White Paper
Industrial cloud security

Introduction

The industrial automation industry has increased its demand for virtualisation. From virtualised HMI's, historian's, advance analytics' through to simulation & training environments. Virtualisation gives the benefits of reduced hardware & hardware foot print, easy data backup & recovery and simplified system portability, which leads to streamlined engineering, reduced man hours and lower capital expenditure.

The next evolution to local virtualisation is to host the system in the cloud. Taking advantage of

- Near limitless amounts of processing power and storage capacity
- Government regulated cyber security protection
- Pool of engineering resources to access, fault find and maintain systems nationwide

The 3 points combined allow mitigation of high up front capital expenditure for localised hardware & software and drastic reduction in site travel, saving hundreds of thousands of dollars.

Virtual challenges

The challenge with virtualisation and hosted environments isn't a technical one. The key concerns keeping hosted solutions from immediate adoption is exposure to cyber threats and the lack of internal industry expertise to manage and mitigate them.

According to the Australian Cyber Security Centre threat report 2017

"The ACSC continues to observe malicious adversaries and criminals using rudimentary techniques and known network vulnerabilities to compromise networks that lack baseline cyber security measures"

"This opportunistic targeting is simple and cheap, and will continue as long as computers, networks and devices fail to implement baseline security."

Industrial automation industries are continuously being left exposed to loss of production and business reputation, through a combination of inadequate cyber protection and lack of security awareness & internal expertise.

An example of this is the impact of the Petya virus that infected a multinational confectionary manufacturer in Tasmania, halting operations.

When exposed by the media, the company made the following public statement

"We are placing 500 workers on cleaning duty whilst efforts are made to restore production",

With 500 paid workers on standby, we can quite easily estimate operational losses in the hundreds of thousands of dollars per day of downtime.

The irony in all of this is the Petya virus targeted known Windows vulnerabilities that could have been quickly and easily guarded against, had there been a trusted technology partner to provide a clear mitigation strategy for ongoing protection.

Figure 1 - Cyber Security

Collision of two worlds

Proprietary control systems were composed of their own operating systems, communication protocols and dedicated visualisation & control networks, ensuring production systems remained isolated from the information (corporate) environment for decades. This insulation also meant control systems had the luxury of remaining in operation for extended lifecycles without the need for upgrading.

However, ever since the early 90's the demand to improve operational efficiencies across the entire enterprise; in realtime, has transformed industrial automation systems. These transformations are

1. Use of IT & public network infrastructure instead of dedicated networks
2. Use of Windows instead of dedicated UNIX/LINUX operating systems
3. Use of open TCP/IP communication protocols instead of dedicated communication
4. Use of hosted infrastructure (cloud) instead of on premise server infrastructure

With the above prominent changes, industrial automation systems have experienced significant benefits, such as

- Drastic reduction in technology costs
- Realtime exchange of information between production and information environments
- Quicker releases of control system enhancements & features.

However along with these benefits industrial automation systems have inherited the side effects that come with information system technologies, exposure to cyber security threats.

Time and technology waits for no one

The industrial automation industry is continuing to experience a significant knowledge gap in the migration away from proprietary serial communication towards open Ethernet (TCP/IP) based communication.

This accelerated transition has left engineers exposed in trying to acquire in-depth IT knowledge, to design manage and maintain wired and wireless Ethernet networks.

With the advent of Moore's law where time and technology waits for no one, the industry is now stepping into another era that TCP/IP technologies have inadvertently lead us into: internet and the cloud.

What this means is the current knowledge gap has been compounded by technological changes brought along with the internet and the cloud. Ultimately this will widen the knowledge gap, leaving organisations exposed in trying to make the necessary step change to compete in tomorrow's market.

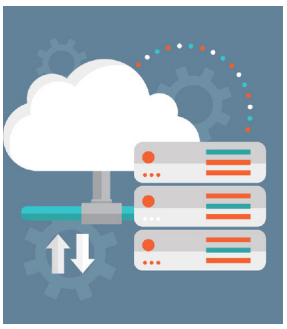

Figure 2 - Cloud computing cloud data storage

Secure data centres

Technological change requires controlled management to protect process reliability, quality, availability and security. These are all aspects that are subject to complex certification and validation, so new and more elaborate cybersecurity threats make protection an enduring challenge.

This level of complexity is alleviated through information provided by the Australian Signals Directorate outlining thought provoking guidelines on how security procedures are implemented, maintained and managed, ensuring data availability for business functionality and how to handle security incidents should it occur.

Cloud provider organisations are well aware and extremely vigilant that data centres are going to become the centre of attention for future hackers. Having this heightened sense of attentiveness, allows data centre providers to immediately gear up and allocate resources to ensure that more robust security procedures are mandated and actioned to remain as secure as they are today.

Figure 3 - CPU Server Unit Room

Evolution of SCADA

SCADA is a prime example of directional evolution in industrial automation, as it progressively moves towards a 'SCADA as a Service' model.

Figure 4 - SCADA as a Service

SCADA systems have been in existence for close to 60 years. From the early stages running on mainframe computers, communicating to remote devices through dedicated radios, to now being hosted in a data centre, communicating to remote devices through a secure public network (public network being a common I.T term for internet infrastructure).

This generation of SCADA system is a natural evolution to the traditional SCADA platform by taking a virtualised environment and hosting it in a data centre. Providing the ability to host and securely access the SCADA system anywhere and anytime using the internet.

With this comes greater cyber security responsibilities that will require a more holistic approach in identifying and protecting against current and future threats.

Your security partner

Traditional IT security techniques are not suitable for industrial automation environments OT, due to the misaligned emphasis of primary protection focuses. Where IT have a primary focus on data confidentiality, integrity then availability (C-I-A triad) vs the OT environment having a primary focus on data availability, integrity then confidentiality (A-I-C triad).

Plant availability is essential to keep social infrastructure like power, gas and petrochemical plants operational, even in the advent of a security breach. Once this is considered, separate IT/OT network & security domains become a business imperative.

Therefore, it is paramount to choose an established and field proven technology partner, that has both a national and international pool of security practitioners that can provide the right advice and support regardless of location and time zone.

Conclusion

Continued media headlines reporting cyber security threats disabling operations from a variety of process intensive and manufacturing industries, make it clear that cyber-attacks are on the rise.

As outlined by Prime Minister Malcom Turnbull in the national 'Australia's Cyber Security Strategy' document

"The scale and reach of malicious cyber activity affecting Australian public and private sector organisations and individuals is unprecedented. The rate of compromise is increasing and the methods used by malicious actors are rapidly evolving"

Knowing this, an owner or operator of critical processing facilities, would need to ensure that the right security measures are put in place, which can be continuously maintained and modified throughout the evolution of cyber threats.

An immediate alternative, would be to take advantage of a secure hosted infrastructure in combination with a trusted security technology partner to quickly bridge the gap in security. This alternative approach allows organisations to focus on new and cutting edge technologies by taking advantage of the transformative benefits of cloud computing without high upfront capital expenditure.

Ajay Trivedi
Functional Expert – Network & IT Systems
CISSP, GICSP, CISA, PMP, VCP6-DCV, MCP, Microsoft Specialist (Server Virtualisation), HiNE,
SPLUNK Certified User
Yokogawa Australia & New Zealand

Shalveen Sharma
Product Manager - IA Systems & Solutions
BEng (Electrical), DipElec, MENGNZ
Yokogawa Australia & New Zealand

Yokogawa Australia & New Zealand

YOKOGAWA AUSTRALIA PTY LTD
Australia Head Office - Sydney
Tower A, 112-118 Talavera Road, Macquarie Park NSW 2113

Melbourne
9 Lakeside Drive, Burwood East VIC 3151

Perth
Unit 1, 115 Belmont Avenue, Belmont WA 6104

Adelaide
96 Sir Donald Bradman Drive, Hilton SA 5033

Brisbane
18A Metroplex Avenue, Murarrie QLD 4172

YOKOGAWA NEW ZEALAND LTD
New Zealand Head Office - Auckland
Unit 1H, 5 Ceres Court, Albany Auckland 0632

Christchurch
11B Sheffield Crescent, Burnside Christchurch 8053

Contact us in Australia:

Email: enquiries@au.yokogawa.com
Website: www.yokogawa.com/au
Phone: 1300 558 965

Contact us in New Zealand:

Email: enquiries@nz.yokogawa.com
Website: www.yokogawa.com/nz
Phone: +0800 706050

Follow us: