HYDROCARBON ENGINEERING

CYBER-ENEMIES AT THE GATE

Avoiding the cybersecurity problem is no longer a viable strategy, but putting protections in place is more straightforward than it seems. **Alexandre Peixoto, Emerson,** explains.

For years – arguably even decades – many operational technology (OT) teams have practiced cybersecurity by obscurity. Systems were explicitly air-gapped to segregate every level of OT operations, and to provide the best protection against intrusion and interruption. Systems that never saw the outside world never needed to fear external attacks.

Today, however, the OT paradigm is changing. The most successful organisations around the globe are embracing connectivity to the wider world to unlock the operational efficiencies that drive competitive advantage in a global marketplace. These companies are implementing new technologies that unlock seamless data mobility from field to edge to cloud.

Nowhere is this more apparent than in the hydrocarbon processing industry, where technologies are rapidly changing to help organisations improve performance and continue to thrive in an unstable market. Successful organisations need connectivity to drive critical visibility and analytics both at the edge and in business systems, but navigating this change means finding new ways to ensure systems are cybersecure.

The new normal

Gone are the days where oil and gas, chemical, and petrochemical operations had deep benches of highly experienced personnel to drive efficient operations. Now, experienced analysts, operators, and technicians command a premium – in the rare instances they can be found. As a result, today's operations run very differently than those of just a decade or two ago. In many places, small crews of personnel are centralised and cover a wider area than ever before. Many of those individuals are coming from a new generation raised on constant connectivity and instant access to data, and workers of all ages require these features to perform their work efficiently (Figure 1).

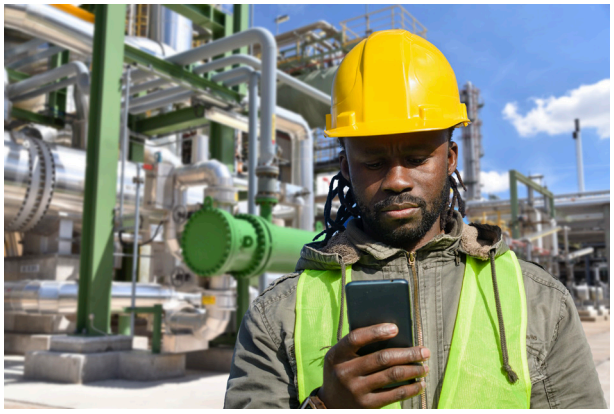

Figure 1. Modern digital workers expect constant connectivity, in the control room and in the field, for enhanced decision support.

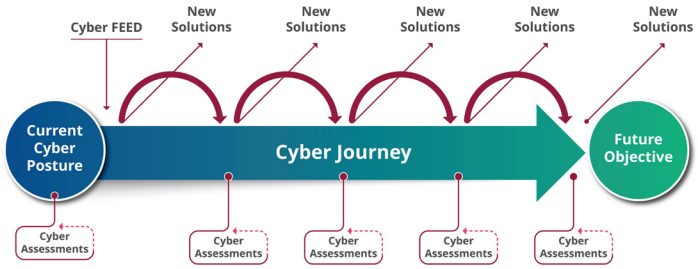

Figure 2. Cybersecurity is not set-and-forget. Any implemented solutions should be regularly re-evaluated for effectiveness via scheduled cyber assessments.

To meet the needs of this diverse workforce, data must be highly mobile. Edge solutions must contextualise data and deliver it to mobile devices in the field – and to business analytics systems in corporate offices – for constant awareness of plant health, instant mobilisation of resources, and enhanced collaboration, all to drive operational efficiency. This new connected, mobile workforce is the solution to increasing efficiency in the modern era, but it cannot work when companies must fear that bad actors may be able to insert themselves in the middle of the communication networks and wreak havoc.

Many organisations know they need to move in the direction of a boundless automation future, but they also see the ever-increasing number of cyberattacks now targeting OT assets. They know cybersecurity solutions can enable connectivity, but the same shortage of personnel necessitating change also impacts an organisation's ability to properly assess their need and build a roadmap for success. And even for organisations that may still have a deep bench of expert personnel, those people rarely have the time to commit to researching, identifying, implementing, and maintaining the cybersecurity solutions that will fit their unique needs, especially when threats change seemingly constantly.

But while implementing and maintaining secure yet connected operations is not a simple task, neither is it an insurmountable one. To succeed, teams must start by charting their journey, while also not being afraid to make course adjustments along the way. Several strategies can help them start and maintain those goals.

Define a starting point

The cybersecurity journey is key to navigating the external threats that can disrupt operations. Successfully navigating that journey requires teams to understand their necessary cybersecurity architecture and to know the steps they need to take. Air-gapping has long been a non-starter for OT systems, but interconnecting enterprise networks to everything else without a clear cybersecurity strategy is not an acceptable approach either.

One of the first steps of a cybersecurity journey is knowing the organisation's starting point. Every organisation – and in many cases each plant within an organisation – starts from a different place. A well-executed cybersecurity assessment can help teams successfully map out the key elements of their entire journey, while keeping in mind that a cybersecurity journey is an evergreen process because the threat landscape is evolving continuously.

For example, one of the key ways to identify critical steps on the cybersecurity journey is to understand the organisation's

existing cybersecurity posture. For some organisations, this might simply mean the development of policies and procedures that OT system users must follow. For others, it might be a complex environment of previously installed information technology (IT) solutions, each with varying levels of effectiveness. A cybersecurity assessment can help teams put a frame around existing solutions to determine what is working and what is not, and to show what is missing (Figure 2).

Define needs

One of the most common missteps on a cybersecurity journey is trying to find and implement solutions before defining the organisation's overall cybersecurity needs. Exciting, new cybersecurity solutions emerge each day, and it can be tempting to think that one appliance will fit every need across the environment, but this is rarely true. To implement solutions that work over the system's lifecycle, teams need to define the 'why' of their cybersecurity journey before they define the 'how'.

Need definition must consider the unique requirements of operating cybersecurity solutions in an OT environment. Whether an organisation has a deep bench of expert IT personnel, or a single person managing all of the company's technology, OT typically needs tailored solutions. All-in-one solutions engineered for the flexibility of IT systems typically do not function well within OT. Moreover, companies designing solutions for IT environments are rarely prepared to properly support OT issues. When defining need, it is important to consider the uptime requirements, safety concerns, and business drivers that are unique to OT. Although having similar cybersecurity goals, IT prioritises data confidentiality and record keeping, while OT prioritises system availability and safety.

Build the roadmap

After OT teams have defined their unique cybersecurity and business needs, they can begin to lay out the architecture to meet those requirements. As a team builds out its cybersecurity implementation roadmap, it is important to consider not only the solutions they will put in place, but also a plan to monitor those solutions. For example, an intrusion detection system reporting to a rarely used workstation is unlikely to draw the quick attention necessary when an attack occurs. Similarly, antivirus solutions put in place but never checked will have a very short window of efficacy.

To address these types of issues, organisations should develop written policies for monitoring and response of cybersecurity systems to ensure they will work properly and at full efficacy across their entire lifecycle. Patching is critical for cybersecurity solutions as well, so keeping these systems up to date is essential. Not implementing these and other best practices will hinder the overall cybersecurity posture of protected systems.

Build a cybersecurity culture

Once a path is defined and the OT team begins putting architectures and monitoring policies in place, organisations need to focus on compliance. The three pillars of cybersecurity – technology, process, and people – are all interlinked. The right technologies and processes must be in place to ensure security, but people must also be trained to use the technology properly and understand the value of a cybersecurity mindset.

Figure 3. Comprehensive training highlights the value of cybersecurity processes and procedures, facilitating buy-in from personnel across the organisation.

Cybersecure behaviour is not intuitive – it is learned. A key part of any cybersecurity journey should be developing training to teach personnel how to properly use the new solutions that are put in place. Moreover, part of that training should help users understand how a cybersecure operation protects and supports them. When technology, process, and people are all working together, users are more alert to how global changes may impact their ability to operate securely, and how that secure operation improves their own lives.

Users who see personal value are more likely to faithfully follow processes and procedures to help keep the organisation secure. With the right technology in place to help them maintain cybersecure operations, users can meet the organisation's benchmarks much more easily (Figure 3).

Identify key partners

Many of today's OT groups are choosing not to define, develop, and implement their cybersecurity journeys alone. With this approach, it is very difficult to stay up-to-date with the most current threats and their mitigations, and as more governments around the world increase cybersecurity regulation, keeping up with the mandates also becomes increasingly complex.

To address this and related issues, many of today's most successful organisations are partnering with automation solution providers who operate in both the OT and IT space to relieve the burden of developing a cybersecurity journey that fits their unique OT needs. Organisations partnering with experienced automation solution providers can count on expert guidance to help them select, install, maintain, and monitor the technologies that will work best for their unique environment.

Prepare for the future

In contrast to the isolationist cybersecurity policies of the past, modern cybersecurity solutions in the OT space

are designed to enable connectivity, rather than prevent it. Organisations moving toward connectivity strategies enabling widespread OT connectivity and real-time monitoring have created a fundamental shift in the way teams approach security – requiring them to thread the needle between uber-security and full convenience. Concepts like the zero-trust network architecture are securing identities, data, applications, networks, etc, in a more customised way, enabling enhanced connectivity and monitoring in real time.

To meet this new normal, both OT teams and their partners are considering more forward-thinking strategies. A team that needs to wait for every solution to be fully vetted, readily available, and tested by every major customer in the market will always be behind. Instead, modern users need ways to implement the pieces of larger cybersecurity initiatives, like zero trust, today, and then continue to evolve those solutions over time.

To meet this need, automation solution providers are now exploring ways they can plot zero trust architectures that will not be executed in a single year. They know the direction of the architecture and are building it piece by piece. As those pieces emerge, they can be implemented to update the existing architecture of their users. This agile development will help meet new threats as they arrive.

And while this new flexible model does create some uncertainty, it is also far more effective at adjusting to meet emerging threats, regulations, and shifting control architectures by empowering OT teams to meet their ever-changing security needs, without having to rip and replace entire architectures every time a significant new threat emerges. These types of cybersecurity solutions will be both more adaptable, and more cost-effective.

The most successful journey starts today

A rise in incidents around the globe has put the spotlight on OT cybersecurity, and few organisations still think they can hide from threats. Instead, forward-thinking organisations are taking steps to build a strong cybersecurity posture by shoring up defences as efficiently and effectively as possible. Doing so not only creates a work atmosphere that protects personnel and production from harm, but also fosters a more agile environment, unlocking the tools that allow OT teams to do more with less by driving better visibility and collaboration across their enterprise.

The tools and strategies necessary to successfully execute a cybersecurity journey are available today, but the journey takes time. The sooner an organisation starts to build its roadmap, the sooner it will be ready to operate in the modern economy.