Small steps BIG IMPACT

Alexandre Peixoto, Emerson, USA, discusses leveraging practical cybersecurity steps to safeguard energy operations and build resilience.

One of the most critical drivers of cybersecurity implementations around the globe has been regulation. After all, it is human nature to wait for enforcement before starting a new habit. Take vehicles, for example. Without speed limits, many would drive at excessive rates. In fact, few people even chose to employ their seatbelts – a lifesaving technology – in most areas of the world until there was a penalty in place for failure to buckle up.

As a result of this inherent resistance, regulations around cybersecurity for operational technology (OT) systems have become more prevalent lately, particularly in Europe due to the revised Network and Information Security Directive and the Cybersecurity Resilience Act. With so many pressures on modern hydrocarbon manufacturers – productivity, shareholder value, sustainability, etc. – cybersecurity is not seen as a quick win in quality or productivity, so governing bodies are trying to create other incentives, knowing the importance of risk mitigation in this area.

Yet, regulation is a poor catalyst for cybersecurity. Many organisations forget that the possibility of a fine is the smallest possible risk

they face from an ineffective cybersecurity posture. In truth, most of the pressures manufacturers face, such as productivity and shareholder value, are very much at risk when an attack happens. As evidenced by recent, high-profile attacks, today's cyber-attacks can easily impact digital systems, or even an entire enterprise for days or even weeks, resulting in revenue and reputation loss, and risks to the safety of personnel and local communities in the worst case (Figure 1).

Properly implementing cybersecurity solutions ahead of regulation will never result in a penalty, so it makes sense to get started on a cybersecurity solution as soon as possible. So why are OT teams reluctant to do so? In most cases it is because they are already running lean and wonder where they will find the time, and/or how they will get the approval to implement such complex technologies. But these teams are missing a critical concept: there is much that most OT teams can do to improve their cybersecurity posture, even with limited resources and expertise. Following a few key strategies provides many teams with just what they need to get started on their cybersecurity journey.

Identify the starting point

One of the key stumbling blocks for OT teams looking to improve their cybersecurity posture is not knowing how to frame the problem and, therefore, not understanding where to start. In most cases, the key to getting started is to understand the issue as a whole. A great place to begin is to identify the team's assets and systems, rate their criticality, and then consider the threats to those systems and their consequences. Often, a simple site assessment can go a long way toward helping an OT team understand what their key cybersecurity drivers are, and what the potential consequences are if they fail to act and protect them (Figure 2).

Some teams will find that they are at the very beginning of cybersecurity implementation, where all their assets are connected to everything else, or are wide open both locally and externally. Yet even these teams can find very defined starting points. Even beginning with one asset at a time can build momentum for a dramatic reduction of risk.

For example, does the plant have a critical asset that is guaranteed to shut down production and/or cause a safety issue if operated with malicious intent? If the answer is yes, securing that asset is an area where even a small team can focus their efforts. First, the team can identify if that asset has any exposure to the outside world. If so, that exposure needs to be mitigated. But even if it has no external exposure, it should still be protected against internal tampering as well.

Starting at such a granular level is often a more efficient and comprehensible strategy than trying to tackle organisational security from the top down. For OT teams struggling to get started, a granular approach can provide a starting point that launches other initiatives, all of which can eventually coalesce into a large scale plan over time.

Do the simple things first

Among the main reasons OT teams express a reluctance to implement cybersecurity solutions is that they see the technologies that information technology (IT) teams implement, and quickly identify that they are expensive, complicated, and often unsupported by OT vendors. Moreover, few teams want to implement solutions that are likely to create more work in maintenance and monitoring – teams are already lean, especially in remote sites.

However, while many IT technologies truly are complex, expensive, and time consuming, most OT teams getting started on their cybersecurity implementations do not need such comprehensive solutions. Spending lots of money on flashy technologies is no guarantee of 100% cybersecure operations. Often, the simplest and most cost-effective solutions are the most important, so teams should build a foundation of simple solutions by tackling risk surfaces in small bites.

Figure 1. The risks of cyber-attacks on OT systems are high, but so are the rewards for maintaining a cybersecurity posture to manage them.

Figure 2. A cyber assessment is often the first step to a cybersecurity evolution.

For example, many OT teams can create a significant improvement in their organisation's cybersecurity posture simply by checking user accounts and their privileges. Creating individual user accounts and assigning them privileges based on their unique roles is a low-cost solution that can typically be performed by the administrator of the site, and it will have a massive positive impact on the plant's overall cybersecurity footprint. In addition, ensuring systems are segmented correctly by creating space between the enterprise level and the OT space is another simple task OT teams can perform to harden their systems. Focusing on implementing a layered architecture in OT systems can also dramatically reduce risk.

Teams that have secure access and proper segmentation in place still face cybersecurity risks, but they typically do not immediately need to turn to complex IT solutions. Another small step such teams can take is to prepare for the unexpected – implementing a backup and recovery system so they can be back up and running quickly in the event of a breach.

None of these solutions require a massive outlay of money, technology, or expertise, nor do they require significant hands-on maintenance over time. Yet all of them will provide significant improvement to the plant and enterprise's cybersecurity posture (Figure 3).

Select solution providers who support success

Many orgaisations consider finding a solution that works well with their control system to be the biggest barricade to effectively implementing cybersecurity. However, these groups are framing the problem incorrectly. Today's most effective automation suppliers are well aware of the need for cybersecurity, so they should be a partner for cybersecure implementations of their systems, instead of simply a technology vendor. An effective automation supplier should be able to point to a comprehensive manual for securely deploying their technologies.

Any automation system should also come with guidance for securely setting up workstations, and the system itself. Moreover, effective automation solution providers will offer clear guidance on how to harden their systems – the dos and do nots – as well as how to set up and maintain user accounts securely. Ultimately, the OT team should not need an engineering team to perform custom configuration every time they need to add an automation solution, but they should instead have fast and easy access to practical documentation guiding them through secure configuration.

In addition, it is important to consider that the complexity of securing automation solutions increases with the number of different solution providers. The more varied the technologies that must be interconnected, the more complex an automation architecture will become, and each custom engineered solution becomes both a potential point of failure, and a potential point of contention as to which vendor is responsible for support. Maintaining a holistic ecosystem of seamlessly integrated technologies as part of a boundless automation vision can dramatically simplify both the ability to implement cybersecure solutions, and to manage that cybersecurity solution over the lifecycle of an organisation's assets.

Get ahead of the curve and stay there

Unlike safety, where many of the risks tend to stay static against the lifecycle of a process, cybersecurity risks are continually changing, even if the organisation's assets, processes, and protection solutions do not. Ultimately, cybersecurity is a lifetime commitment, which means once solutions are in place, OT teams need to ensure they continue to meet the needs of the organisation. While protectors must be vigilant at all times, attackers will only need a single opportunity to significantly impact a digital system with a cyberattack.

Therefore, one of the best strategies an OT team can follow is to perform regular assessments. Once the first cybersecurity solutions have been put in place – even if they are simple and basic steps – the team should set up regular auditing and reassessment of the system. As part of the reassessment, the team can evaluate if the solutions they implemented are still working, and if they are sufficient to mitigate the threats the organisation currently faces. In some cases, the solutions will still be enough, and in others, the team will likely need to make updates (Figure 4).

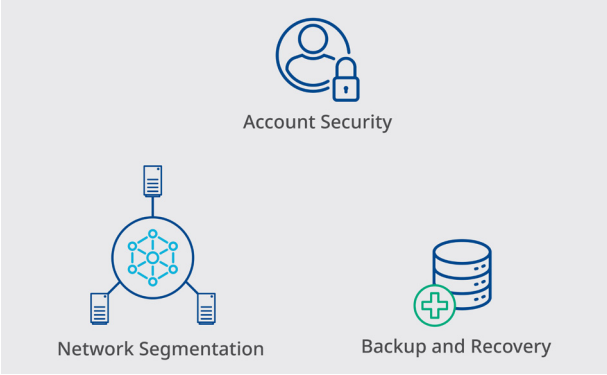

Figure 3. There are many things OT teams can do today – that are neither costly nor complex – to improve their cybersecurity posture.

Figure 4. Regular assessments are critical to maintaining an effective cybersecurity posture in a dynamic threat landscape.

The simple act of implementing basic cybersecurity mitigation steps and assessing them regularly starts the organisation on a cybersecurity journey. The first steps not only increase security, they also increase knowledge, typically revealing another layer of security the team could implement. Though it starts simply, the process will get more complex, but at a pace that is manageable.

For example, as a team implements more account security, they might notice legacy operating systems that could be updated for increased security, a solution that can be planned and budgeted as part of a future initiative. Once they understand the operating systems better, segmenting systems becomes easier. And with all those strategies under their belt, one day they may be installing firewalls for a further layer of protection. Every step keeps the team ahead of the curve and, more importantly, ahead of the organisations doing nothing, making them a less desirable target for the opportunists that make up most of the cyber-criminal community.

Generate buy-in

A team that cannot contextualise the cost of a cybersecurity attack will be unlikely to garner the support it needs to be successful. For most people interested in cybersecurity, protection for its own sake is justification enough for investment. However, in most organisations, OT teams must secure corporate funding to begin initiatives, and that funding is often tied to business outcomes. Fortunately, cybersecurity does directly impact business outcomes, though that connection must often be explained.

For example, 'We need to implement a cybersecurity solution because we do not want to risk falling victim to a cyberattack' is far less compelling than, 'Without cybersecurity protection, if we are attacked the same way our competitor was, we risk at least a week of downtime at an incredibly high cost per day. There will likely be rebuild costs of tens of thousands of dollars, as well as a safety impact that could endanger the lives of personnel, and/or an environmental impact from discharge that could incur thousands or even millions of dollars in fines. We also risk stock price damage from the reputational hit we take.'

Ultimately, securing buy-in is about putting the need for cybersecurity in terms that decision makers will understand, which typically comes down to lost revenue and production. The correlation is valid, but it is difficult to infer when not presented explicitly.

Today is the day to start securing systems

Cyber-criminals do not wait for regulations, and neither should organisations hoping to maintain their operations. Regardless of an OT team's expertise, there are concrete, basic steps they can take today to ensure their systems are less likely to fall victim to an attack. Moreover, when implemented following some simple strategies, those same steps typically start teams on a journey of continuous improvement that gradually reduces their exposure with each new step. This type of an improvement programme can have a concrete impact on a company's bottom line, as well as their safety and reputation – especially if they manage to stop an attack.