txOne networks | OT Cybersecurity. Simplified.

Yes. OT Cybersecurity is Achievable.

Build Resiliency by Mastering the Basics

Facts, fiction, and something in between.

On any given week, a new headline announces the impending threat from advanced attacks or nation-state actors. While it is true that these issues exist, what is usually missing from the report is the number of attacks from these sources compared to the others. Indeed, there is a lower percentage of attacks from nation-state actors than insider threats, which pale compared to the ~90% of attacks attributed to organized crime and other actors[1].

When the attack statistics are coupled with the motivations, 94.6% of which is for financial gain[1], we gain some clarity of the real-world truth. The cyber-criminals are operating a business driven by profits. To provide the maximum returns, target companies with poor security protections first. Suppose it is too difficult or time-consuming to attack Company Y because their security blocks the common attacks. Move on to Company X, which doesn't have protection. It's a simple case of "focus on the easiest target."

A common mindset for security is "It won't happen to us. Why would we be on their target radar?" For most organizations, this is true of nation-state attacks. However, cyber-criminals don't need to spend time finding targets manually, it's automated. When the basic security issues are detected by a cyber criminal's automated scanner, you pop up on their hit list as a juicy target that is easy to attack.

Yes. OT cybersecurity is achievable.

Do you know what makes security seem so difficult and hard to approach? A constant stream of information that describes the global cyber situation as hopelessly complex, which only a unicorn security team with an endless budget can defend against.

The good news, this is not the case. There is that a path to improvement exists for every organization, no matter what your current maturity is, and it all starts with mastering the basics. Why the basics? For the overwhelming majority of organizations, the attack that brings them down all starts from something simple like a weak password, poor remote access controls, or an unpatched vulnerability (often months or years old).

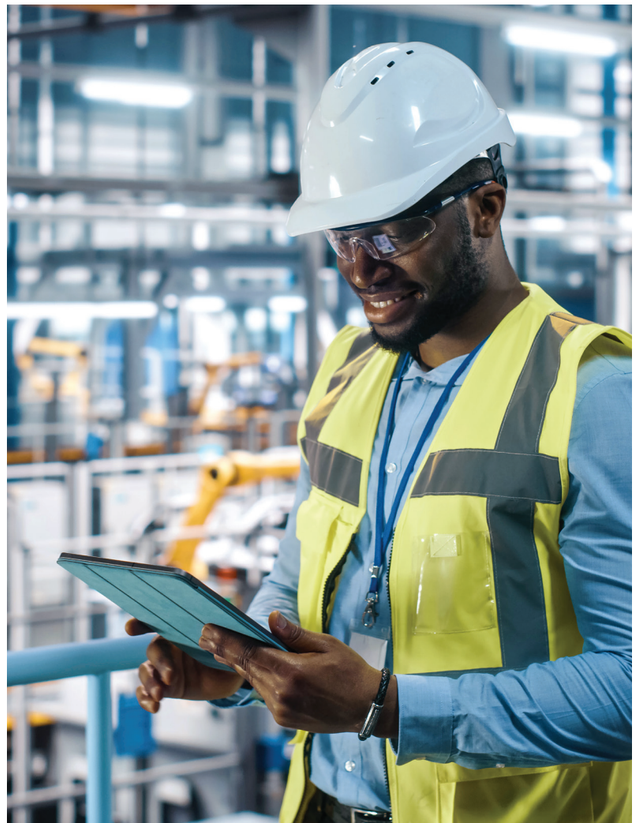
The real challenge to security resiliency is knowing where to start the journey. As with most things, moving from zero to one is the hardest step.

[1 - Verizon 2023 Data Breach Investigations Report - verizon.com/dbir]

Master the basics.

The collection of items and tasks that every organization should have in place, no matter the size or industry, is commonly called "basic cyber hygiene." These hygiene tasks are your first steps. Before you take any actions to defend against advanced attacks and threats, you first have to master the basics.

Defending against the latest nation-state attack is not the first step.



Basic Cyber Hygiene

The tasks and actions your organization should take first will differ based on where you are in your journey. With this in mind, completing the following tasks using an iterative approach will significantly improve your organization's overall OT security.

The tasks can be categorized into three steps:

1. **Address the immediate known issues**
2. **Assess your current maturity level**
3. **Start with low-risk/high-reward tasks**

Approaching security does not need to be a daunting task. The best method for improving your OT security is the one your organization can complete. So, consider these steps as a journey of improvement where each step improves security over time. Keep in mind that by focusing on small steps, rather than getting stuck trying to do everything at once, your organization will become more secure and resilient than it otherwise would be.

1. Control access to the OT environment – including IT and Internet connections.

If there is a connection between the OT environment and IT, or even a single device and the internet, put a robust OT-aware firewall in front of it.

Because these connections already exist, the exercise of assessing the risk and considering what protection is needed can be skipped. Instead, assume the risk will be realized and take action immediately.

2. Begin identifying devices and systems within all OT environments.

It is essential to know and track what devices and systems you have in your environment. You can't protect what you don't know you have. This will take time to complete and then prioritize for action.

Define a simple process and get everyone working on it – "For every device you use today, write down these pieces of information." Quickly, you will have a good list to start prioritizing decisions.

3. Fix the password issues that will exist.

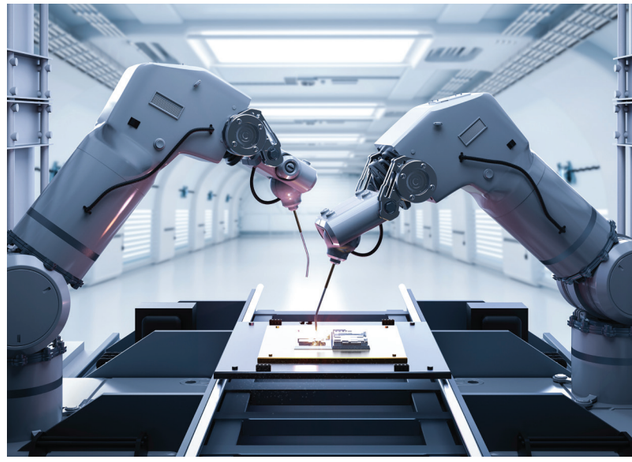
You can safely assume that there is significant password reuse, weak passwords, cross-domain passwords, and no password-used issues throughout your OT environment. When this is the case, it is child's play for an attacker to turn you into a victim.

Set a policy that uses the best practices in password strength but remains usable for the teams using the devices.

4. Scan and assess the state of everything in your environment.

Building out the asset list further, identify the device software and hardware version information and whether backups exist, including for the process files and configuration settings.

Maintain a centralized record of both the asset register and the assessments of them to measure your improvements over time.



5. Start the deployment of endpoint and network controls.

Working closely with the OT Operations Team to avoid unintentional impacts, begin deploying endpoint and network controls where appropriate.

Break down the deployment into different phases. Begin with low-risk systems to build confidence and gain insights on how to best monitor and administer the tools.

6. Monitor the events in your environment and develop an incident response plan.

In parallel, implement a procedure to monitor events, alerts, and any unusual activities. Start this early so security teams get comfortable with interpreting, validating, and actioning the data.

Develop an incident response plan to provide a framework to follow when events occur. Start simple, Including actions, notifications, and reports: think emergency checklist - not a complex flowchart.

7. Begin a security governance program that addresses security in a business context.

As you begin, develop a security governance program that provides a framework to guide maturity. Start with topics like roles and responsibilities, the review process, and decision-making.

The program should include all departments, not just IT and Security teams, to effectively maintain cyber hygiene as a shared responsibility across the entire organization.

8. Train all staff on security. Be sure to put this into a useful context and explain why it matters to them and why they should care.

Lastly, deliver security training to all staff. Focus on answering the question, "Why should I care? It's not my job," by making it relevant to their day-to-day work.

Remember, security that is ignored is worse than no security at all. If there is no security, at least you know there is a protection gap. If it is in place but is ignored, you get a false sense of security.

These simple measures form the bedrock of a secure and resilient OT environment and prepare you to tackle more complex security issues effectively. So, before you delve into the labyrinth of advanced cyber threats, remember - mastering the basics will swiftly bolster your OT security.

As you begin planning this journey, partnering with a security company with deep expertise will help guide you in the right direction to support your organizational goals. TXOne Networks has a strong relationship with leading OT OEMs and OT-specialist System Integrators, making us an ideal choice to partner with as you begin.

Supporting our expertise and drive to help you on your journey, simple yet highly effective tools from TXOne can accelerate velocity by removing complexity, ensuring your program is as efficient and robust as your organization deserves.

Contact TXOne Networks today to begin your OT journey with confidence.

txOne networks

txone.com

TXOne Networks | OT Cybersecurity. Simplified.

Contact Us