

What I Wish They Told Me When I Started in OT Cybersecurity: Hard hats, hard lessons, and the realities of plant-floor cybersecurity

After many years of showing up at *every kind* of site imaginable; refineries, plants, factories, hospitals, substations, water utilities, fabs, and places I'm still not sure were fully on the map. I've realized there's a whole body of OT field knowledge no one ever teaches you in training or certification courses. None of this shows up in NIST, IEC 62443, or your favorite OT maturity model. But all of it shows up in real life. OT cybersecurity isn't just about architectures, assessments, and controls; it's about hard hats, bad Wi-Fi, legacy systems, maintenance windows, and the people who keep critical infrastructure running despite everything we do to their networks — *the OT Environment*.

"OT cybersecurity, where theory meets steel-toe reality."

These are just a few of the things I wish I had known ahead of time...

- While vendors may say they supply the safety equipment you need, this will *not* include steel-toe boots in your size
- Don't wear anything to site that you wouldn't mind throwing out afterward
- TWIC is not Twix. One lets you on docks. The other does not.
- There is more than one kind of safety vest: no-sleeve and short-sleeve and yes, it absolutely matters
- Amazon sells inexpensive Nomex suits in many colors. Also: check what color *your* Nomex suit and hard hat are supposed to be (bonus points if you get it right the first time)
- There is no such thing as a "metric adjustable wrench" just in case someone on site asks to borrow yours
- It's not that OT teams refuse to patch (despite what IT says). It's that they won't patch on the third Thursday of the month. They *might* patch during a maintenance window six weeks from now
- Selfies are strictly frowned upon if you are on or near heavy equipment — of any kind
- If you wear glasses and safety glasses are required, get prescription ones. The site-issued pair will keep you wandering outside the yellow lines
- Check whether corporate, OSHA, or site-specific training is required *before* you show up. The site team will not wait for you to finish it
- There is an IT department. There is no OT department. OT is system engineers, process engineers, maintenance, electricians, and operators. None of them care about firewall rule hygiene
- When conducting a NIST or IEC assessment with site teams, "no answer" to a cyber question is still an answer

- “Five more minutes” on a plant floor means anywhere from 30 minutes to three hours
- If you hear “we’ve always done it this way,” you just found your biggest cybersecurity constraint
- Never assume a cabinet labeled “Network” actually contains networking equipment. Check the supply closet.
- If a control room chair looks empty, don’t sit in it, it probably belongs to someone who stepped away 90 seconds ago
- The loudest room is always where the most important conversation needs to happen
- The oldest Windows machine in the plant will be running the most critical process. Do not point, laugh, act surprised. Note it, shake your head and move on.
- If an operator tells you something is risky, believe them even if it looks fine on paper
- There is always one Workstation no one is allowed to touch, reboot, scan, or even look at too hard – don’t ask.
- Your beautifully written OT cybersecurity policy will be judged entirely on whether it slows production
- If someone says “don’t worry, it’s air-gapped,” it definitely isn’t
- The Wi-Fi password will be written on a Post-it... somewhere... from 2014
- The one time you really need network diagrams is the one time no one can find them
- If a cabinet is labeled “Temporary,” it’s at least 10 years old
- Never ask, “What does this button do?” unless you are absolutely sure you don’t want to find out
- If you arrive in Dockers, a pressed shirt, and polished shoes, the plant will immediately identify you as “corporate” and adjust its answers accordingly
- There is always one engineer who knows how everything works and they’re on vacation
- The VPN you were promised will not work on site
- The jump host will require three passwords, two tokens, and a phone call to someone who left the company in 2019
- If a cable is zip-tied in place, it is mission-critical
- The cleanest room in the plant will house the messiest network
- If someone says, “We can reboot it, but...,” stop talking and listen very carefully

- The historian server is always under someone's desk, in a closet, or in a room labeled "Storage"
- If you plug in a laptop, someone will immediately ask if you just took the plant down
- The OT network rack will be located in the hottest room in the facility
- If a switch has a blinking red light, everyone has learned to ignore it
- Someone will refer to a system by a nickname no one else understands
- If it looks undocumented, it's probably the most important thing on site
- The phrase "we inherited it" explains 80% of the architecture
- You will be asked if you can "just install antivirus" on a PLC
- The most cyber-aware person on site will not have "IT" in their job title

This is obviously not an exhaustive list, but it *is* a list nonetheless. I'm sure many of you could add a few (or a few dozen) more. Please feel free to share your own OT field lessons in the comments.

None of this shows up in NIST, IEC 62443, or your favorite OT maturity model. But all of it shows up in real life. OT cybersecurity isn't just about architectures, assessments, and controls; it's about hard hats, bad Wi-Fi, legacy systems, maintenance windows, and the people who keep critical infrastructure running despite everything we do to their networks — *the OT environment*.

"OT cybersecurity, where theory meets steel-toe reality."