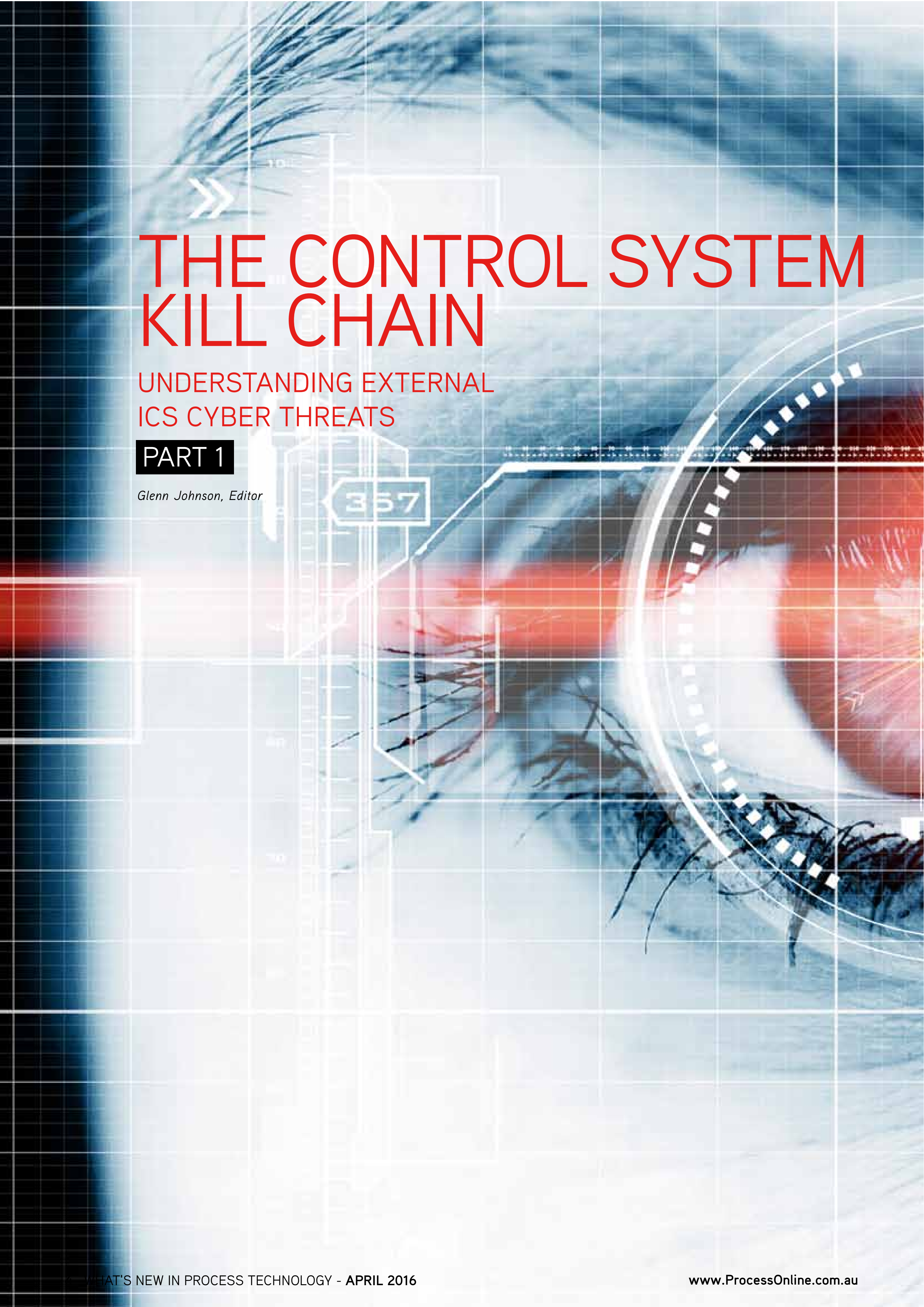
THE CONTROL SYSTEM KILL CHAIN

UNDERSTANDING EXTERNAL ICS CYBER THREATS

PART 1

Glenn Johnson, Editor



© Stock.Adobe.com/au/ Jürgen Fälchle

Understanding the approach a sophisticated external cyber attack adversary may take in infiltrating an industrial control system helps organisations defend against the unthinkable.

The advent of Industry 4.0 and equivalently named industrial technology initiatives has resulted in an increased drive towards implementing the already accepted idea of the interconnection of industrial control systems with business IT systems and the internet. Previous ideas that industrial control systems (ICS) were somewhat impervious to outsider threats (due to their custom and proprietary nature and isolation) are now a thing of the past, and organisations are having to come to an understanding of how to take advantage of the 'emerging fourth industrial revolution' while mitigating potential cyber threats.

This article is a review of some of the currently published literature on the subject of ICS cyber threats, and is intended to provide a general overview of the threat environment as it pertains to industrial organisations and their control systems.

According to the Australian Cyber Security Centre (ACSC), the "cyber threat to Australian organisations is undeniable, unrelenting and continues to grow. If an organisation is connected to the Internet, it is vulnerable". The 'Australian Cyber Security Centre Threat Report 2015'[1] also states:

"Cyber adversaries are aggressive and persistent in their efforts to compromise Australian networks and information. They are constantly improving their tradecraft in an attempt to defeat our network defences and exploit new technologies.

"Australia is an innovative country with a globally important resources sector. We are a regional leader with global interests and important partnerships. This makes Australia a target-rich environment for cyber adversaries.

"There are a range of cyber adversaries motivated to target Australian networks."

A 'cyber adversary' is defined as an individual or organisation (including an agency of a nation state) that conducts cyber espionage, cybercrime or cyber attack. Foreign state-sponsored actors may seek economic and other political or strategic security information for their national advantage, and they typically possess the most advanced and sophisticated tools and techniques, sometimes maintaining covert access to an organisation's systems for years at a time. They are often referred to as advanced persistent threats (APTs).

One of the largest continuous threats also comes from organised criminals, seeking financial gain through fraud and extortion, as well as issue-motivated groups and terrorist organisations.

Why you should be concerned about cyber espionage

If your organisation is a multinational corporation, but also even if it is not, you should not discount the possibility of cyber espionage. Because of Australia's resource-wealth and regional influence, as well as its broad range of commercial interests, expertise in many fields of scientific research, manufacturing and technology, and interconnected partnerships and alliances, it is an attractive target for this type of activity. According to the ACSC:

"The ACSC is aware that cyber espionage adversaries target industry networks in addition to government networks to acquire desired information. Cyber adversaries will target the weakest link; if the network security of their primary target is robust, they will move to secondary targeting of other networks that may hold the same information but are easier to compromise."

Cyber espionage obviously occurs with the intent to covertly collect valuable information and, as such, may not be initially a threat to an ICS, but rather the IT systems of your organisation — so, therefore, more of a threat to the financial viability and intellectual property of the organisation or other organisations and agencies the business may deal with. It therefore aims to not cause any noticeable harm, so as to go undetected. Such attacks can seriously hamper an organisation's reputation, profitability, competitiveness and business opportunities.

©WESTWICK-FARROW MEDIA REPRODUCED WITH PERMISSION

> ONE MITIGATING FACTOR FOR ICT SYSTEMS SPECIFICALLY IS THAT THEY ARE GENERALLY CUSTOM-ARCHITECTED FOR THE PARTICULAR PROCESSING, MANUFACTURING OR CONTROL FUNCTIONS THEY PERFORM.

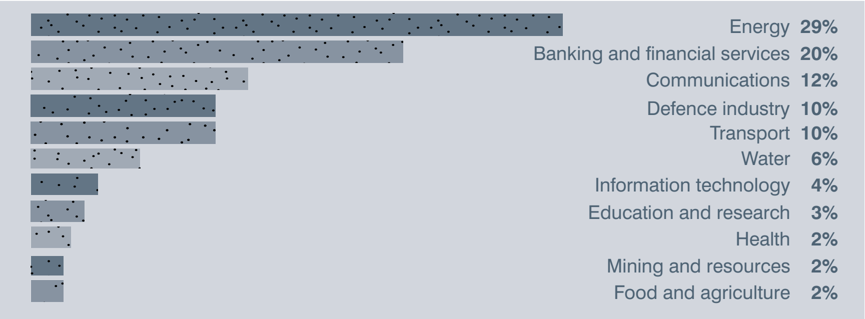


Figure 1: Incidents responded to by CERT Australia affecting systems of national interest and critical infrastructure in 2014. (Source: Australian Cyber Security Centre Threat Report 2015)

However, it is important to note (as we shall see later in this article) that the information gathered can also include information that will assist an overt cyber attack if desired at a later time — including attacks on an ICS. ACSC asserts that efforts by organisations to mitigate risk from cyber espionage will reduce the effectiveness and likelihood of ICS cyber attacks.

Critical infrastructure organisations

The ACSC defines ‘systems of national interest’ as those systems that if compromised could result in significant impacts on Australia as a society. Critical infrastructure forms a subset of these systems and is typically that providing utility services (such as electricity, gas, water and wastewater) and transportation systems.

In 2014, CERT Australia responded to 11,073 cybersecurity incidents, of which 153 involved systems of national interest and government. The top five non-government sectors affected were energy, banking and finance, communications, defence industry and transport.

Cyber attack

As a deliberate act of manipulating, degrading or destroying systems, cyber attacks are a serious concern. Overt destructive cyber attacks, particularly against systems of national interest, would be considered by the Australian Government to be an act of war.

The interconnection of ICS and IT systems makes these types of events more possible — although currently they are considered unlikely outside a period of increased tension or conflict with another country. Hacktivists and terrorists may still pose a threat in this area, but are generally considered to not have the advanced skills and technologies of a nation state. Obviously this threat may still be a risk if your organisation’s defences are weak enough.

One mitigating factor for ICT systems specifically is that they are generally custom-architected for the particular processing, manufacturing or control functions they perform — as opposed to business IT systems that incorporate commonly known technology and processes. This generally makes control systems initially more difficult to manipulate or damage without first gathering considerable specific architectural and process knowledge. This is why protection from covert cyber espionage is as important as direct protection of control systems — to limit or prevent the gathering of the information necessary to perform an ICS cyber attack.

Partnerships and supply chains

In an interconnected industrial world, organisations are increasingly connecting with each other to improve efficiencies. These connections may be many and varied, but commonly manufacturing organisations will have direct connections with organisations in their supply chain — to take advantage of the enhanced supply chain efficiencies that result — and may also allow suppliers such as automation vendors to connect to their automation systems for service and asset management services.

Due to the cost savings as compared with closed network links, the internet is the primary method of connection and may include the use of various technologies including VPN links and cloud services. But, as stated above, a network is only as secure as its weakest link.

Cloud services are a case in point. As a cost-effective method of data sharing between sites, or between business partners and equipment vendors, they can introduce greatly enhanced efficiencies and cost savings. They also offer improvements in some aspects of data security at a lower cost. However, they also introduce their own risks. The ACSC reports the case of a company that in June 2014 was put out of business when a cyber adversary used the company’s legitimate login credentials to delete company data from a cloud service.

Some points the ACSC recommends be considered in relation to cloud services are:

- where the data may reside (offshore versus onshore) and whether the data is subject to foreign government data access laws;
- storing data in multiple locations and allowing more people to access it opens more opportunity for compromise;
- multitenancy cloud computing increases the likelihood of compromise, and proof-of-concept exploits that circumvent virtualisation have been developed.

IT versus ICS cybersecurity

While some aspects of control systems today use similar or the same technology as IT systems (such as computers running Microsoft Windows operating systems), there are significant differences in relation to risk profile, as summarised in Table 1.

“Industrial Control Systems are not designed to ensure resilience against concerted attacks that intend to place components in

©WESTWICK-FARROW MEDIA REPRODUCED WITH PERMISSION

Attribute	IT	ICS
Confidentiality (privacy)	High	Low
Message integrity	Low-medium	Very high
System Availability	Low-medium	Very high
Authentication	Medium-high	High
Non-repudiation (Proof of the integrity and origin of data)	High	Low-medium
Time criticality	Days tolerated	Critical
System downtime	Tolerated	Not acceptable
Security Skills/Awareness	Usually good	Usually poor
System life cycle	3-5 years	15-25 years
Interoperability	Not critical	Critical
Computing resources	"Unlimited"	Very limited with older processors
Software changes	Frequent	Rare
Worst case impacts	Frequent loss of data	Equipment destruction, inquiries

Table 1: Comparing IT and ICS security risk factors (Source: ISA[2])

dangerous operating states. This is expected to be a growing area of cyber-attack and engineering research."

Cyber attacks on IT systems usually focus on general-purpose operating systems and application software, exploiting inherent vulnerabilities via buffer overflows, zero-day vulnerabilities and cross-site scripting, and generally aim to capture valuable information or deny service. ICS attacks can be built on these methods but instead take aim at physical processes, exploiting legitimate design features. Another way to put it is that while IT cyber threats are based on unknown, or unmitigated flaws, ICS threats use persistent design vulnerabilities (PDVs), inherent in the design of the system as part of its function. The ISA refers to these not as "zero-day vulnerabilities" but as "infinite day vulnerabilities".

Developing cybersecurity expertise

It is generally accepted that there is a significant knowledge and experience gap between the IT and OT sections of an industrial organisation. IT departments often have (or *should* have) more cybersecurity expertise, but the staff tend not to have engineering expertise. Operational staff, on the other hand, have engineering expertise but little or no security training and understanding. Bridging this gap is critical as IT and OT systems become more connected and, as a result of this divide, the role of ICS cybersecurity expert is emerging.

"In the IT environment, technology is available to monitor and identify cyber attacks, although there have been many cases where IT cyber compromised systems have gone unseen for months. With critical infrastructure, it is very different. When an event occurs in critical infrastructure such as an electric blackout or a pipe break, the results are immediate and the impact can't be hidden. Without the perspective of an Industrial Control Systems cybersecurity expert, it can be difficult to determine if a cyber breach is the cause of a failure incident."[2]

ICS cybersecurity experts should be employed or trained to provide a similar function to that of an IT security expert, with the same understanding of security threat, risk and mitigation — only with an understanding of the physical automation process, the unique features of the ICS domain and industrial standards and processes. Such staff are needed to help bridge the 'culture gaps' that exist between IT and OT that can exacerbate the threats to the ICS and make it difficult to secure them.

The intrusion kill chain

In defending any system against cyber attack, it is important to understand in a general sense the process an adversary may take to achieve their goal. The term 'kill chain' derives from military terminology. According to a paper presented at the 6th International Conference on Information Warfare and Security (Hutchins et al 2010)[3]:

"A kill chain is a systematic process to target and engage an adversary to create desired effects. US military targeting doctrine defines the steps of this process as find, fix, track, target, engage, assess (F2T2EA): find adversary targets suitable for engagement; fix their location; track and observe; target with suitable weapon or asset to create desired effects; engage adversary; assess effects..."

The reason it is called a chain is because it is an end-to-end process — a failure at any point in the chain interrupts the process. The authors proposed a six-step kill chain model specifically for explaining the methodology for cyber intrusions, defined as reconnaissance, weaponisation, delivery, exploitation, installation, command and control (C2), and actions on objectives.

In Part 2

The concept of a kill chain is important in understanding the approach of a sophisticated external cyber attack adversary. It also helps to understand the challenges faced by such an adversary should they want to perform malicious actions on an industrial control system — it is certainly no simple task. In Part 2 of this article, the concepts around the kill chain and how it pertains to an industrial control system cyber attack will be described in more detail.

References:

1. Australian Cyber Security Centre 2015, *Australian Cyber Security Centre Threat Report 2015*.
2. Weiss J 2016, *What Executives Need to Know About Industrial Control Systems Cybersecurity*, International Society of Automation.
3. Hutchins EM, Cloppert MJ & Amin RH 2010, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Proc 6th Int'l Conf Information Warfare and Security (ICIW 11), Academic Conferences and Publishing Ltd 2011, pp 113–125.

©WESTWICK-FARROW MEDIA REPRODUCED WITH PERMISSION