accessible and, as a wealthy nation, more attractive to cyber attackers and hostile state actors seeking to achieve significant impact or exploitations without incurring the cost of open conflict.

Overall critical infrastructure system related cyberattacks have been trending upwards globally with a year-over-year increase of 4.6%. In the short term, direct costs associated with cybersecurity incidents could cost Australian businesses up to $29 billion per annum. This is both a drain on the economy and a challenge to businesses absorbing overhead caused by new regulations, increasing competition and high consumer expectations for service. Additional political and community pressures on pricing mean that risk management needs to be considered at all points on the chain, not just as an after-thought that layers on cost. Significant as this is, the cost of a successful attack on the Australian national interest could cost human lives, jeopardise national security, cost billions and damage Australian reputation globally affecting trade and the economy. Longer term and more insidious exploits will act to degrade Australia by reducing competitiveness in trade, increasing vulnerability to compromise and corruption and by undermining Australian sovereignty.

The average cost of a single malware attack on a company is $2.4 million. From 2016 to 2017 there was a 22.7 percentage increase in cybersecurity costs. Ransomware damage costs exceeded $5 billion in 2017, 15 times the cost in 2015.
Navigating the Threat Environment

One of the great challenges of the 21st century will be responding to attempts by foreign powers to disrupt critical technology systems. Accenture commissioned a threat intelligence report using real time data on attacks operating across the globe on critical infrastructure. The report indicates that attacks experienced by utilities in foreign nations are similar or the same to those in Australia. Pattern analysis indicates trends that can inform Australian Government policy and prepare utilities to better address their vulnerabilities and achieve resilience.

Insights from the report are as follows;

Industrial Control System related Critical Infrastructure Attacks are Increasing in Scale and Complexity

Australia has seen an increase in attacks on industrial control systems used by critical infrastructures—iDefense findings are broadly consistent with other findings that the number of attacked systems growing from ~24% in 2017 to ~30% in 2018. The Australian Cyber Security Centre reports responding to 734 cyber incidents affecting private sector systems of national interest and critical infrastructure providers to date. This indicates that Australia has not yet achieved sufficient capabilities to prevent or deter attackers.

Australia is a Significant Target

Currently, Australia has one of the world’s longest single electricity grids—spanning over 5,000 kilometres from Port Douglas to Tasmania and delivering power to much of the nation. The opportunity to conduct a high impact attack is significant. Australia is also one of the world’s largest energy exporters, as such (and especially for nation state actors interested in energy trade) the incentive to conduct an attack is great. As many advanced persistent threats invade a system and remain dormant until an opportune moment occurs the degree of risk is not known.

Critical Infrastructure is a Serious Vulnerability

The rise in attacks, combined with impact assessments from global case studies indicate that there is a very high chance that a targeted attack against a major Australian critical infrastructure operator will inevitably have a significant impact and could occur at any time. Both the opportunity and the incentive for such an attack are significant. The ability of operators of Australian critical infrastructure to prevent, detect or respond to such an attack is low.

Figure 1: Accenture’s threat intelligence capability iDefense IntelGraph shows that Australian Critical Infrastructure is experiencing an increasing number of attacks from a range of actors.

Trending Malware Families (In IG)
Challenges to Securing Critical Infrastructure

With the threat of an imminent major attack on the radar, many experts are highlighting the difficulties in securing critical infrastructure from threats and achieving preparedness for a co-ordinated response. The difficulties of securing critical infrastructure from attacks are centralised on three key themes—the barriers of detection, lack of security measures and the inherent vulnerability in infrastructure networks.

1. Difficulty of Detection
Most threats to the critical infrastructure are in the form of advanced, persistent threats which linger and accumulate for years without exposure. Since most critical infrastructure attacks are done by nation-state threat actors with resources and funds—most of the malware and attack vectors seen are highly sophisticated. In that, most malicious actors will endeavour to disguise the intrusion as a part of usual customer traffic, making it difficult to expose or uncover. This means that the extent of the potential damage is not known.

2. Lack of Security Measures
Most attacks on critical infrastructure are possible due to weak protection mechanisms on the systems or through phishing emails. Most critical infrastructure operators are running out-of-date systems and due to the scale of these networks, it’s difficult to transition these legacy systems into something less vulnerable. Without the appropriate security controls and patches, these infrastructures lack resilience and will be unable to ward off today’s advanced threats.

3. Infrastructure Weakness of Current Infrastructure
Australia—like many other nations have built critical infrastructure in centralised ways. This creates a central point of failure where one intrusion point can have a ripple effect throughout. It’s time to rethink the current infrastructure integrations and dependencies.

Case Studies

Energy companies and other utilities have historically been primary targets for cyber attackers and Australia has the unfortunate title of being one of the world’s first nations to experience a cyber-attack on critical infrastructure.

Maroochy Shire, Queensland, Australia 2000
In April 2000 the Sunshine Coast urban centre inexplicably drowned in raw sewage as millions of litres of effluent began spilling out into local parks, rivers and car parks. The system had been hacked remotely by a disgruntled employee operating out of his car. The employee had helped install the sewage system and when he was rejected for a job with the Maroochy Shire Council he decided to get revenge. It took the experts a while to figure out that an exploit was occurring because they hadn’t seen it before. In fact, Maroochy Shire was witnessing one of the first critical infrastructure attacks in the world.

Russia, December 2017
In December 2017, a Russian malware called “Triton” was discovered targeting Industrial control systems in December 2017. This malware was designed to target the Triconex Safety Instrumented System, an industrial control system used to monitor the performance and critical systems inside of oil and gas industrial environments. The malware infected a Saudi Arabian petrochemical plant and caused the control systems to unexpectedly shut down.
Envisioning the Cyber Resilient Utility of the Future

Cyber resilience in the critical infrastructure community can only be achieved through authentic engagement between Government and the industry sector.

The creation of a trusted community with a commitment to security and risk management will be essential. As in infectious disease management, the Australian community will only be as strong as its weakest member—thus inoculating the whole community against a threat increases the resilience of the entirety of Australia, even beyond the critical infrastructure community. Accenture has identified three key themes for the creation of a strong and cyber resilient critical infrastructure community.

**Information Security for Trusted Networks**

Utilities that are competitors will have reservations about sharing details of their security experience and preparations. The Australian Government will need to establish a high standard of security to manage, store and transfer data sent from and to companies and maintain confidentiality. As this system will store and manage sensitive company data and would also be a target, whatever system the Australian Government chooses should be Information Security Manual compliant and include verification measures for receipt and transmission of materials.

**Platform for Community Consultation and Engagement**

Utilities and Government should work together to achieve a standard and co-ordinated operating procedure for responding to reports of critical incidents in the community which could include specific preventative measures, preparation of contingency operating capabilities and co-ordinated policy and media responses. Regularised review and reporting will ensure that standards reflect the risk environment and effectively draw on the experience of the whole community to ensure the best response—especially if the community can benefit from international engagement through Government.

**Standardised Risk Frameworks and Approaches**

Utilities and Government can achieve a rigorous and robust community approach to cyber security and resilience if risk frameworks are standardised at a high level. This will enhance security measures across the community from members with immature or absent risk management approaches to those with developed and mature practices.
This assures the critical infrastructure community and stakeholders that a standard of ‘best practice’ risk management has been achieved—this will also help to defray costs to individual companies. Guidance and remediation governance frameworks will act as a guide for companies in an ongoing way to ensure that their standards are current and create a pool of capability.

Accenture has the expertise and experience required to support the collaboration of Australian Department of Home Affairs and Australian critical infrastructure assets to create a strong and cyber resilient community. Accenture brings:

a. specialised and highly cleared security staff with subject matter expertise on critical infrastructure, Industrial Control Systems, foreign interference and cyber security,

b. state of the art technology implementation and real time threat intelligence on cybersecurity,

c. agile delivery methods and change transformation designed to rapidly review and update legacy systems, achieve consensus and deliver innovative technology solutions.

d. A connected community of consultants across the Utilities, Infrastructure and Government sector industry and significant experience in risk profiling for corporate governance.

References


About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialised skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 459,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.