Brief: S&R Pros Can No Longer Ignore Threats To Critical Infrastructure

When Selecting Security Vendors, Look For Specialized Industry Expertise

by Rick Holland
with Stephanie Balaouras and Katherine Williamson

WHY READ THIS BRIEF

For years, security and risk (S&R) professionals have focused almost exclusively on protecting the organization's sensitive information resources, such as customer data, intellectual property, and trade secrets, and the systems that process and store this information. Until recently, S&R largely ignored the organization's operational technology and automated systems. As organizations instrument, automate, and interconnect these systems to improve safety, improve service reliability, reduce costs, and generate new sources of revenue, they do so with more sophisticated software and network connectivity. If something is controlled via software and connected to a network, it will be compromised. Now S&R pros must worry about how they will protect the integrity and availability of gas pipelines, power grids, and medical devices, just to name a few examples. As the Internet of Things explodes, S&R pros will have to contend with the security and privacy of a plethora of connected things; in this brief, we focus on the cybersecurity of critical infrastructure and industrial control systems found in the energy, waste water, and chemical industries.

THE THREAT TO CRITICAL INFRASTRUCTURE IS REAL

Security and risk pros got a major wake-up call in 2010 when Stuxnet, sophisticated malware codeveloped by the Israeli and American military, targeted Iranian industrial programmable logic controllers and, according to some reports, wiped out one-fifth of Iran's nuclear centrifuges.[1] This success made it immediately clear that critical infrastructure, including nuclear centrifuges, power grids, water systems, and transportation systems, was now vulnerable to cyberattack.[2] Stuxnet is an example of the highest tier of threat against these environments, but there are others, and they are targeting nongovernment entities:

- **Adversaries are ready to pounce on Internet-connected devices.** At the 2013 Black Hat Europe conference, Kyle Wilhoit, a researcher from Trend Micro, demonstrated how adversaries are eagerly awaiting an opportunity to target critical infrastructure. For his research, "Who's Really Attacking Your ICS Equipment?" he set up Internet-facing honeypots that emulated supervisory control and data acquisition (SCADA) and industrial control system (ICS) devices found in a water treatment plant.[3] Wilhoit's research results were disturbing; it took only 18 hours to find the first signs of attack on one of the honeypots. In addition, 12 of the 39 attacks could be classified as targeted.[4] If you have SCADA or ICS equipment that is connected to the Internet, you can be sure that adversaries will target it.

- **State-sponsored agents will target private companies' operating critical infrastructure.** Wilhoit's research didn't cover the attackers' motivations, but there are other examples that draw this out. In March 2012, the US Department of Homeland Security (DHS) issued alerts related to a gas pipeline sector cyberintrusion campaign against multiple pipeline companies.[5] More recently, infamous

Chinese hacker UglyGorilla has been implicated in a similar reconnaissance activity, this time against a Northeastern US utility company. "He plucked schematics of its pipelines. He copied security-guard patrol memos. He sought access to systems that regulate the flow of natural gas. He cruised channels where keystrokes could cut off a city's heat, or make a pipeline explode. He was looking for information China could use to wage war."[6]

- **Attackers are leveraging watering hole attacks.** Close to the four-year anniversary of Stuxnet, security firm F-Secure discovered that the websites of ICS vendors were being targeted in watering hole style attacks.[7] The attackers replaced legitimate software installers with Trojanized versions, including the Havex remote access Trojan (RAT).[8] When the ICS/SCADA administrators installed the software, they gave the adversary access to their environment. The malware then proceeded to sniff traffic specific to ICS/SCADA environments. F-Secure stated: "The malware component gathers any details about connected devices and sends them back to the command and control (C&C) for the attackers to analyze. It appears that this component is used as a tool for intelligence gathering."

Examples like these are disconcerting for both policy-makers and the operators of critical infrastructure. In the United States, the National Institute of Standards and Technology (NIST) released the voluntary "Framework for Improving Critical Infrastructure Cybersecurity" to provide guidance for federal agencies.[9] There is also growing activity within the security vendor community in what has traditionally been a niche security space.

SECURING OPERATIONAL TECHNOLOGY IS DRAMATICALLY DIFFERENT

In the classic book *Men Are from Mars, Women Are from Venus*, author Dr. John Gray provides a practical way for men and women to improve their communication by acknowledging the differences between their needs, desires, and behaviors.[10] There are fundamental differences between traditional information technology (IT) and operational technology (OT). Thus, just like the Martians and Venusians, S&R pros from IT and OT must respect and accept each other's differences and learn to work together. Only then can the relationships be successful. To do this S&R pros should understand that:

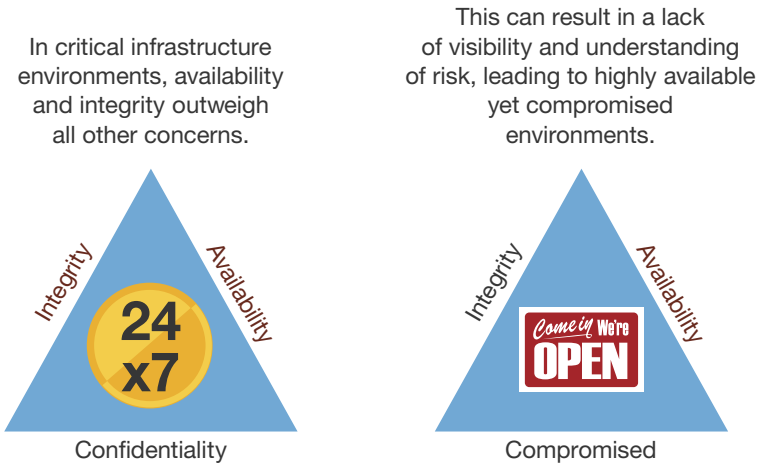
- **Availability reigns supreme.** In OT environments, the traditional confidentiality, integrity, and availability (CIA) triangle is applied very differently. Availability and integrity trump confidentiality; safety and performance are also a high priority. One cannot understate the cultural differences with this approach; attempting to play the "this isn't secure, you cannot proceed" card won't work. Unfortunately, this focus on availability can result in a lack of visibility and understanding of risk, which can lead to highly available yet compromised environments (see Figure 1).

- **There is no margin for error.** In your traditional corporate IT environment, you may have intrusion prevention systems (IPS) deployed as intrusion detection systems (IDS), or web application firewalls (WAFs) that are deployed out of band so as not to block legitimate traffic. In an OT environment, imagine that the legitimate traffic you inadvertently blocked stopped a critical process that takes out a power grid or shuts down a water pump to a municipality. Prevention becomes a problem, and the importance of change management increases tenfold.

- **Refresh cycles are generational.** In the traditional IT world, hardware is typically refreshed every three or four years. In the OT world, hardware is refreshed every 20 to 30 years. Much of the hardware deployed in OT networks is insecure by design and simply won't be replaced for the sake of security. Security needs aren't enough to overcome the huge capital investments made in this equipment. As a result, security is bolted on, not baked in.

- **Endpoint security is challenging.** The need to ensure the availability and integrity of OT systems makes endpoint security very difficult. In some cases, endpoint security isn't even an option for proprietary operating systems running in these environments. In other cases, when a Windows endpoint is an option, OT organizations elect not to deploy patches or agents for fear of affecting availability and integrity. Companies like Kaspersky Lab have OEM relationships with vendors like Emerson to provide protection on Windows-embedded operating systems. They work with the vendor to ensure that patches and security updates don't affect availability or integrity.

Figure 1 In OT Environments, Availability Reigns Supreme



117142 Source: Forrester Research, Inc.

SECURING OPERATIONAL TECHNOLOGY REQUIRES INDUSTRY EXPERIENCE

During the spring of 2013, we saw two notable acquisitions in the market for critical infrastructure protection. These acquisitions signal growth in the critical infrastructure protection market and the value of having specialized knowledge and expertise in the industries most concerned about critical infrastructure. We expect to see additional acquisitions as traditional information security vendors seek to increase their knowledge and capabilities within OT environments. S&R pros should note that:

- **Lockheed Martin acquired Industrial Defender.** On March 12, Lockheed Martin announced an agreement to acquire privately held Industrial Defender, headquartered in Foxborough, Massachusetts.[11] Industrial Defender's Automation Systems Manager (ASM) provides visibility into security, compliance, and change management activities across industrial control system environments. Industrial Defender has had success working with regulated industries like power companies that must meet North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements.

- **General Electric (GE) acquired Wurldtech.** On May 9, GE announced an agreement to acquire privately held Wurldtech Security Technologies, based in Vancouver, British Columbia.[12] Wurldtech provides technology and services to help assess, protect, and certify critical infrastructure and industrial products. Wurldtech offers the Achilles certification for device manufacturers; this assessment provides a benchmark for the secure development of the applications, devices, and systems found in critical infrastructure. According to Wurldtech, "four of the top six global automation vendors use Wurldtech Achilles products to increase the security robustness of their products."[13] Given that GE no doubt competes with these automation vendors, it remains to be seen how much longer competitors will seek out these Achilles certifications. GE plans to keep Wurldtech as a separate business unit in an attempt to allay these concerns. This acquisition does highlight the trend of hardware vendors increasing their security knowledge and capabilities.

Beware Of IT Security Vendors Masquerading As OT Security Vendors

Given the market opportunity around critical infrastructure protection, it isn't surprising that vendors are rushing to provide products and services to address the need. Many of these vendors lack experience working with OT and are taking a traditional information security approach to solving the problem. It isn't uncommon to see a vendor promoting a traditional network security solution such as intrusion detection or intrusion prevention as being "critical infrastructure/ICS/SCADA ready," when in fact the solution doesn't speak the protocols typically seen in these environments.[14] Understanding a vendor's experience and a solution's capabilities specific to your environment is critical. There are vendors with technologies and services that actually have experience securing OT environments (see Figure 2).

Figure 2 Example Vendors With OT-Specific Security Solutions

Vendor	Solution	Comments
BAE Applied Intelligence	Industrial Protect	Industrial Protect is a security appliance developed to protect connections between IT and OT networks. The appliance provides hardware-based security, ensuring the validity, integrity, and authorization of data exchange.
Bayshore Networks	Bayshore IC	Bayshore Networks provides a platform that evaluates and enforces industry standards and customized application-layer policies. Bayshore Networks' technology is Pallaton, an embedded, extensible, XML-based policy language.
Digital Bond	Consulting	Digital Bond provides research and consulting services for control system security. Digital Bond offers numerous tools, including SCADA Honeynet and Quickdraw SCADA ICS.
GE Wurldtech	Achilles	Wurldtech provides products and services for both device manufacturers and operators. Wurldtech provides security assessments to vendors as well as protection profiles to operators. Wurldtech also certifies both manufacturer devices and operator security practices.
Kaspersky Lab	Industrial Security Suite	Kaspersky Lab provides industrial security consulting as well as endpoint protection for devices running in industrial environments. Kaspersky Lab has partnerships with automation vendors like Rockwell Automation, Emerson, and Siemens. Kaspersky Lab also offers protection solutions for the operators of critical infrastructure.
Lockheed Martin Industrial Defender	Automation Systems Manager (ASM)	ASM provides visibility into security, compliance, and change management activities across industrial control system environments.
Red Tiger Security	Consulting	Red Tiger Security is a focused SCADA Security consultancy, training, and research firm. Some of Red Tiger Security services include: penetration testing, red-teaming, incident response, and SCADA Security maturity modeling.
Secure Crossing	Zenwall	Secure Crossing leverages a whitelisting approach. By allowing only the selected protocols and specific actions within those protocols and disallowing all other traffic, Zenwall provides the level of filtering needed for a customer to solve SCADA, Remote Location, or Zone Level security.

117142 Source: Forrester Research, Inc.

Figure 2 Example Vendors With OT-Specific Security Solutions (Cont.)

Vendor	Solution	Comments
SecurityMatters	SilentDefense	SilentDefense provides situational awareness and network monitoring designed and developed for industrial control systems. SilentDefense employs a proprietary technology, the Deep Protocol Behavior Inspection, to monitor critical processes to detect cyberattacks.
Sourcefire, part of Cisco Systems	FirePower	FirePower offers network based intrusion detection and prevention. FireSight provides passive network visibility into hosts, users, assets, applications, files, protocols, and vulnerabilities within critical infrastructure environments.
Tenable Network Security Solution	Passive Vulnerability Scanner (PVS)	PVS provides real-time passive assessments of SCADA/ICS environments. PVS performs asset discovery, identification into risks from assets, applications, and services. PVS offers visibility into vulnerabilities, suspicious network relationships, and compliance violations.
Tofino Security	Tofino Industrial Security Solution	Tofino Security appliances provide inline network segmentation with firewall, content inspection, and connection management capabilities.

117142 Source: Forrester Research, Inc.

RECOMMENDATIONS

YOU MUST HAVE VISIBILITY ACROSS YOUR OPERATING NETWORKS

Do you know if your OT networks are highly available yet compromised? Do you know what types of unauthorized changes are occurring? The accidental insider threat vector could have very similar ramifications as the external malicious threat actor. In Forrester's experience working with many critical infrastructure organizations, visibility into these networks and the changes occurring within them is extremely limited. To start improving your visibility, Forrester offers these recommendations:

- **Build relationships with OT leadership staff.** Too often, reporting lines between IT and OT don't exist and relationships between the groups are immature and, in some cases, nonexistent. If you don't have a relationship with OT, build one. If you do have a relationship, improve it. Explain to them that you want to enable their work in a safe and highly available manner.

- **Extend your network awareness and visibility.** Since 2012, we have recommended that S&R pros adopt network analysis and visibility tools to give them situational awareness into their corporate and extended partner networks; this same recommendation applies to OT networks.[15] The main consideration for network-based visibility is an understanding of the protocols your OT devices leverage.

- **Even with awareness and visibility, prepare for incidents.** Once you have visibility into these networks, when you see malicious activity occurring, you need a plan to contain and remediate it. If you have detective controls, you need to make sure you have integrations into preventive controls that can be called on in an incident response scenario.

ENDNOTES

[1] Source: David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," The New York Times, June 1, 2012 (http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?smid=pl-share).

Source: William J. Broad, John Markoff, and David E. Sanger, "Israel Test on Worm Called Crucial in Iran Nuclear Delay," The New York Times, January 15, 2011 (http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html).

[2] Source: Michael Joseph Gross, "Stuxnet Worm: A Declaration of Cyber-War," Vanity Fair, April 2011 (http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104).

[3] Supervisory control and data acquisition (SCADA) networks are systems and/or networks that communicate with ICS to provide data to operators for supervisory purposes as well as control capabilities for process management. Source: Kyle Wilhoit, "Who's Really Attacking Your ICS Equipment?" Trend Micro, 2013 (http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf).

Industrial control systems (ICS) are devices, systems, networks, and controls used to operate and/or automate industrial processes. These devices are often found in nearly any industry — from the vehicle manufacturing and transportation segment to the energy and water treatment segment. Source: Kyle Wilhoit, "Who's Really Attacking Your ICS Equipment?" Trend Micro, 2013 (http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf).

[4] Source: Kyle Wilhoit, "Who's Really Attacking Your ICS Equipment?" Trend Micro, 2013 (http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf).

[5] Source: Mark Clayton, "Alert: Major cyber attack aimed at natural gas pipeline companies," The Christian Science Monitor, May 5, 2012 (http://www.csmonitor.com/USA/2012/0505/Alert-Major-cyber-attack-aimed-at-natural-gas-pipeline-companies).

[6] Source: Michael Riley and Jordan Robertson, "UglyGorilla Hack of US Utility Exposes Cyberwar Threat," Bloomberg Businessweek, June 13, 2014 (http://www.businessweek.com/news/2014-06-13/uglygorilla-hack-of-u-dot-s-dot-utility-exposes-cyberwar-threat).

[7] Watering hole attacks, also known as strategic web compromise (SWC), occur when threat actors compromise websites that will subsequently infect their actual targets. Upon visiting the site, a zero-day exploit compromises the unsuspecting visitor. The threat actors use the newly infected target as a launching point for intrusions against the targeted organization. For more information, see the May 15, 2014, "Introducing Forrester's Targeted-Attack Hierarchy Of Needs, Part 1 Of 2" report.

[8] Source: F-Secure, June 23, 2014 (http://www.f-secure.com/weblog/archives/00002718.html).

[9] Source: "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology (NIST), February 12, 2014 (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf).

For more information, read the upcoming Forrester report, "New NIST Cybersecurity Guidelines Target Firms That Serve US Federal Agency Customers."

[10] Source: John Gray, Men Are from Mars, Women Are from Venus, Harper Paperbacks, 2012.

[11] Source: "Lockheed Martin To Acquire Industrial Defender," Lockheed Martin press release, March 12, 2014 (http://www.lockheedmartin.com/us/news/press-releases/2014/march/0312hq-industrial-defender.html).

[12] Source: "GE to Acquire Wurldtech to Advance Cyber Security Efforts for Critical Infrastructure and Operations Technology," General Electric press release, May 9, 2014 (http://www.genewscenter.com/Press-Releases/GE-to-Acquire-Wurldtech-to-Advance-Cyber-Security-Efforts-for-Critical-Infrastructure-and-Operations-46fe.aspx).

[13] Source: "Achilles Communication Certification," Wurldtech Security Technologies (http://www.wurldtech.com/data/content/file/WUR_ACC_Data%20Sheet_LR.pdf).

[14] Protocols like DNP3, Modbus, ICCP, IEC, and Siemens S7.

[15] We have provided in-depth information about network analysis and visibility in a previous report. See the January 24, 2011, "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" report.