

**Energy Policy**  
INSTITUTE OF AUSTRALIA



Public Policy Paper  
Paper 4/2016

## CYBER SECURITY POLICY IN THE ENERGY SECTOR

Gary Waters and Luigi Sorbello  
Jacobs Australia

April 2016

---

*The Energy Policy Institute of Australia is an independent and apolitical energy policy body.*

*The Institute advocates that Australia must maintain a secure investment climate and be internationally competitive, whilst moving towards and contributing as much as it can to global efforts to build a low-carbon society.*

*The Institute was originally established in 1999 to support the Australian government in the activities of the Asia-Pacific Economic Cooperation (APEC) Energy Working Group.*

*The Institute's public policy papers are published in the public interest. They are authored either by Institute board members or by invited experts and do not necessarily reflect the views of the Institute or any of its members. They may be cited or republished in whole or part with appropriate attribution but copyright remains with the Institute.*

**For further information please visit the Institute's website  
[www.energypolicyinstitute.com.au](http://www.energypolicyinstitute.com.au)**



## ***Key Points***

- National economies and infrastructures are heavily dependent on the energy sector, which itself is increasingly dependent on Information Technology (IT) systems.
- Ensuring security of supply is an urgent priority in the face of the increasing need for diversity of renewable and clean energy supply, evolving standards, and the escalating sophistication of the cyber security challenges.
- The solution requires an effective energy and climate policy framework, strong industry leadership, and a pro-active bias for collaboration in the energy sector ecosystem to address security of supply and the cyber security challenges.
- A disciplined “Systems Engineering” approach, that considers all facets of the complex energy system, including policy, regulation, technology, supply chain, standards, processes, people, detection, protection and defence, remediation, and compliance, can provide the framework to more effectively manage the cyber security challenges and provide a more holistic, coordinated and increased cyber-readiness capability for the Australian energy sector.



## **Background**

In the past year, there have been increasing incidents of “disruptive” cyber attacks where attackers have destroyed critical business systems, leaked confidential data, held companies to ransom, and taunted executives. While all attacks are disruptive to some degree, a recent trend is not the hidden persistent access for data and exfiltration of intellectual property but attacks that deliberately draw public attention to the cause of the attackers via a crippling loss of critical systems and public release of confidential data. These disruptive attacks, often termed “asymmetric”, can cause a significant and disproportionate level of damage without the attackers needing significant resources.<sup>1</sup>

The energy sector is not immune to such attacks; indeed, along with financial and utility enterprises, energy companies have experienced substantially higher cyber crime costs than health care, automotive and agriculture organisations; with some of the most costly attacks emanating from malicious insiders. High-impact, high-visibility, disruptive attacks are increasingly sophisticated in approach and coordinated in execution.<sup>2</sup>

Governments exercise their international and national responsibilities through Critical Infrastructure Protection (CIP) programs to provide stability and confidence in Systems of National Interest. One of the key CIP priorities for national governments is the need to ensure continuity and security of energy supply and distribution against the debilitating effects of cyber attack. The energy ecosystem is mainly made up of an electrical production system, an electrical generation and distribution network and an oil and gas production and transportation system. This largely interconnected and complex ecosystem can be considered as a system-of-systems. Even with increased diversity of supply from generation sources, and geographic diversity of transmission, distribution and pipelines, attacks can nevertheless cause significant national disruption, loss of productivity, and other direct and indirect damage.

This paper outlines the scale and scope of the cyber challenge facing the energy sector, examines the inherent vulnerabilities in Industrial Control Systems (ICS), and calls attention to the need for a Systems Engineering approach to improve the cyber resilience of the sector.


## ***The Cyber Security Challenge***

The energy sector is heavily reliant on ICS which have been in use for more than 30 years, with the early SCADA (Supervisory Control and Data Acquisition) systems implemented before the exponential advances in computer chip technology and the internet era connectivity. They used proprietary protocols and software, and IT security consisted mainly of physical protection of the host computers.

---

<sup>1</sup> See Mandiant Consulting, ‘*M-Trends 2016*’, Special Report, February 2016.

<sup>2</sup> See HP Enterprise, ‘2015 Cost of Cyber Crime Study: Global’, October 2015.



ICS is a general term that encompasses several types of control systems, including: SCADA systems; Distributed Control Systems (DCS); and Programmable Logic Controllers (PLC). Common weaknesses identified in ICS include: credentials management; network design weakness; lack of formal documentation; weak firewall rules; audit and accountability (event monitoring); and permissions, privileges, and access controls.<sup>3</sup>

Within the last 10 years, there has been a rapid increase in the connections to SCADA systems. Today, with the Internet of Things (IoT), we are seeing an acceleration in the use of ICS technologies for connectivity, sensors, process automation, monitoring and control. In concert, there has been a movement away from proprietary protocols and software to using the same standards and solutions as enterprise and administrative IT systems.

The energy sector's cyber security challenge is twofold. The first is that there is still a large embedded base of legacy ICS elements in the sector. The second is that ICS and SCADA systems are now being exposed to threats and vulnerabilities they were never exposed to before, or not to such an extent.

There has been an expansion of the attack surface - with attack vectors now including internet facing devices, portals, third party vendors and contractors with direct connections to the ICS, open layer 2 ports, weak virtual private network (VPN) configurations, personal computers, phishing emails with embedded trojans, flash drives, vulnerable operating systems, back-up servers, and communication links.

As just one example of the energy sector's vulnerability, on 23 December 2015, parts of western Ukraine were plunged into darkness after a computer virus affected the networks of several regional electricity companies. The Ukrainian power grid was penetrated and large segments were taken offline in a very well-crafted attack that focused on bringing the system down but also focused on how the provider was likely to respond to the outage. It was this example that moved the US National Security Agency director, Admiral Michael Rogers, to argue that cyber security and energy sector specialists need to work with the government to keep the country and its people safe. He suggested that the future needed to be about partnerships and integration.<sup>4</sup>

### ***ICS Vulnerabilities***


Attacks on ICS are increasing, and more resources are needed to monitor, detect and analyse anomalous activity in control system networks. Because control system protocols are typically not authenticated, do not require security-grade integrity checking and are left wide open to OSI layer 2 attacks, they are highly vulnerable.<sup>5</sup>

---

<sup>3</sup> See Victoria Yan Pillitteri, Computer Security Division, US NIST; Presentation to Federal Computer Security Program Managers' Forum, 5 June 2013.

<sup>4</sup> RSA Conference 2016, San Francisco 1 March 2016, Keynote Speech. Reported in Mary-Louise Hoffman, 'Adm. Michael Rogers: Govt-Industry Partnership Needed to Ensure Citizen Privacy, Safety', Executive Gov, 2 March 2016.

<sup>5</sup> See 'The State of Security in Control Systems Today', SANS Institute InfoSec Reading Room, June 2015.



Specifically, the energy sector needs to address the vulnerabilities in the Applications and IT systems including servers, workstations, and commercial operating systems such as Windows, UNIX and Linux, employed for energy management, business process and administrative purposes. Even though exploit kits targeting ICS controllers have been proliferating, penetration testing reveals that one of the fastest routes onto the ICS network is via these commercial operating systems.

In addition, the energy sector must also apply the same IT discipline to the Operational Technology (OT) used in its industrial networks, such as SCADA systems, power line relays, sensors, specific software and other control technologies that are embedded in and that monitor, control and operate power plants, transmission and distribution grids, and pipelines.


Controllers in the ICS are a key threat vector, especially the communication protocols, and energy companies have recognised the risk that a significant percentage of industrial controllers do not use authentication to effect system changes that control switch gear, machine parameters, and so on. Many have now moved to introduce encryption and more tightly-controlled processes such as identity management, authentication, and role-based credentialing to improve authorised access, protection and resilience. It is essential to do a rigorous analysis of the security controls built into IoT devices and services they wish to use. At a minimum, an audit of an IoT device's communications channel, use of encryption, an analysis of the type of data it collects, stores and transmits, and the security of the end-point(s) with which it communicates, is paramount.

Administrators can now create application layer and identity-based policies to alert and block unauthorised change. Business rules can be created on specific process control commands, asset types, user role, time of day, and location. Network appliances are being brought to market that can undertake asset inventory of all devices on the network, and using deep packet inspection undertake analysis of the open application layer protocols, and vendor proprietary configuration layer communications.

In the movement of operational control devices from electromechanical to IP enabled, the same engineering design rigour used in commercial grade IP data networks such as Ethernet and cyber security design principles, must be applied to the various ICS elements such as firewalls, gateways, switchers and routers. Physical security and access to firewalls, communication rooms, and unsupervised ports on Layer 2 access and distribution switches are also points of infiltration, and for the connection of unauthorised devices, and need to be assessed in the system-of-systems approach.

With well-trained, knowledgeable personnel using the requisite toolsets, organisations are able to detect security breaches that do not disrupt normal operations. The ability of Advanced Persistent Threats (APTs) to remain undetected depends on their operating below network threshold levels or system noise. It is vital, therefore, that the energy sector continues to invest in people, processes and technology to increase its cyber readiness.

Energy companies' cyber readiness must include pre-deployed contingency plans and relief mechanisms that will help to restore the companies' systems. These response and recovery procedures will not only help companies contain and minimise a cyber-exploit as quickly as possible, but they can also serve as a record, and through information-sharing mechanisms, can



provide a basis for other companies in the sector to learn how to better protect themselves. Thus, there is a corresponding need for business continuity plans and enterprise-wide security assessments to consider security vulnerabilities across the whole energy supply chain. These include power plants, distribution systems, refineries and storage terminals, and the networking of transmission lines, pipelines and cyber systems.

The engineering design rigour must extend to cyber hygiene practice such as penetration testing and vulnerability scans and patching of devices in the ICS/SCADA networks. If legacy devices in production environments cannot be scanned because of their proprietary protocols, “security by obscurity” can provide a misleading sense of cyber risk assurance and response readiness.

### ***A Systems Engineering Approach***

In the last decade, the energy sector has seen the continuation of a sustained transition from a centralised generation, transmission and distribution system to a more decentralised system-of-systems, characterised by market deregulation, privatisations, multiple enterprises, increased renewables/low emission generation sources, and large uptake of residential rooftop solar. This transition is accelerating, driven by new technologies such as commercial and residential battery storage, government incentive schemes, and the increased need for renewables and low-emission supply sources to meet the November 2015 COP 21 climate change commitments on greenhouse gas (GHG) reductions.


Decentralisation brings increased resilience benefits from diversity, but it also brings a significantly expanded cyber attack surface and heightened risk of infiltration for malicious exploit and disruption. Given the interconnectedness of a decentralised system, it is difficult for any enterprise to establish a cyber boundary and enforce protective and detective measures without a comprehensive asset inventory of the devices and systems that support, or are connected to, the ICS and enterprise networks.

A relevant cyber security Risk Assessment Framework, allows enterprises regardless of size, and degree of cyber risk and sophistication, to utilise best practice cyber risk management and prioritisation principles. However, whichever cyber risk assessment framework is used, it is invariably incapable of being used alone. The framework is a tool to provide a holistic risk assessment, assist understanding, provide guidance, and facilitate prioritisation in the implementation of cyber resilience programs.<sup>6</sup>

The tool cannot provide answers to the questions of what are the end-to-end requirements of the system and whether the correct design has been incorporated. There is still the need to apply a sound and proven engineering methodology that includes an enterprise’s objectives, end-to-

---

<sup>6</sup> It is worth noting here that the US National Institute of Standards and Technology (NIST) released the voluntary *Framework for Improving Critical Infrastructure Cybersecurity* in February 2014 to provide a common language organisations can use to assess and manage cyber security risk. The US Department of Energy then released its energy sector cyber security framework in January 2015, designed to assist energy sector organisations to: characterise their cyber security posture; identify gaps or excesses in their existing cyber security risk management programs; recognise the utility of existing sector tools, standards, and guidelines; and effectively demonstrate and communicate their risk management approach to both internal and external stakeholders. See Department of Energy, ‘Energy Sector Cybersecurity Framework Implementation Guidance’, January 2015.



end needs, operational requirements, business processes and people. The cyber security challenge is a problem that spans all enterprise boundaries and needs to be considered by all functional areas.

A Systems Engineering approach is uniquely suited to building resilience to the cyber security challenge that faces large-scale and complex systems such as those found in the energy sector. It begins with identifying an enterprise's top-level needs without pre-supposing solutions or remediation designs, and brings together the expertise of all stakeholders in the problem space.

Key process steps include: understanding goals and needs, discovering end-to-end system requirements, developing a concept of operations, ensuring a supporting enterprise security architecture, undertaking preliminary system design and iterative design reviews, producing interface specification and design, defining operational performance measures, defining cyber test strategy, undertaking system test and verification test, and frequency and type of vulnerability assessments.

Importantly, it establishes an effective baseline, and one that is maintained by strong configuration and change management discipline. Strong governance - a part of this approach - provides the clarity and accountability for effective execution and reporting to executive management, boards and government and industry fora. Using a capability maturity model such as the Electricity Subsector - Cybersecurity Capability Maturity Model (ES-C2M2) from the US Department of Energy, provides an assessment methodology to maintain or lift maturity in specified domains to target measures, and to collaboratively report these assessments to industry fora.<sup>7</sup>

A Systems Engineering approach is essential - piecemeal won't work - as the attack surface is too expansive, the perimeter ambiguous and ill defined, and people and processes are operating across multiple entity boundaries. Focusing on three key steps is suggested:

- First, adopt a Systems Engineering approach to the complex system of cyber resilience.
  - This holistic approach will ensure that attention is focused on the whole system, providing strategic guidance to stakeholders and strong governance.
  - Incorporating a cyber risk assessment framework will assist in quantification and prioritisation of initiatives, investment and resources.
- Second, undertake workforce information security education and training, develop cyber standard operating procedures, enforce cyber security best practices, and undertake security audits.
  - This strengthens the enterprise's cyber resilience posture, and
  - When combined with step 1, places the enterprise on a leadership trajectory in the energy sector.
- Third, effectively cooperate with energy policy makers, regulators, and other energy sector stakeholders, and participate in cyber security and resilience initiatives in the sector.

---

<sup>7</sup> US Department of Energy, 'Electricity Subsector - Cybersecurity Capability Maturity Model', February 2014.

## ***Conclusion***

National economies and infrastructures are heavily dependent on the energy sector, which itself is increasingly dependent on IT systems. Ensuring security of supply is an urgent priority in the face of the increasing need for diversity of renewable and clean energy supply, evolving standards, and the escalating sophistication of cyber security challenges. This requires an effective energy and climate policy framework, strong industry leadership, and a pro-active bias for collaboration in the energy sector ecosystem.

A disciplined Systems Engineering approach, that considers all facets of the large and complex energy system, including policy, regulation, technology, supply chain, standards, processes, people, detection, protection and defence, remediation and compliance, can provide the framework to more effectively manage the cyber challenges facing the energy sector. This will provide a more holistic, coordinated and increased cyber readiness capability for the Australian energy sector.

---

## ***About the Authors***

**Dr Gary Waters** is an independent consultant who holds a PhD in Political Science and International Relations. He retired from the RAAF as Air Commodore with 33 years' service, working in the Department of Defence for four years and then in the private sector and academia for the last eleven years. Gary recently retired as Head of Strategy and a Principal Consultant for Jacobs Australia but still consults to Jacobs Australia and key Jacobs clients. He has written or co-written over a dozen books on national security, including cyber security, and has worked on complex systems management.

**Luigi Sorbello, BE, MEngSc, CPE** is currently Executive Director – Telecommunications with Jacobs Australia, specialising in cyber resilience. Before joining Jacobs Australia in February 2016, Luigi had a 35 year career with Telstra Corporation in a number of onshore executive roles responsible for Network and IT systems, Enterprise Architecture, delivery of its IP Network Transformation Program, NBN Transit network concept, and delivery of a number of ICT projects to the Department of Defence. Offshore assignments included COO of TelstraClear, Telstra's former NZ entity. Luigi is a Fellow of the Institution of Engineers Australia.