Addressing ICS/SCADA Cyber Risk

BY ROBERT BIGMAN

Introduction:

In addition to the many challenges Chief Information Security Officer's (CISOs) must already deal with, recently the topic Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) risks has fallen into the collective laps of cyber security organizations to solve. **However, unlike traditional systems with mature operating systems (e.g., Linux), commercial applications (e.g., Oracle) and standards-based protocols (e.g., TCP/IP), the ICS/SCADA environment is a mishmash of highly proprietary, obscurely encoded, and limited functionality systems that increasingly sit as (usually, poorly documented) end-point devices on enterprise networks.** While CISOs everywhere are still struggling with securing even traditional network end-point devices, the additional responsibility to now also secure arcane ICS/SCADA systems and networks clearly raises the CISO stress-level to new heights. This article both articulates these vulnerabilities and offers a recommended approach for CISOs and organizations to remedy ICS/SCADA cyber risks.

A Clash of Cultures:

Until recently, most CISOs (and their cyber security organizations) paid little (if any) attention to ICS/SCADA systems and networks. Traditionally, ICS/SCADA was part of the infrastructure that the people who "worked outside" were responsible for. ICS/SCADA systems and networks were part of the operational platform (e.g., oil/gas production, security system, traffic management) and not visible to the people who "worked inside" and managed enterprise Information Technology (IT) systems and networks. Accordingly, the people who "worked outside" were also not visible to the people who "worked inside." The two cultures (for the most part) almost never needed to talk to each other even though their worlds (as early as 1998) were beginning to increasingly intersect. The cultural difference is indeed proving to be a significant factor in addressing ICS/SCADA security risks. As noted, the part of the organization that manages and monitors ICS/SCADA systems are professionally and organizationally integrated into the business area that develops, delivers and administers the business technology (e.g., oil/gas production

About the author:

Robert Bigman is the former Chief Information Security Officer at the Central Intelligence Agency where he held the position for 15 of his 25 agency career years.

Receiving numerous awards, Robert built the model information security program used today in the US Intelligence Community.

As the top security professional in the agency, Robert contributed to almost every Intelligence Community and US Government information security policy, and frequently briefed congressional committees and presidential commissions.

Bob current is the founder of 2BSecure where he continues to advise both fortune 500 and governments around the globe.

infrastructure). They are almost never part of the organization's IT profession and organization. Indeed, many of the people who manage ICS/SCADA systems have little (if any) knowledge of the organization's IT technology infrastructure (other than being an IT service user), corporate IT policies, governance rules and strategies/plans. ISC/SCADA planning, development and operations are "part and parcel" of the planning, development and operations of the business technology organization. The business technology organizations have their own lexicons, process cycles, management techniques, professional development/career tracks and, yes, corporate cultures. ICS/SCADA systems are managed by business unit technology people and not corporate IT technology people. In large companies, this also includes ICS/SCADA security engineering and operations. ICS/SCADA security people are (like the business technology people) part of the business technology organization and not part of the corporate IT security (i.e., CISO) or corporate security (CSO) organizations. ICS/SCADA security people tend to speak about "event codes," "6LoWPAN," and "signal gateways," and only recently have terms like "firewalls," "intrusion-detection," and "file integrity monitoring" "creeped" into their lexicon. ICS/SCADA security has even become a specialized discipline within the industrial/device control industry. However, people in this field tend to come from/associate themselves with the ICS/SCADA industry and not the cyber security industry.

Of course, the flip side of this coin is also true. Ask any corporation CISO about their organization's ICS/SCADA systems and you will most likely get the "deer in the headlights" look! Rarely, is a CISO also responsible for ICS/SCADA systems. **In fact, interviews have found that IT technology people know far less about ICS/SCADA systems than business unit technology people know about corporate IT.** Not only do CISOs not know about the organization's ICS/SCADA systems (nor the people that operate them), more worrisome, they also cannot tell you if, where and how corporate ICS/SCADA systems connect into/share bandwidth with their IT LANs and WANs. Not surprisingly, when CISOs are (eventually) brought into the ICS/SCADA systems security discussion, they tend to have very little to offer. Most CISOs, simply do not understand both ICS/SCADA systems technology and how to secure them. CISOs live in the world of commercial IT, where systems operate without power limitations, operating systems run without memory limitations and applications are coded without concern for programming language limitations. There is a large body of knowledge and both open-source and commercial tools available to secure commodity IT and budgets to secure same are almost always respectively higher than budgets to secure ICS/SCADA systems.

The Technology Challenge:

As noted earlier, the greatest challenge to securing ICS/SCADA systems (with or without the participation of corporate IT and the CISO) is their increasing exposure to greater network access and the inability to integrate traditional technical controls (especially in older processors with both limited operating system functions and limited memory capacity).

ICS/SCADA systems were never built to be secure. They were designed to be lightweight, low energy consumption, limited functionality processors. Both the microprocessor and the operating system ran (for the most part) proprietary firmware and (optionally) a Unix/Linux variant instruction set. The ICS/SCADA application functions were limited to sensor signal collection and formatted message forwarding to a corporate industrial network monitoring system, usually using a proprietary communications protocol. However, as ICS/SCADA technology became more sophisticated, they were able to perform even more functions (e.g., two-way message communications) using smaller microprocessors, with increasing application functionality and, most importantly, the introduction of the TCP/IP communications protocol stack. **It was this evolution of ICS/SCADA technology (from arcane/proprietary processing devices to recognizable "commodity" microcomputers) that opened the door to potential security exposures.** It is exactly at this time that the two cultures (described earlier) should have begun planning how to

smartly (and securely) integrate evolving ICS/SCADA technology with corporate IT networks and systems.

However, this never happened. Corporations everywhere found opportunities to save money and increase operational efficiency by interconnecting their vulnerable (now TCP/IP aware) ICS/SCADA systems to their existing corporate IT networks. While they certainly save money and indeed become more efficient, they also introduce potentially grave security risks that are not easily remedied. As a result we now have potentially millions of ICS/SCADA systems at risk due to their unmanaged connections into corporate IT networks. Horror stories abound about the ability of hackers to use penetrations of corporate IT networks to then move laterally and remotely control ICS/SCADA systems (e.g., December 2015 Ukrainian Power Company). There is empirical evidence of attacks against ICS/SCADA systems using the corporate IT network as a launching point in the Oil/Gas industry, manufacturing industry and, most worrisome, hospital/health care and medical device industries. Of course the inverse of this connectivity is also occurring. Hackers are now exploiting corporate IT systems by entering the network via ICS/SCADA systems, usually via third-party companies under contract to monitor the ICS/SCADA infrastructure. While the most prominent example of this attack is the Point-of-Sale network attack on the Target Corporation (2013), there are numerous empirical examples of these hacking campaigns. In fact, there is considerable threat intelligence of sophisticated hacking organizations using tools and hacking services to identify ICS/SCADA systems that are both openly exposed to the Internet or easily accessed via other networks (e.g., third party companies).

Isolation – The Best Remedy:

So, what is a CISO to do when they are handed this, often serious, risk to remedy. An immediate response (should be) to first establish the necessary integrated governance structure to ensure that all future requests to connect ICS/SCADA monitoring/support systems to corporate IT networks receives sufficient management and technical security oversight. This is a classic “stop-the-bleeding” approach. However, as noted earlier, what about all the existing connections that already place the organization at unacceptable risk?

A possible remedy is to establish an integrated team that combines representatives from the business unit’s ICS/SCADA technology organization with technical representatives from IT security to find all said network connections and document them by a criticality risk priority order. Obviously, corporate IT network connections to sensitive ICS/SCADA systems (e.g., two-way message protocols that modify control system functions) or exposed ICS/SCADA system TCP/IP endpoints (e.g., external building security monitoring devices) that have access into core IT network routing functions) are of the highest risk. Once identified and cataloged by risk priority order, the next step is to ensure that they are all properly secured to the identified risk level. Of course, the first reaction to address the risk will be to simply physically disconnect the ICS/SCADA system monitoring function/ protocol from the corporate IT network. Another approach is to better secure the actual ICS/SCADA endpoint devices. While some of the newer ICS/SCADA devices (although very few) with higher performance and greater memory can run more secure operating systems (e.g.Green Hills Integrity RTOS) and secure protocols (e.g., IPSec), this approach does nothing to address the lack of security in the large body of “dumb” ICS/SCADA devices. Physically disconnecting the “dumb” devices from the network certainly eliminates the risks, however it also limits the ability to have any visibility/control into the ICS/SCADA network monitoring the control device(s). Of course, it also leaves the operational business unit with a new unfunded mandate since they need to develop a new capability to monitor/ manage their industrial platform. Another solution is to build TCP/IP layer 2 cryptographically isolated subnets (islands) that retain connectivity with the corporate IT network but do not allow any unauthorized data to pass between them.

Products like Entegra**BLU**™ enable organizations to build the necessary isolation between ICS/SCADA networks and the IT corporate network, without resorting to physically disconnects. Entegra**BLU**™ employs hardware (i.e., layer 2) VPNs to enable organizations to efficiently isolate the "dumb" ICS/SCADA device networks without wholesale re-architecting of the corporate IT network. The ICS/SCADA monitoring/control consoles can be logically (e.g., IPSec VPN) connected into the ICS/SCADA networks from isolated corporate IT network workstation endpoints, potentially even using software defined networking (SDN) capabilities.

Another option would be to extend only one-way data pipes from the ICS/SCADA systems networks to the existing monitoring networks. While such one way (i.e. data diode) approaches do isolate the ICS, they limit the flexibility and role of the operators to a monitoring function, and the data may still be intercepted. The ICS itself is safe, but the data may not be secure. Entegra**BLU**™ can provide an encapsulation of the data stream to protect it from intercept in this case. Ultimately, organizations can use these combinations of technologies to also securely access ICS/SCADA networks and perform device management, firmware/software patching and even trusted remote access monitoring. Defense in depth is the key to a robust security approach, and the Entegra**BLU**™ defense at the border is the key first line of defense.

By building cryptographically isolated subnets (ICS/SCADA network islands), organizations can both efficiently protect their ICS/SCADA network investment and ensure that they cannot be accessed by an exposure in the corporate IT network. Similarly, organizations can also be confident that any exposures within the ICS/SCADA networks do not put the corporate IT network at risk.

Conclusion:

As noted, there are two significant changes that need to be made in organizations to address the ICS/SCADA system network risk. First, organizations need to make structural changes in the way they manage and secure both their IT corporate and ICS/SCADA networks. It is essential that organizations implement stricter and more integrated programmatic and technical governance to enable the two cultures to work together and make "corporate" risk-aware decisions. Second, organizations need to implement truly segmented networks to protect ICS/SCADA monitor networks that are connected to the corporate IT network using layer 2 cryptographically isolation technologies.

Contact

See what EntegraBLU™ can provide for your network security…

info@entegratec.com