Creating a Comprehensive Framework to Protect Operational Technology Assets

BUILDING Cyber Security

By Andrew Froehlich,
President of West Gate Networks

The ability to remotely manage systems including HVAC units, vehicle fleets, manufacturing equipment and other operational technologies (OT) is seen as a tremendous time and money saver. However, a failure to properly protect OT assets can lead to data theft, loss of remote management and an overall danger to those working in or around them. Fortunately, help is on the way. Building Cyber Security (BCS) is a non-profit organization formed to create a comprehensive cybersecurity framework that's simple for owners of OT assets and systems to follow. BCS includes board members from both the private sector and US military/law enforcement. This collaborative effort will help the organization formulate a complete picture of the types of threats we all currently face. In this article, we lay out how BCS plans to develop a cybersecurity framework that can help organizations reduce risk while potentially increasing the overall value of OT assets.

What BCS hopes to accomplish from a cybersecurity perspective

The purpose of BCS is to create a system of standards, guidelines and best-practice advice for owners and operators of operational technologies. Unlike IT security frameworks that have been around for years, there currently is no comprehensive framework specific to OT security. According to Rick Varnell, BCS Advisory Board Chairman: "IT security is a well-defined role with plenty of cybersecurity frameworks to work from. This is not the case with operational technologies. Additionally, most enterprise and asset-based organizations don't have OT experts within IT. Where IT and OT intersect is a very important topic and it's why it's so important to bring in thought leaders from different verticals within the public and private sectors. Additionally, we are also seeking input directly from OT manufacturers themselves. These three groups best understand the current OT cybersecurity landscape as well as where it is headed in the future. Our goal is to extract the insights and knowledge they've gathered over the years in protecting OT from bad actors. We can then take that knowledge and package it into a concise and easy to follow OT cybersecurity framework."

Another board member, former director of the NSA and US Cyber Command, Admiral Mike Rogers, also has

a take on how operational technologies will soon be handled within organizations. "In the future, you're going to see an IT/OT cybersecurity construct that has a much more integrated approach. Currently, the OT side of operations tends to think about security from a physical – rather than cyber perspective. IT is just the opposite as they think cyber-first with little thought put into physical aspects. If these two parts can be brought together, we can get better outputs from both IT and OT."

Why OT is becoming an increasingly formidable security risk

Unlike IT security, OT security remains a relatively new topic with far fewer experts in the field. This includes not only operational experts – but the manufacturers of OT systems that are attempting to better secure their devices and platforms to match IT cybersecurity benchmarks. Adm. Rogers is beginning to see the right steps being made within certain OT manufacturers: "Cybersecurity within much of the OT product development process has long been an afterthought – if it's thought of at all. However, this is beginning to change now that the market is growing and customer interest in better security of these devices is at an all-time high. Developers of OT products are finally beginning to take security more seriously as it will soon impact their bottom line."

Emerging network technologies including 5G also brings current OT security capabilities into question. The ability to rapidly deploy IoT and IIoT sensors throughout buildings and campuses holds tremendous value while simultaneously increasing risk from a physical and cybersecurity perspective. "5G is a great example that changes the dynamic of smart building architectures, for example", says Rogers. "Buildings are becoming more like modern automobiles – they're increasingly less mechanical and less autonomous. As we see automobiles being joined through software and networks, the same is happening to buildings, campuses and plants. While we've long been talking about the pros/cons and security issues of network-connected cars, less thought has been put into this same situation with smart buildings and the infrastructure within buildings. Smart buildings and 5G integrations are great examples of the types of OT risks we're seeking to mitigate.

A founding member of BCS, Matt Davis, CEO of 5G LLC, whose company focuses on utilizing real estate assets to address 5G demand notes, "The expansion and capabilities of 5G are significant. 5G technology drives the need for over 5x the real estate locations in order to drive coverage and capacity at closer proximity. Working with technology companies, carriers, and real estate property owners, 5G LLC's participation with BCS is meant to drive the secure standards for wireless implementations for real estate owners, tenants, clients and carriers. The result of these standards is certifying property for secure wireless communications."

The BCS approach to helping organizations reduce OT risk

BCS hopes to take on OT risk in three different ways. First, the organization is currently bringing on manufacturers of OT products and services to assist with guidance on how to integrate cybersecurity features directly into their products. Adm Rogers optimistically reports "we're now seeing OT cybersecurity firms creating interesting partnerships with manufacturers of OT systems. Cybersecurity is not the core business of most OT manufacturers – but they're beginning to partner with cybersecurity companies so they can bake security directly into their products."

Second, BCS plans to build a comprehensive cybersecurity framework like those found within IT – but with OT-specific issues in mind. As Rick Varnell puts it: "We need to learn some of the lessons we learned in the IT world – and move them into the world of OT. Some businesses right now have two different groups responsible for securing IT and OT devices. These two groups often take drastically different approaches, and the one hand doesn't know what the other hand is doing. Our methodology is to take what we've learned from securing devices in IT and apply it to the OT cybersecurity side of the business."

While many aspects of OT cybersecurity overlap with IT cybersecurity, much of OT security risk mitigation does require a different set of skills. Securing industrial equipment, sensors and platforms is often drastically different compared to securing IT devices such as PC's, smartphones, and other commonly deployed endpoints. Many OT systems are highly customized and require a deep understanding of how the software and architecture works prior to being able to competently secure it. The BCS security framework will be designed to assist owners of OT assets to easily understand the risks of different types of OT systems and best-practice guidelines on how to secure them.

Finally, BCS intends to use their framework as an incentive launchpad for organizations that choose to implement it. Insurance companies are working with the non-profit to align their OT insurance premium pricing structure. The more segments of the BCS security framework that an organization implements and maintains, the lower insurance premiums they will be offered. Thus, BCS not only intends in helping lessen security risks – but also to increase the overall value of OT assets.