BLACK & VEATCH

ASK THE EXPERT

Smart OT Cybersecurity Starts before Asset Construction

IAN BRAMSON

Vice President of Global Industrial Cybersecurity

KEON MCEWEN

Head of Solutions Development Industrial Cybersecurity

Under attack: That's the condition of critical infrastructure today, and threats are accelerating.

This reality appears in the FBI's most recent Internet Crime Report, which tracks data from the Bureau's Internet Crime Complaint Center (IC3). Overall, the number of ransomware incidents shared with IC3 increased by 18% between 2022 and 2023, while cases targeting critical infrastructure rose from 36% to 42%.

FBI Director Christopher Wray summarized what's at risk when he addressed the U.S. House of Representatives members this past January. "Hackers are targeting our critical infrastructure — our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems," he said, adding that the intent is "to wreak havoc and cause real-world harm to American citizens and communities."

To help organizations combat these threats, we talked to two cybersecurity experts from Black & Veatch. **Ian Bramson**, vice president of global industrial cybersecurity, draws his expertise from more than 25 years of helping organizations secure digital environments. **Keon McEwen**, head of solutions development, has 10 years of industrial cybersecurity experience.

Sponsored by

BLACK & VEATCH

T&DWorld

What's driving the need for cybersecurity in operational technology?

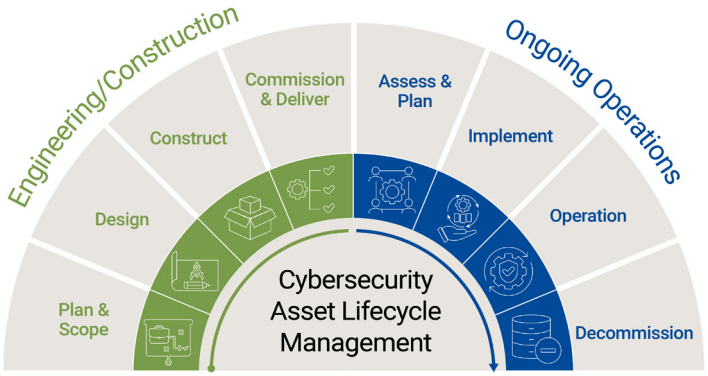
Over the past several years, operational technology equipment has been getting increasingly connected as organizations push to become more automated and efficient. Devices now connect to each other and the cloud, so there is connectivity growing both inside the organization and externally.

Together, connectivity and automation create an ever-expanding attack surface, meaning bad actors have more ways to get into the network and more things they can do once they're in.

What are the risks of having OT systems vulnerable to cyberattacks?

With connected operational technology, we're talking about cyber-physical systems, which means systems with integrated physical processes and digital controls. It's the digital world going into the real world of impacts. So, hackers want to take a valve that was closed and open it. They want to overheat something that shouldn't be overheated. They want to shut things down and blow things up.

The consequences are very different. If you open the wrong valve, it can put the site, the environment, and public safety at risk. Operational risk covers everything from small-scale events to national security. The entire complexion of cybersecurity is changing because of what is at stake.



How should organizations address cyber risks to operational assets?

Where is industrial cybersecurity today? Where does it live? It lives on all the existing brownfield plants and sites. Organizations are trying to protect the things they already have. A lot of organizations are playing catchup and plugging holes. What many haven't thought about is moving the cybersecurity starting point all the way back to when they're looking at building something new, whether it's a greenfield project or an upgrade.

Today, cybersecurity is not represented well enough when organizations build new assets. Cybersecurity is not in the requirements documents. It does not have a seat at the planning table in any significant way. That has to change with how the threat environment is changing. Things are more connected, and bad guys are getting more powerful every day. This means you must start building cybersecurity into building plans from the beginning.

What are the advantages of having cybersecurity built-in rather than bolted-on?

Organizations across industries are in various stages of their cybersecurity journey. While the most common approach to implementing cybersecurity protections is during asset modernization or retro-fitting upgrades for brownfield projects, new project builds are also a prime, untapped opportunity.

Many components of a cybersecurity plan can be more effective and significantly more cost-effective to build in from the beginning of your asset development and construction.

Take segmentation, which is the process of dividing a network into distinct segments with separate controls and access permissions so that bad guys can't get in and go wherever they want to go. It's very difficult and time-consuming to do this on a network that's up and running. You've got to think about production downtime and figure out what different parts of the network should be doing. The network maps you're using may not be accurate. Many people are involved in this effort, and it's not always that effective.

When you can build network segmentation from the beginning, you can cut down the number of people involved, design the network for its optimal function, and after it's built, you can test it. It's much more affordable, too.

You can also build in an intrusion detection system (IDS), which gives you visibility over your network. Planning that IDS from the very beginning means you can have visibility across the network from day one. That's what cybersecurity is. It all comes down to visibility and control.

How should organizations view OT cybersecurity to ensure they focus on the right things?

At Black & Veatch, we advocate for consequence-focused cybersecurity. Especially in operational environments, think about safety and uptime. The greater the consequence, the more you should focus on mitigating the risk. It's also crucial to remember that technology is going to keep evolving. You can keep up with it, but do not get left behind. That is not the right answer when you're protecting critical infrastructure.