FIVE ACTIONS FOR IMPROVING **OPERATIONAL TECHNOLOGY SECURITY** IN THE DATA CENTER

January 2017

BAYSHORE

INDUSTRIAL-STRENGTH CYBERSECURITY™

FIVE ACTIONS FOR IMPROVING **OPERATIONAL TECHNOLOGY SECURITY** IN THE DATA CENTER

Introduction

Data centers contain operational technology (OT), which broadly refers to computerized industrial equipment. Data center OT system functions include heating, ventilation, and air conditioning (HVAC), fire suppression, power generation and conditioning, telecommunications, physical access control, and building automation. These systems are network connected and are often accessed through the Internet for monitoring and maintenance purposes.

Unfortunately, this connectivity puts not only these systems, but also the rest of your data center, at significantly increased risk from attacks. Attackers can take advantage of OT security weaknesses, such as those described in our recent white paper, "Operational Technology Security Challenges for the Modern Data Center", to attack and compromise both OT and IT assets within the data center. This could lead to data breaches and other typical incidents, but it could also cause major operational disruptions for your data center.

Many organizations are heavily focused on the protection of sensitive data and are not aware of the increasing risks to their data center operations and the potential consequences of attacks. In a recent example, an attacker remotely accessed an HVAC system. Alarms and auto protections were disabled, and temperature in the data center was increased. Servers and other equipment either failed or automatically shut down to prevent overheating causing significant downtime and repair costs. Similarly, an attacker could remotely tamper with the data center's power systems to cause an outage. The attacker could also issue commands to the data center's generators that cause them to operate well outside safe thresholds, damaging or destroying the generators and potentially causing a fire. There are many other examples as well, all of which underscore that OT systems pose real risk to data centers.

In this white paper, we provide **five actionable recommendations** for what you can start doing today to address your data center's current and future security risk from OT systems. Just these five recommendations encompass a great deal of what your organization needs to do to improve its data center's OT security.

Action 1: Understand your OT security risk.
Any new security effort should begin with an assessment of risk. This is particularly important for OT security, because every environment is different. Not only does every data center face a unique combination of threats and vulnerabilities, but every data center also contains vastly different physical and digital assets that need protection. Part of what makes OT security assessment different is that OT brings the physical and digital worlds together. For example, an attacker could compromise an OT asset in a way that physically damages or destroys the system, or even endangers the data center personnel. Understanding your OT security risk must involve not only the cyber risks and the physical risks, but their intersection.

In order to understand your OT security risk, you should perform the steps below. Note that these steps are not comprehensive; additional steps may be necessary. For example, you may need to do a security assessment for the network infrastructure used by the OT devices. The fundamental steps are as follows:

1. **Inventory existing OT devices.** Without an accurate inventory of OT devices, any OT security risk assessment will be incomplete and therefore inaccurate. There are tools that can help with identifying devices, such as network scanners and packet sniffers, but they are unlikely to find all OT devices. For example, scanning tools may not work across segmented networks. Also, the use of active scanning techniques may cause some older OT devices to react in potentially dangerous ways. Other considerations include the mobility of some OT devices and the use of short-range wireless networking technologies. Ultimately it is necessary to physically check all areas of the data center, with assistance from data center personnel who are familiar with the systems that may incorporate OT components.

2. **Document the basic characteristics of each OT device.** In addition to recording the fundamental information, such as the vendor and model of the device and its physical location(s), a variety of technical information should be documented. Examples include what software it uses (operating system, applications, etc.) and what versions are currently installed, which forms of networking it uses and can use, which protocols it uses for OT communications, which types of local interfaces it has (USB ports, etc.), and which applications or data need to be accessed remotely. In addition, it is important to document the OT device's criticality to the organization. What functions does the OT device perform, and how could manipulation or disruption of those functions affect the OT device, the data center, and the organization?

3. **Perform a risk assessment for each OT device type.** You should be able to use your organization's existing risk assessment methodologies to do this. Just make sure to take into account both digital and physical risks, and both external and internal threats. Note that an internal threat does not necessarily mean a rogue employee; many security incidents happen because of human error. A risk assessment that does not include internal threats will produce misleading results.

4. **Research which additional OT device types will be acquired soon.** Introducing a new type of OT device into the data center may significantly affect risk, so any short-term plans should be identified and the impact on risk analyzed to the extent feasible. Similarly, you should identify any major changes planned for existing devices, such as a new operating system version about to be released that will add new functions or security features.

5. **Summarize how data center OT is already affecting the organization's risk.** It is incredibly important to formally summarize how OT devices in the data center are already affecting the organization's risk. This summary should take into account the device inventory, device characteristics, risk assessments, and information on short-term changes to data center OT. The summary will be invaluable for educating others within the organization about the current state of security and the potential impact of successful attacks against one or more data center OT devices.

Action 2: Develop security requirements for OT devices.
Every organization with a data center should have digital and physical security requirements defined for its OT devices. Without such requirements, it is much less likely that OT devices will be secured effectively and have that security maintained over time. Ideally, your organization's existing IT security policies could simply be applied to OT, but in reality that's usually a terrible idea because of differences in IT and OT:

- IT devices are usually centrally managed, but most OT devices are not. Security changes that are easy to implement on many IT devices through a few clicks may need to be implemented manually on each OT device.
- Most IT devices do not need constant availability, so rebooting them to cause patches, configuration changes, and other security maintenance efforts to take effect is not a major problem. Most OT devices need to be available and functioning at all times, so outages needed to maintain their security may seriously disrupt data center operations.
- IT devices have a wide range of robust security features built in. Most OT devices have relatively limited security features, and some OT features have few security features or none at all.
- OT devices and software often have complex dependencies such as safety consequences. So the system may need testing after update/upgrade to ensure functionality is maintained.

These are all important considerations when developing OT security requirements. Make sure that each OT security requirement is feasible for your environment. Recognize that some important requirements cannot be met by all OT devices, and identify alternate ways of meeting those requirements instead of abandoning them.

Examples of possible topics for digital OT security requirements include the following:

- Changing all default passwords
- Enabling stronger authentication than passwords alone
- Disabling all unneeded services and protocols
- Configuring OT software and firmware to enforce sound security practices and to reject unauthorized configuration changes
- Patching OT software and firmware
- Encrypting all wireless communications
- Enabling and configuring logging, then monitoring the logs (ideally continuously, otherwise frequently)

Your OT security requirements should also address physical security, potentially covering topics such as the following:

- Allowing only authorized personnel to have physical access to OT devices and any cables or wires they use for communications (e.g., Ethernet cables)
- Monitoring all physical access to OT devices, or at least the areas where OT devices are located
- Specifying which physical interfaces (e.g., USB ports) are not permitted to be used, and defining the conditions under which such interfaces must be disabled or removed

In addition to defining security requirements for OT devices, it is also an absolute necessity to define safety requirements. The combination of digital and physical worlds may introduce new safety concerns for OT devices or at least make certain unsafe conditions more likely to occur. For example, an external attacker could send commands to a boiler to increase its temperature beyond a safe threshold. A robotic arm could accidentally be commanded to swing beyond 90 degrees. Security and safety risks must be considered together so that the organization's requirements cover both realms.

Action 3: Plan to acquire an IT/OT gateway.
As previously mentioned, many OT devices may not be able to meet all of your organization's digital security requirements. This is not necessarily a negative statement toward the OT devices and their vendors, but rather a reflection that OT devices are often used for decades. There is no way of designing an OT device that will definitely be capable of providing adequate protection against the threats and vulnerabilities of the next 20 or 30 years. There are also many cases where an OT device vendor goes out of business or stops supporting a particular product, basically ending any security updates for the devices.

The solution to these situations is to utilize a security technology known as an IT/OT gateway. An IT/OT gateway monitors all network communications to and from your OT devices, as well as the security events happening within those devices, to look for any signs of attacks or compromises. IT/OT gateways understand OT protocols, including specific OT commands and their data values, so they can identify and block commands that should not be permitted for security or safety reasons. Earlier in this white paper there was an example of an attacker tampering with HVAC temperature settings. Such an attack would easily be stopped by an IT/OT gateway because it would block commands to disable safety systems, and would recognize the specified temperature value as being above the permitted threshold.

IT/OT gateways also provide notable benefits to your organization's business. For example, they can translate OT operational data from vendor or product-proprietary formats into standard formats, then transmit that data to your organization's IT systems. This alone can be a major cost savings. For example, it enables centralized security compliance reporting for regulatory purposes instead of requiring staff to physically visit each OT system periodically, harvest its operational log data, and manually convert that data into a reportable format. Likewise, it enables business systems to study operational data to identify impending failures so that proactive maintenance can be performed, preventing costly outages.

Key steps to perform when planning to acquire an IT/OT gateway include the following:

1. **Educate yourself on IT/OT gateway capabilities.** Many IT professionals have not yet worked with IT/OT gateways, so it's reasonable to spend some time learning about their capabilities and what the current products offer.
2. **Determine how an IT/OT gateway can help pay for itself.** Examples of this are reducing the organization's security and safety risk, improving preventative maintenance planning, and enabling centralized regulatory compliance reporting.
3. **Make the case for the IT/OT gateway to management.** This may be necessary to get approval for IT/OT gateway procurement. The summary documented at the end of Action 1 (Understand your OT security risk) may be particularly helpful for this.
4. **Budget money and resources.** Like deploying any other new enterprise security control into production environments, IT/OT gateway deployment will take time. Keep in mind the calendar time, the financial budget, and the staff resources needed to select, procure, configure, test, and deploy an IT/OT gateway, as well as perform ongoing management and maintenance tasks. Over time the IT/OT gateway should lead to considerable money and resource savings, compensating for much or all of the initial costs.

Action 4: Add OT security considerations to enterprise documents.
Many of your organization's OT security considerations will be documented in security policies, as discussed under Action 2 (Develop security requirements for OT devices). However, there are other enterprise documents that may need to be changed, or at least reviewed, to ensure that they support OT security as well. Failure to do this may cause OT security to be overlooked and forgotten, making the likelihood of successful attacks against OT devices far greater.

First, your organization's key security documents besides policies, such as security plans and procedures, need to take OT security into account. This includes adding the IT/OT gateway to your enterprise security architecture and creating procedures for using, securing, and maintaining the IT/OT gateway itself.

Second, your organization's procurement-related policies and processes should take OT security into account. An example is establishing a formal set of security and safety requirements for all future OT device purchases. Another example is requiring that the security staff be notified before any new type of OT device is purchased, as well as giving the security staff the ability to specify how such an OT device must be secured.

Your organization may be affected in other ways as well. A common issue is penetration testing. Penetration testing documents, such as policies and rules of engagement templates, must explicitly state the potential impact of disrupting the availability or integrity of OT devices. Some organizations may choose to avoid any penetration testing involving OT devices, while others may put strict safeguards in place to minimize the risk to the organization. Make sure to carefully look for potential issues such as penetration testing so that they can be addressed proactively instead of reactively.

Action 5: Expand security education and training to include OT.

Your organization's security professionals must be educated and trained on OT security so that they are prepared to do their jobs with OT security in mind. It's important to provide OT security education and training to others within your organization and outside your organization as well. OT devices are often maintained at least in part by people who may not have prior knowledge of security practices. For example, a device vendor's technician may visit your site periodically to perform routine maintenance tasks. He or she may not be aware of the risks that work might inadvertently pose to your organization, such as connecting a USB drive to an OT device, which could allow malware to spread.

Here are a few examples of considerations for OT security education and training:

- Train physical security personnel about OT device physical security concerns. Make it clear how they should respond if they see certain human behaviors occurring in proximity to OT devices.
- Create educational materials on OT secure design and coding practices for the organization's software developers. When the developers start writing apps for OT—if they haven't already—they will understand what their responsibilities are and how they can fulfill them. (Note that requirements corresponding to these responsibilities should also be documented in your organization's security policies.)
- Prepare affected personnel not only to handle current OT security considerations, but also new and changing considerations related to acquisition of emerging OT technologies.

Conclusion

Your organization's data centers already contain OT devices. These devices link together the digital and physical worlds. That provides many benefits but also introduces substantial security and safety risks that cannot be ignored. This paper has described five actionable recommendations that you can start following today to improve data center OT security:

- Action 1: Understand your OT security risk.
- Action 2: Develop security requirements for OT devices.
- Action 3: Plan to acquire an IT/OT gateway.
- Action 4: Add OT security considerations to enterprise documents.
- Action 5: Expand security education and training to include OT.

These recommendations give you a major edge over other organizations by ensuring that your data center's OT devices do not provide an easy route for attackers to compromise or otherwise disrupt your data center's assets. The acquisition of an IT/OT gateway also provides business benefits that may help your organization save additional money. It is important that you start implementing these recommendations as soon as possible, because the longer you wait, the more work you will have to do to catch up.

Bayshore Networks is a pioneer in developing solutions for addressing OT-based threats in data center environments. The Bayshore IT/OT Gateway safely and securely protects data center infrastructures, devices, data, and staff from today's rapidly evolving threats. The Bayshore Networks product is highly customizable, enabling it to be used to monitor and analyze any OT protocol for instructions that might jeopardize data center operations, safety, or security. For more information on Bayshore Networks, visit https://www.bayshorenetworks.com/products/.