Cyber-Physical Risks: When Data Attacks Meet Physical Safety Meeting Kit

WHAT'S AT STAKE

A cyberattack used to mean stolen passwords or a frozen email inbox, but those days are over. Today, attackers can reach into a factory and crash a robot, override a safety interlock, or shut down the building's heating and cooling. When the digital and physical worlds connect, every weak password becomes a potential injury — and every worker is on the front line.

WHAT'S THE DANGER

Phishing into the Plant

Most cyber-physical attacks start with one clicked link in an ordinary email. From the office network, attackers move laterally into operational systems. Malware that begins on a laptop can reach machine controllers within hours.

Tampered Sensors and Alarms

- Spoofed gas, temperature, or pressure readings
- Suppressed alarms that should have stopped the line
- False alerts that trigger unnecessary evacuations

Unsecured Remote Access and Robots

Vendors and contractors often connect into plant systems through laptops, tablets, and VPNs left open. Forklifts, AGVs, and collaborative robots take their commands over the network and can be redirected at the worst moment. Workers nearby may have no warning before a vehicle changes course.

HOW TO PROTECT YOURSELF

Cyber safety on the shop floor is everyone’s job.

Notice Equipment Acting Strangely

- Unexpected restarts or reboots without explanation
- Set points or timers changing on their own
- Alarms that don’t match the real conditions

Treat Every Login Like a Lock

Use strong, unique passwords on every system, and never share credentials with co-workers — even when it is faster. Enable multi-factor authentication anywhere it is offered, including on plant tablets and HMI panels. A login is the difference between a controlled machine and a compromised one.

Watch for Phishing on Plant Devices

HMI tablets, shared kiosks, and dispatch terminals are prime targets because they sit at the intersection of office and plant. If a message looks off — unexpected sender, urgent language, strange link — don’t click it and don’t dismiss it. Report it so they can warn the rest of the crew.

Lock Down Removable Media

USB sticks and personal devices are one of the most common attack paths into plant networks. Use only company-approved drives on plant systems, and never plug in something you found in the parking lot or got from a vendor without inspection. Treat unknown media the same way you would treat unknown chemicals.

If It Happens: Act Fast

- Stop the machine using the physical e-stop
- Isolate it from the network if you safely can
- Report to IT and supervision immediately
- Don’t try to log back in or ’fix’ it yourself

FINAL WORD

The line between a keyboard and a kill switch is thinner than ever. When data attacks reach the physical world, the people who keep operations safe are the same ones who notice when something’s off. Stay alert online, stay alert on the floor — they’re the same shift now.