BELDEN
SENDING ALL THE RIGHT SIGNALS

White Paper

Industrial Cyber Security—Essential to Assure Availability, Safety and Resilience

Foundational Controls for Security, Compliance & IT

Don't believe there are real cyberthreats to your operations network and control systems? Data shows otherwise. Better foundational industrial cybersecurity practices can help prevent disruption to your operations and financial risk to your bottom line.

Industrial control systems (ICS) are the workhorses of our physical world, and those systems are becoming more networked and more accessible by the day—often from anywhere on the planet with an Internet connection. Security experts worry that the growing dependence on Internet-connected devices, also called the Internet of Things, or IoT, is outpacing our ability to secure them. As some have wittily observed, the "S" in IoT stands for "security."

Gartner Research in late 2016 predicted there will be 8.4 million Internet-connected devices by the end of 2017, a pace that leads to an estimated 20.4 billion "things" operating in—and running—our world by 2020. This security concern is particularly warranted within industrial and critical infrastructure, where cyberthreats can result in physical disruption, loss of availability and even risk to the environment and public safety.

Table of Contents

On the other hand, many ICS professionals continue to feel that the actual threat to plant operations and process controls is light, given their highly purpose-built industrial equipment, specialized communications protocols, air gaps, unique automation systems and processes, and safety instrumented systems. Unfortunately, that's not what the data shows in a National Cyber Security and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team report for the U.S. Dept. of Homeland Security.

Disruption Can Be Costly

Disruption is also not just an operations hit—the costs to the business overall can be significant:

- When the Michigan Board of Water and Light was hit by ransomware in April 2016, the total impact for a few days' outage plus related costs was disclosed later that year to be in excess of $2 million. While it was the corporate side of the utility that was impacted, experts said access to the operations side of the organization would not have been difficult, especially since the attack came through email. This event demonstrates that an incident can be costly. Fortunately, they had cyber insurance.
- The biggest, and what is believed to be the most costly, attack in history occurred in 2012 to Saudi Aramco. A terrorist faction called "The Cutting Sword of Justice" used Shamoon malware to take down Saudi Aramco's operations. The company was impaired for months, and costs were estimated to be well over $1 billion dollars (since Saudi Aramco is privately held and has never disclosed its incident costs, it's not known for sure). However, over 35,000 computers had to be replaced, the entire global organization was disconnected from the Internet to reduce the scope of the attack, and business processes were reduced to paper, pens and phones.

FY 2016 Incidents by Sector (290 total)

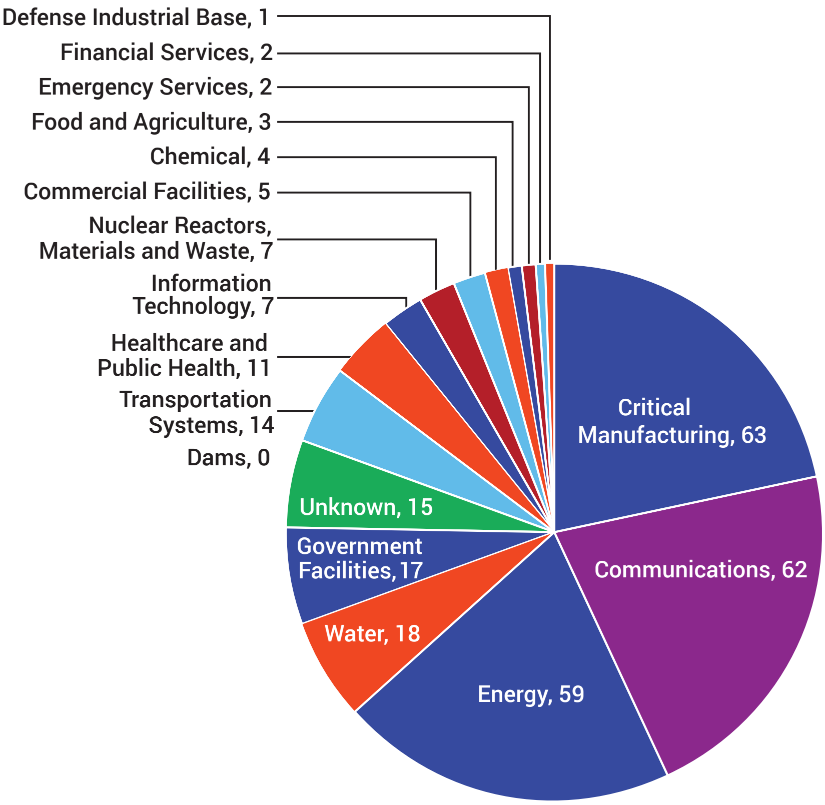

Fig. 1 Top three known critical infrastructures under attack are 1) Critical Manufacturing 2) Communications and 3) Energy. Source: https://ics-cert.us-cert.gov/Year-Review-2016 Incident Response Pie Charts FY2016

It's Not All About Hackers and Attacks

Here are a few other incidents illustrating three common and costly areas of disruption that can occur due to internal employee or contractor errors, malware propagation and equipment failures. These errors and incidents, which occur without any malicious intent, are very common, are viable threats to operations, and are among top concerns by plant management due to disruption and cost.

Case Study and Lessons Learned: U.S. Water Utility Hacked

ICS security can and should be seen as an essential requirement, supporting and enabling availability and safety. Operations and process controls must not be disrupted, and this remains top priority within nearly any industrial or critical infrastructure organization. Unfortunately, as the latest rounds of malware and ransomware have impacted businesses globally, it's become obvious that cyber risks must be addressed even in the most challenged industrial environments. Let's examine a recent industrial incident and then summarize some useful industrial-specific security lessons learned for availability and safety goals.

An unnamed water district, dubbed the Kemuri Water Company (KWC) in Verizon's 2016 Data Breach Digest experienced unexplained patterns of valve and duct movements over at least 60 days. It was discovered that attackers were manipulating the chemicals used to assure safe drinking water and also altering the water flow rates, causing disruptions to water distribution. Many other activities had gone on unnoticed, including theft of more than 2.5 million unique data records, until Verizon's forensic investigation started.

In this case, physical harm and safety was at risk, but luckily didn't happen due to alert functionality that caught the chemical and flow control issues. Also, it appeared that the type of outside attackers who gained access were likely "hacktivists," who are usually not motivated by financial gain. Indicators are they were experimenting and shopping their access around to others with more knowledge of the unique environment.

What's Wrong with This Picture?

Look at how KWC set up its network in Fig. 2, as depicted in the Verizon 2016 Data Breach Digest. Can you tell where they went wrong? (Here's a hint: Note the seven red callouts in the diagram.)

Verizon's forensic investigation found that three known threat actor IP addresses had gained access multiple times to the water district's operations technology (OT) and IT assets, including:

- The supervisory control and data acquisition (SCADA) application, valve and flow control applications, and the PLC systems
- IT management systems
- Internet web server application
- Financial and customer account information

KWC had no visibility or insight to the IP addresses being used from global locations accessing their network, assets and controllers, and manipulating their field I/O. They also hadn't caught the millions of records being electronically stolen from their site. What can be learned from the investigation into their case?

Cyber Security Lessons Learned

KWC had multiple foundational security control weaknesses or exploitable vulnerabilities that Verizon said made them a great candidate for easy hacking from the outside—with a potential high impact to safety and availability. Let's look at each and how Belden's Cyber Security product suite could have helped:

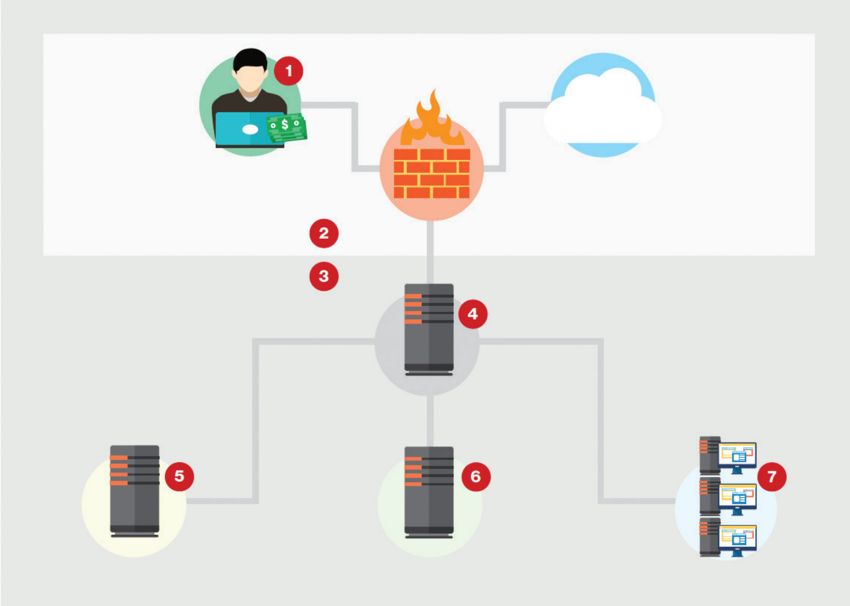

Fig. 2 KWC's network architecture was a large factor in the success of their breach. Legend: 1. Customer access to payment system, 2. External (Internet), 3. Internal (corporate access), 4. AS400, 5. PLC management, 6. Finance access (PII access), 7. IT management. Credit: 2016 Verizon Data Breach Digest

- Weak password hygiene in the customer web application. Water customers used an Internet payment application to access their accounts from laptops, desktops or mobile devices. This application only required weak credentials (user name and password—no second authentication factor) to gain access to customers' personally identifiable information (PII), payment data and water usage.

  The first factor in the attack to consider was that the web-facing application server customers used had a cross-site scripting vulnerability the hackers could exploit. The second factor was that the username and password methodology for creating user credentials was easy to exploit. For both of these types of weaknesses, Tripwire could have helped.

  - Regardless of how rigorous or weak any organization's password hygiene is, Tripwire solutions can alert on multiple login attempts to a given asset, host or endpoint. They can also test for password length, password complexity and other password specific settings. Over time, organizations can improve credential requirements as they educate users, and Tripwire products can be adjusted for more rigorous password hygiene to reflect the business' unique requirements.
  - Tripwire products can passively monitor logs and correlate events such as login attempts and credentials. By monitoring multiple types of host syslogs, these correlations can reduce the time it takes to see suspicious behavior beginning to traverse the networks and assets.
  - Tripwire has proven integrations with many identity management systems. The integrations can be used to create efficient workflows with the context and details needed when credential misuse or suspicious behaviors may warrant an alert and follow-up.
  - With deep packet inspection capability, Tofino's Xenon security appliances could have denied attackers the ability to modify to the programmable logic controllers (PLCs). Tofino Xenon can be deployed behind the switch or router and in front of the PLC, DCS, RTU, or IED to filter, based on the contents within commonly-used industrial protocols such as DNP3, Modbus/TCP, GOOSE and OPC DA. This seamlessly creates smaller, more secure network segments. Tofino Xenon security appliances are stealthy devices

Disruption Can Be Costly, Part Two

- Oil pipeline shut down for six hours after software is accidentally uploaded to a PLC on the plant network instead of the test network. **Net impact? $250K**
- 13 auto assembly plants were shut down by a simple Internet worm; 50,000 workers stop work for one hour while the malware is removed. **Net impact? $14M**
- Operators at a major US nuclear power plant forced to "scram" the reactor after cooling drive controllers crashed due to "excessive network traffic." **Net impact? $2M**

with no IP address, making them invisible to attackers. However, Tripwire products can monitor and report on configuration settings for Tofino Xenon units, giving operators visibility into the units and to assure ideal configuration state, and detect unauthorized or inadvertent modifications to firewall settings.

- Direct Internet access to ICS (and bad network architecture). The Internet-facing web server that hosted the customer payment application was directly connected to the AS400 system, which in turn housed the SCADA management application, giving the administrator (and threat actors) direct access to interact with the control system. The water district's valve and flow control application on the AS400 was used by the three known threat actors to manipulate the PLCs and subsequently water chemistry.

  Tripwire solutions can continuously monitor for changes on servers, workstations, HMIs, data historians, databases, email servers/Active Directory and more. In this case, Hirschmann's Industrial HiVision network management software can visualize devices it sees on the network and could potentially have presented a visual depiction of assets, making this poor network architecture obvious. If modifications from an ideal state allowed for the AS400 to be directly connected to the Internet, Tripwire's products could have alerted administrators that a change was made to the corresponding network settings.

  Tripwire solutions can alert on suspicious logons, and would also be able to monitor for unknown or foreign IP address logon attempts after normal business hours. Tripwire can also track accounts, group membership, ports, applications and services, DLLs and other changes that may occur on the systems it monitors. Hirschmann's EAGLE20/30 industrial firewall, if placed between the AS400 and the control system, can create a secure and protected zone to limit access to its SCADA application. To provide more robust protection without requiring changes to network architecture, Tofino security appliances can be deployed similarly in front of the field PLCs or DCS to inspect all incoming and outgoing traffic and alert (and optionally deny) on any traffic that is unauthorized or blacklisted.

  Encrypting traffic is another way of creating a secure network, as it prevents man-in-the-middle attacks and ensures traffic is received only from trusted sources. Hirschmann's EAGLE20/30 and GarrettCom's Magnum 10RX, Magnum 5RX and Magnum DX940 firewalls and routers provide multiple types of encryption techniques and VPN connectivity for multiple remote sites and networks.

- Privileged administrative user. The lone AS400 system administrator had no corporate oversight, and for convenience was using the same login credentials for remotely accessing both the AS400 and the payment application web server from his laptop. Least-privilege rules would've been difficult for this smaller utility with only one system administrator. However, there could've been some better practices in place.

  Best practices for securing UNIX systems often include restricting remote administrative logons in several ways. First, by removing the capability for the "root" user to log on remotely. Second, by removing remote password authentication completely, allowing only key exchanges for logons. These minor changes are often seen as inconveniences by administrators and therefore are often not implemented or reversed. Tripwire's ability to test for these settings could have rendered the attacker unable to log in in the first place.

- Login credentials in cleartext accessible from the Internet. The login credentials and IP address were found in clear text within the initialization file (.ini)—an old-school technique known as "security through obscurity" (STO). The same credentials worked to log into the payment application web server. A simpler way to say this? "Hey, here's how to log onto our systems—all of them..."

  With a simple query, Tripwire products can locate cleartext files that contain administrative credentials, PII or payment card information. The ability to locate and alert on improperly-stored sensitive information can be extremely valuable.

- Harden your network infrastructure. An automation network that is engineered with a security mindset is a defensive asset in its own right. Belden switches, routers and firewalls from the Hirschmann, GarrettCom and Tofino brands can be used to create a defense-in-depth network approach by applying the concept of "zones and conduits" from international security standard IEC 62443 as shown in Fig. 3. Many different security features, such as network access control, firewalling and address spoofing detection, can be used to significantly harden the security posture of the network. Industrial HiVision can monitor the network and display the security status of the network devices, as well as provide information on their software level and configuration integrity.

- Single Point of Failure. One AS400 served as the water district's SCADA Application system. The system was old, operating system updates and patches weren't installed, and again, one lone administrator was working to make things easier—but not with security in mind.

  Tripwire solutions can continuously monitor and assess systems, configurations, hardware, software and firmware versions, and show when patches are available but not applied. Within industrial settings it is not unusual for patching to be limited—if performed at all. The old saying, "If it ain't broke, don't fix it" applies here. However, at least in this case, the security of the AS400 would have benefited from being continuously monitored by Tripwire solutions, since its cyber risk was high due to lack of updates and patches.

It Can Happen to You

This is a clear example of how better ICS and SCADA security practices could have prevented process controls and business activities from being disrupted. For industrial firms, availability is a top priority, and operations teams often see industrial Cyber Security as unnecessary due to their high trust environment.

It's easy to believe "it could never happen to us." However, noting the weak or absent foundational ICS and SCADA security in the Kemuri analysis should give you pause to consider what your environment holds—to some degree similar risks are probably present.

It might be a stretch to catch plant engineers or contractors charging personal devices on PLC or HMI USB ports, or allowing a contractor or family member wireless access from the hidden router in the back room, but these are just two real-world examples among many. ICS security best practices and awareness training may be something to consider for your own environment.

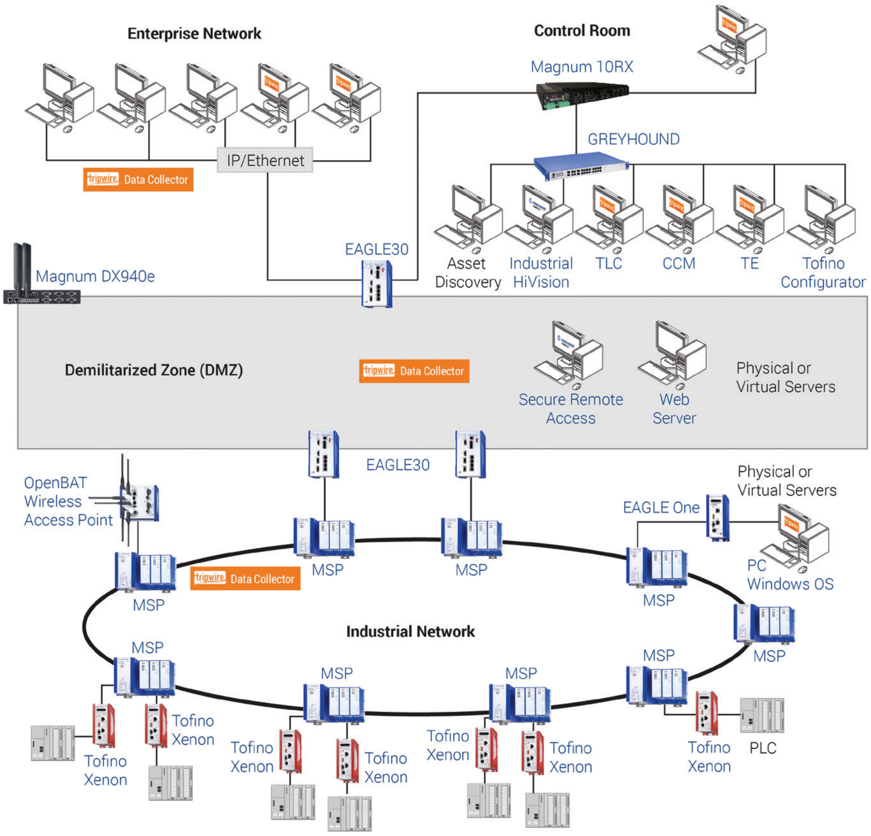

Fig. 3 Reference architecture secured with Tripwire and Belden solutions.
Legend: TLC = Tripwire Log Center, CCM = Tripwire Configuration Compliance Manager, |TE = Tripwire Enterprise

Getting Started

- Begin with a Cyber Security assessment to discover gaps you can then discuss and prioritize internally. Given how connected most organizations are becoming, consider including the corporate side as well as plant operations in the assessment. Plus, IT may be where the budget exists for taking this important first step.
- Determine what industrial security standards and best practices you need to work against. Most assessments will work to identify weaknesses and countermeasures according to some type of industrial Cyber Security standard appropriate to your industry. For water and treatment utilities, standards to consider are the American Water Wastewater Association's Process Control System Security Guidance for the Water Sector, the National Institute of Standards and Technology (NIST) Cyber Security Framework, and the International Society of Automation (ISA) Industrial Automation and Control Systems Security/International Electrotechnical Commission (IEC) 62443 standards.

Summary

We will continue to see overall ICS cyber risk increase as industrial and critical infrastructure becomes more interconnected and even field I/O becomes Internet-aware. With attackers and insiders adapting and evolving their tactics, this will work to put physical assets at even greater risk. As recent malware "CrashOverride" (AKA Industroyer) and "Trisis" (AKA Triton) have proven, knowledgeable industrial outsiders are becoming increasingly sophisticated about how to levy disruption for the biggest impact to our cyber-physical assets. In the November 2017 Trisis malware attack against a Middle East utility, researchers confirmed that attackers used industrial protocols and safety systems to cause disruptions.

Regardless of the industry, these lessons learned should give rise to an understanding of how important and essential ICS security is to building resilient organizations—that is, ones that can suffer internal mistakes or contractor errors and still avoid large-scale outages or costs associated with disruption. Industrial and critical infrastructure organizations should assess what's most critical to their operations and profitability, leverage the most foundational basics for layering defenses as much as their environments will allow, and build increased resiliency into their day-to-day operations.

> *You know my top concern? It's my own guys. Well-meaning as they may be, they cause most of my headaches. They're constantly tinkering with the control systems and sometimes update the firmware with "improvements" without telling me (or anyone, really). So then when stuff goes wrong, I don't know why, they're not always around and I don't even know what to back out and replace with what. And that doesn't even account for all the unexpected updates to our Windows systems that IT surprises us with.*
>
> *—Plant Manager with mixed industrial equipment environment*

Belden Competence Center

As the complexity of communication and connectivity solutions has increased, so have the requirements for design, implementation and maintenance of these solutions. For users, acquiring and verifying the latest expert knowledge plays a decisive role in this. As a reliable partner for end-to-end solutions, Belden offers expert consulting, design, technical support, as well as technology and product training courses, from a single source: Belden Competence Center. In addition, we offer you the right qualification for every area of expertise through the world's first certification program for industrial networks. Up-to-date manufacturer's expertise, an international service network and access to external specialists guarantee you the best possible support for products. Irrespective of the technology you use, you can rely on our full support – from implementation to optimization of every aspect of daily operations.

For more information: www.belden.com | www.beldensolutions.com | Follow us on Twitter @BeldenIND

Americas
1.855.400.9071
www.belden.com

EMEA
+49 (0) 7127 / 14 1809
www.beldensolutions.com

Be certain.
Belden.