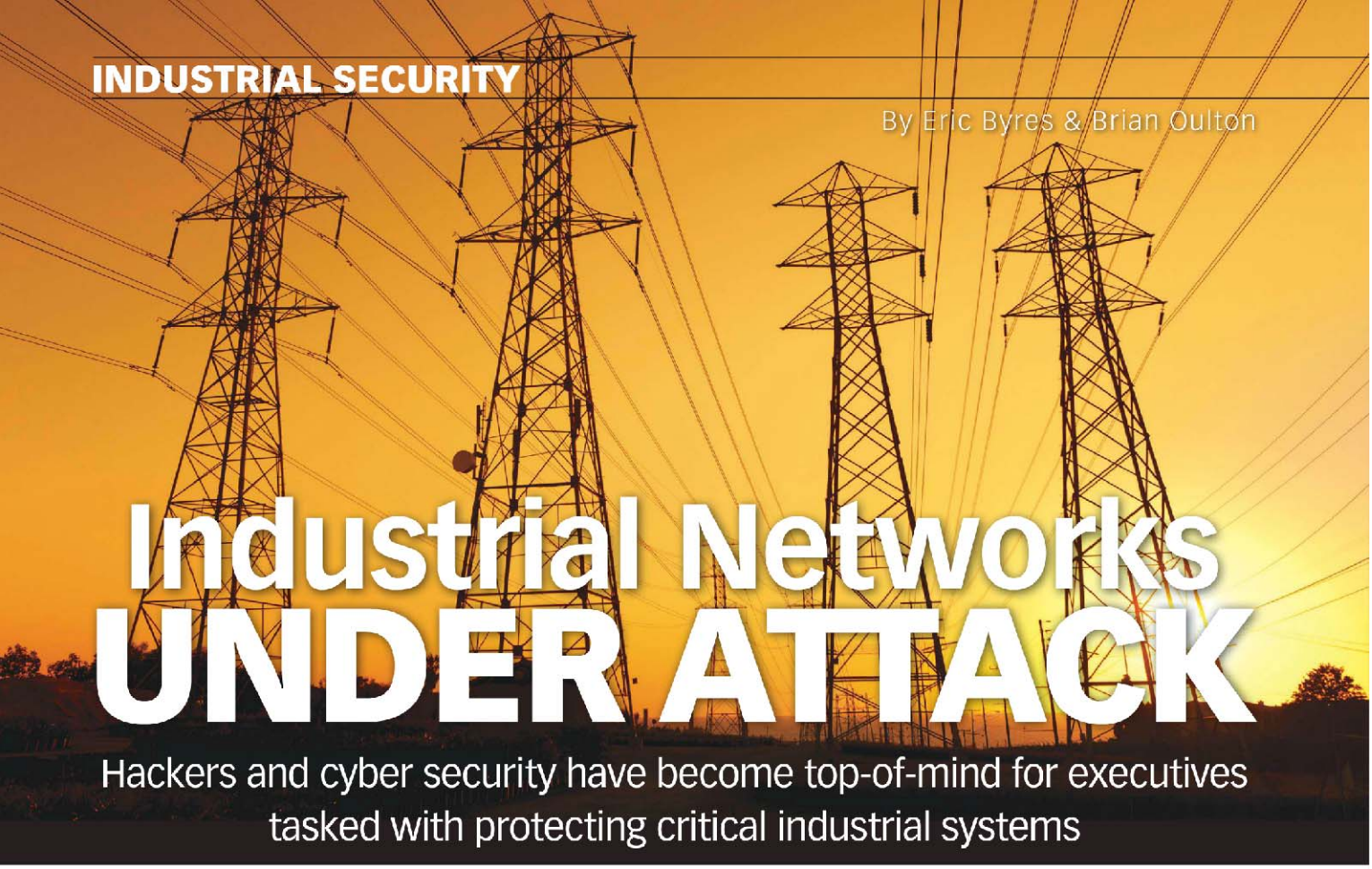
By Eric Byres & Brian Oulton



Industrial Networks UNDER ATTACK

Hackers and cyber security have become top-of-mind for executives tasked with protecting critical industrial systems

Since the discovery of the Stuxnet malware in 2010, industrial infrastructure has attracted some of the most sophisticated cyber attacks on record. Industrial networks and systems have become a key target for hackers.

Even if your business is not focused in key critical infrastructure industries such as energy, water and transportation, many enterprises have a SCADA (supervisory control and data acquisition) or process control network somewhere within its organizational structure. These networks are undergoing the kind of attacks that previously had only been experienced by financial and government institutions.

Those network attacks pose a huge vulnerability — one you may never know you had.

The Industrial Network Challenge

In the past, industrial networks ran on proprietary networks, used proprietary equipment and were isolated from business networks and the internet. This was the era of "security by obscurity" and "security by air gap."

Over the last decade, however, industrial networks have been migrating from proprietary systems to commercial off-the-shelf (COTS) technology. Although the adoption of Ethernet was initially slow, it has been rapidly increasing now that issues such as determinism (the ability to have predictable delivery of network packets) and rapid failure recovery (resolved by new redundancy protocols that offer low fail-over times) have been addressed.

In addition, increased demand for real-time industrial information meant connecting plant floors to enterprise networks and the internet. Keeping a modern industrial system running requires a constant stream of updates from the outside world — the result is that the industrial floor has become a hotbed of communications activity, and it is no longer isolated.

Furthermore, devices such as PLCs (programmable logic controllers) and DCS (distributed control systems) were designed with a focus on reliability and safety, rather than security — making many of them easy to exploit, particularly older units

Since industrial networks are often required to run at all times and withstand hazardous environments, many security policies are never deployed — operational necessities and safety regulations overrule them. Even traditional IT security strategies such as patching are often impossible, due to conflicting industry-specific regulations.

Add it up: vital networks with millions of hard-to-secure nodes, interconnected with enterprise networks and the internet; running 24 hours a day in heavily regulated environments with safety concerns; and the focus of the smartest security researchers and government warfare hacking programs in the world.

It's a lot to contend with.

A High Threat Level

In the past, the main reason for securing industrial networks was to protect against inadvertent network incidents or attacks from insiders. Legacy industrial

equipment such as older PLCs, DCSs and RTUs (remote terminal units) were not designed to elegantly handle malformed or heavy network traffic. In order to ensure reliable production, Industrial-specific firewalls were, and still are, used to permit only messaging required for operations.

The risk of an external cyberattack — especially one targeted at industry — was considered minimal, until the rise of terrorism in the new millennium and the disclosure of the game-changing Stuxnet malware in 2010, which specifically disrupted the centrifuges used for uranium enrichment at Iran's Natanz nuclear facility, thus proving that industrial sabotage by malware is possible.

Stuxnet was successfully introduced into an apparently air-gapped facility with the use of a USB key. Its discovery and the public release of its design had multiple impacts:

Stuxnet Legacy 1 – Security researcher focus on industrial systems: Stuxnet's fame drew security researchers' attention to hacking industrial systems. In 2011, more industrial control system vulnerabilities were made public — many with exploit codes available on the internet — than in the entire previous decade.

Stuxnet Legacy 2 – New advanced persistent threats target industry: Stuxnet's design provided a toolkit for other sophisticated malware known as advanced persistent threats (APTs); however, unlike Stuxnet that targeted an industrial process, recent APTs have been focusing on industrial espionage to steal business information. APTs are hard to detect, they can hide and collect data for years, and the losses resulting from them are financial- and reputation-related rather than safety or environmental incidents. Critical infrastructure such as financial services has been dealing with APTs for years, but they are new to the industrial space. An example is the Night Dragon attacks that stole business information from petro-chemical companies in North America, including energy contract information, oil field bids and production data.

Stuxnet Legacy 3 – Focusing cyber terrorism in the United States and the Middle East: According to a June 2012 article in *The New York Times*, Stuxnet was attributed to a joint U.S./Israeli intelligence operation called "Operation Olympic Games" started under President George W. Bush and expanded under President Barack Obama. As word spreads, attacks from nation states, criminals or other hackers will increase. Particularly for security executives with facilities in the United States or the Middle East, now is the time to renew your industrial cyber security efforts.

The Impact

A successful attack on an industrial network could mean production losses, significant safety or environmental issues or the theft of intellectual property, including information obtained from the enterprise network. Indeed, the industrial network could be the simplest backdoor to your enterprise network.

With reliable, continuous production a high priority, industrial networking devices with usable lives of 10 to 20 years and restrained spending, the solution is not the wholesale replacement of equipment.

Security Best Practices

A combination of best practices using technologies designed for industrial security, and a focused effort is effective in mitigating industrial system attacks.

It is important that your security staff is familiar with industrial security standards. No matter what industry you are in, the ISA IEC 62443 (formerly ISA-99) standard should apply. Major oil, gas and chemical companies such as Exxon, Dow and Dupont are using it and its strategies are often used successfully in the field.

Particular industries also have their own standards, such as NERC CIP for the North American power industry. The NERC not only develops reliability standards, it assesses adequacy, monitors the system and educates, trains and certifies industrial personnel. Unlike IEC 62443, which is a voluntary standard, NERC CIP has enforcement powers.

Here are seven steps to ICS and SCADA security, which condenses numerous industry standards and best practice documents. The result is an easy-to-follow process (Download a white paper detailing this process at http://web.tofinosecurity.com/download-7-steps/):

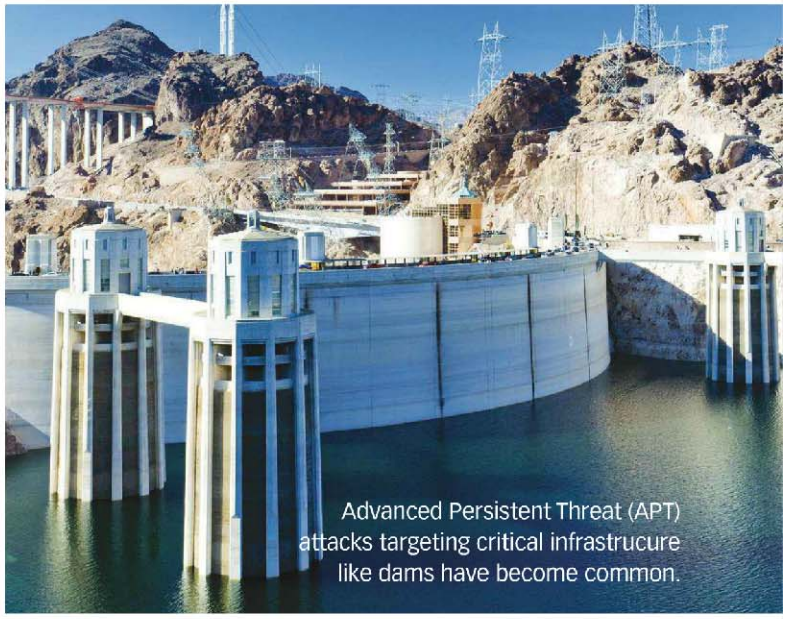
1. Assess existing systems: Understand risk and prioritize vulnerabilities.

2. Document policies and procedures: Determine your organization's position regarding ICS and develop company-specific policies.

3. Train personnel and contractors: Develop and institute policy awareness and training programs.

4. Segment the control system network: Create distinct network segments and isolate critical parts of the system.

5. Control access to the system: Provide physical and logistical access controls.



Advanced Persistent Threat (APT) attacks targeting critical infrastrucure like dams have become common.

6. Harden the components of the system: Lock down the functionality of components.

7. Monitor and maintain the system: Update anti-virus signatures, install patches and monitor for suspicious activity.

Another best practice is to follow the principles of Defense in Depth, which emphasize using many layers of defense, and avoid reliance on a single technology such as a perimeter firewall.

It is important to look for technology solutions that are designed for the plant floor. The harsh physical environment, the staff skills, the unique communication protocols and the focus on safety and reliability distinguish industrial requirements from IT requirements.

Here's a guide to selecting technology:

• **Industrial components**: First, ensure that all network components — including cabling, cabinets and active equipment — are industrially hardened, resilient and have high mean-time-between-failure (MTBF) ratings. The demands of the plant floor are typically much harsher than the typical IT environment and require equipment to match. Furthermore, the requirement for 24-hour operations means that availability, not confidentiality, is the most important security attribute on the plant floor.


It is critical that security and event monitoring is integrated into industral management systems.

Redundancy and robustness: Having equipment that is easy to disrupt makes the attacker's job easier and the support staff's job much more difficult. Active components of the network, such as switches and routers, need to support industrial redundancy technologies such as Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). If security or production cameras are part of the network, then the switches must have the bandwidth and multicast video support necessary to support these services.

• **Seek technologies that integrate with industrial network management systems:** Industrial switches and routers are supported and secured by trade personnel that are typically not IT professionals. This means that integration into industrial management systems is critical for both support and security event monitoring. The same holds true for firewalls that secure communications between business networks and industrial networks or other areas of the plant — they all need to integrate into your industrial network management system of choice.

• **Deploy firewalls that secure industrial protocols:** Firewalls should be optimized to secure SCADA protocols such as Modbus and OPC, rather than email or web traffic. Web and email messages simply have no place on a plant floor system — products that inspect these protocols simply add cost and complexity to the security solution.

• **Practice Defense in Depth with zone-level security:** Using the best practice of Defense in Depth, security should not end with a perimeter firewall for the plant network. Instead, production networks should be segmented according to ISA IEC 62443 standards. Each zone of devices should be protected with its own industrial firewall that can be deployed into a live plant network without risk to operations.

Focus Your Efforts

Your enterprise IT team focuses its efforts on its most important assets. Every control system has one or more assets that would seriously impact production, safety or the environment if successfully attacked. These might be the safety integrated system (SIS) in a refinery, the PLC controlling chlorine levels in a water filtration plant, or the RTU in an electrical substation.

Your control engineers know what really matters to the operation. If those assets are aggressively protected, the chance of a truly serious cyber incident is massively reduced.

Another area for focus is detection. The industrial automation world is poor at detecting anything unusual on control networks. Make sure your firewalls and other security devices have good reporting capabilities, and are integrated into an industrial management system. Your production engineers and operators should be immediately alerted if a read-only remote operator station suddenly tries to program a PLC.

Waiting for the IT team to analyze the event the next morning is too late.

Teamwork is Required

As the vulnerability of industrial assets increases, it is important to understand the ways in which industrial and enterprise-level security intersect and diverge. IT and engineering teams need to work together within organizations, as all industry participants must work together to ensure that best practices are in place and that innovative advances to security are developed and deployed.

Whether your organization is a critical infrastructure provider or your enterprise has one or more industrial networks, securing these networks has never been more important. ▮

Eric Byres is CTO at Tofino Security, part of Belden's Hirschmann industrial networking group. He is an expert in the field of critical infrastructure security and can be reached at eric.byres@belden.com. Brian Oulton is Director of Industrial Vertical Marketing at Belden. He has 27 years of experience in the industrial automation industry and can be reached at brian.oulton@belden.com.