FEDInsider

Addressing Urgent Security Needs for Operational Technology

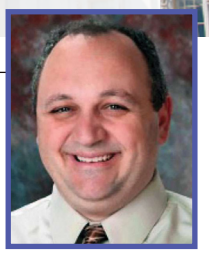
Operational technology today interacts heavily with IT networks, which is convenient for users but also carries many risks

Featured Experts:

- **Bob Costello**
  Chief Information Officer,
  CISA

- **Matthew Swenson**
  Division Chief,
  HSI Cyber Crimes Center

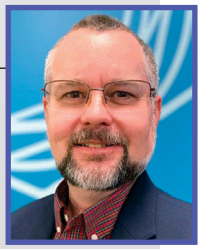
- **Joseph Fourcade**
  Lead Cyber Analyst,
  Veterans Affairs



- **Michael Dransfield**
  Sr. Technical Executive,
  Control Systems Cybersecurity, NSA

- **Josh Brodbent**
  Regional Vice President,
  Public Sector Solutions, BeyondTrust

- **Marty Edwards**
  Vice President,
  Operational Technology Security, Tenable



Unlike information technology, or IT, which is almost exclusively contained within the digital realm, operational technology (OT) involves the use of software and hardware to control physical processes, devices and infrastructure. Examples of these devices can be as small as tiny sensors or as large as the control centers of massive hydroelectric dams.

Originally, OT was kept on separate networks where attackers would have needed physical access to control panels, levers or switches in order to negatively affect a system. But recently, IT and OT networks have started to combine, which allows control of OT operations remotely through IT networks. That makes controlling OT more efficient, but also brings the host of IT cybersecurity problems over to the OT side, where there are few protections to stop them. This has created an increasingly dangerous situation where cyber attackers can physically hurt systems, infrastructure or even people.

Several experts in this field recently gave their thoughts about the problem and possible solutions at a FedInsider roundtable discussion. The following are some key points they made about keeping OT safe.

Separate IT and OT Networks As Much As Possible

While this seems like a simple answer, sometimes the best solutions don't need to be complex. Until recently, IT and OT networks were kept separate using a variety of methods to ensure safety. In the early days, this meant physical separation, which later evolved into more advanced solutions like cryptographic encapsulation or virtual LAN's.

"The first thing I would say is, unless it's fully a requirement, you still need to keep these IT and OT domains separate," said Michael Dransfield, Senior Technical Executive, Control Systems Cybersecurity for the NSA.

Dransfield described some modern ways that separation can be achieved without physically separating the networks. He mentioned there are ways to limit the exposure of a linked network by having the OT components only transmit the bare minimum data required to function, and to force those transmissions to be one way. Despite the limited exposure when using this method, many believe that is still too much and advocate for going back to total physical separation.

"I would say you should maintain separate identity systems for those higher security environments that exist in OT," said Marty Edwards, Vice President, Operational Technology Security at Tenable.

Edwards explained that OT systems should not be in the same domain as other so called corporate systems. And employees should not be capable of sitting down at their machines and logging into OT systems, especially in environments where only a very limited number of highly qualified people should have access to OT operations.

Designing for Convenience Increases Exposure to Cyberattacks

If a computer scientist twenty years ago was asked to predict the prevalence of operational technology and its uses today, they likely would have fallen well short of the mark given how much OT is now widely available in all sectors and even with the general public. Security systems, smart devices, intelligent environmental controls and other OT items have all taken hold in the mainstream. These items, while convenient, are often not designed by IT focused individuals, or by those with a deep understanding of cybersecurity.

"A lot of times when you have an OT device, what you have is something provided by a hardware manufacturer or an installer who is typically in a line of business that isn't traditionally IT," said Josh Brodbent, RVP, Public Sector Solutions at BeyondTrust. "Whether it's cameras, manufacturing, HVAC, refrigeration, or other devices, the IT side is all new to them."

Brodbent gave an example where a company was told that they had a vulnerability with one of their smart refrigerator models, but they didn't worry because there has not yet been an attack made against them. That means that there are potentially thousands of vulnerable refrigerators sitting in homes and offices right now just waiting for an attacker to exploit them.

"From an investigative perspective, I think that creates a significant number of attack vectors for threat actors," said Matthew Swenson, Division Chief, DHS Investigations Cyber Crimes Center. "Because as more and more systems come online and become accessible and integrated with other traditional IT systems..." the problem will only get worse.

Swenson said that many modern OT devices were like double edged swords. They are convenient and easy to control remotely, but also come with significant risk. And in addition to being vulnerable to attacks themselves, they can act as a gateway for an attacker to infiltrate a connected IT network.

There Is Hope In The Cloud

Every expert on the panel agreed that separation of IT and OT networks is the best solution to increase security for OT networks. But physical separation is not always feasible. However, as technology improves, it appears that cloud technology will be able to help put that separation back into place. With unlimited space in the cloud and the ability to configure the infrastructure however users want, it makes it possible to keep OT and IT networks apart while still allowing them to communicate through highly defined and monitored channels.

"We made sure that everything [at Veteran's Affairs] was segmented away from everything, but with the ability to communicate up at an enterprise level to one area within the cloud," said Joseph Fourcade, Lead Cyber Analyst for the Department of Veteran's Affairs. "It's not traversing the rest of the internet or the rest of the IT infrastructure, so it's not causing any type of problems or putting us at risk."

Despite some advances in cloud technology, Fourcade said that vendors still needed to do more in order to ensure proper cybersecurity for OT. This includes resetting or eliminating default passwords for OT devices and determining the best way to encrypt all traffic. Keeping OT that has been networked with IT safe will always present a challenge, but it is one that can be overcome if government and industry continue to work together on innovative protections and solutions.

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

Carahsoft
11493 Sunset Hills Road
Suite 100
Reston, VA 20190

(888) 936-2246
Tenable@Carahsoft.com
Carahsoft.com/Tenable
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
Twitter.com/Carahsoft

Tenable
6100 Merriweather Drive, 12th Floor
Columbia, MD 21044
Contact: **Susan Foster**

(301) 908-8974
SFoster@Tenable.com
Tenable.com/solutions/it-ot
Facebook.com/Tenable.Inc
Linkedin.com/company/TenableInc
Twitter.com/TenableSecurity

BeyondTrust
11695 Johns Creek Parkway, Suite 200
Johns Creek, GA 30097
Contact: **Josh Brodbent**

(870) 362-6581
JBrodbent@BeyondTrust.com
BeyondTrust.com
Facebook.com/BeyondTrust
Linkedin.com/company/BeyondTrust
Twitter.com/BeyondTrust