THE CHALLENGE

Protecting Against Cyber-Attacks

With rising threats of cyber-attacks and security breaches, there is an urgency within companies to protect their virtual borders by updating Information Technology (IT) and Operation Technology (OT) systems.

Production Impacts and Updates

As society continues to shift to include more machine learning, AI, and data analytics, renovating IT and OT systems has become vital. One of the biggest struggles for manufacturers when updating these systems is minimizing downtime and limiting the negative impact on production.

Reduce Risk: Cybersecurity

Solution

With a cohesive IT/OT team approach, OT managers gained confidence seeing that downtime would be minimized by personalizing communication to each plant involved to ease concerns about downtime, scheduling updates to work within planned maintenance windows, and gaining an overarching knowledge of OT systems to prevent upgrades from negatively effecting line equipment.

POLYTRON

3300 Breckinridge Boulevard, Suite 100, Duluth, GA 30096
Polytron.com | (855) 794-7659

EXECUTIVE SUMMARY

Reduce Cybersecurity Risk within Existing Production Downtime

Client: Globally recognized beverage manufacturer

Challenge:
Update IT and OT systems to protect against cyber-attack, while minimally impacting production.

Solution:
Partner with Polytron for IT and OT networking and implementation

- Personalized communication with plant leaders to ease concerns about downtime
- Schedule updates to work within scheduled maintenance/downtime windows
- Expertise on OT systems to prevent updates from impacting line equipment

Results:
Fully protected OT and IT networks and the peace of mind that comes from having all software updated and secured.

Securing Virtual Borders

The global IT group at a beverage manufacturer was handed a mandate. With news of security breaches and increasing urgency around warnings from Microsoft and the National Institute of Standards and Technology (NIST), the writing was on the wall. The Chief Information Security Officer (CISO) charged the group with securing the company's virtual borders.

The mandate included not just Information Technology but Operational Technology safeguards as well, reflecting the widening awareness that OT is no longer an isolated island of automation. With manufacturers moving toward more machine learning, AI and data analytics, and the proliferating links between people, machines and software driven by the Industry 4.0 transformation, the factory floor is now connected all the way up to the enterprise.

Cyber Risk in Industrial Systems

These increasingly permeable systems meant the manufacturer was vulnerable to intruders gaining access to their systems and creating the alarming risks of:

- Facility shutdown initiated by cyber-attack
- Disabled manufacturing infrastructure
- Worker safety compromised
- Product quality and safety threatened
- Millions of dollars of lost revenue plus expense
- System capabilities held ransom for payment
- Intellectual property theft

Charged with the responsibility of preventing these potential and formidable setbacks, the IT group faced two primary challenges.

Challenge 1: Minimize Downtime Needed to Install Patches System-Wide

The IT group was focused on fulfilling its mandate, but OT production leaders had their own concerns in meeting production goals. Having the IT group send a team to each plant with instructions to shut it down for a day or more, so they could patch computers, would not be positive for morale or revenue.

The IT group would need a plan for minimizing downtime with a persuasive way to communicate the plan to get the production teams on-board.

Challenge 2: Bridging IT and OT

With OT networks being peripheral to IT's responsibilities, and with IT running the project, there was some uncertainty about how to address OT security.

OT networks differ from IT in their connections with equipment ranging from pumps and belts to motors and valves – and with product moving through the system around-the-clock. This creates complications that require IT teams to understand the OT network before beginning work.

Finding the time necessary for this investigation is a tall order for busy IT teams. This can create delays that the IT group feel it can hardly afford in light of the risks the business is currently facing.

Solution: Bring on a Knowledgeable Partner

The IT group turned to Polytron, a system integration partner who had already been instrumental in connecting the company's manufacturing assets. With in-depth knowledge of computers, machines and industrial controllers, setting up IP addresses for industrial networks, and deploying data collection solutions, Polytron's background in cyber protection gave the IT group confidence they would help provide the outcome necessary for success.

Set Meetings at Each Plant to Discuss Project Goals and Tactics

Polytron personalized communication to each of the 68 plants included in the project and scheduled time with personnel to share credentials that would give managers confidence in the process. Presentations detailed the patching approach and demonstrated an understanding of the manufacturing process with the assets that would be affected.

The system integrator was able to show knowledge of the space and ability to adjust to the pressures of production, processes, and environmental and safety concerns. This allowed the production managers to feel more comfortable allowing Polytron to come in and work on their equipment.

Polytron's practice is to align the work with the plant's planned downtime. Polytron meets with plant leaders to review and prioritize the list of assets that need to be patched based on what best fits the plant schedule.

Once managers saw that downtime would be minimized – and that Polytron had ample expertise with plant equipment – they committed to the project and fully supported the work.

Bridging IT and OT

Polytron's experience working with both sides – IT and OT – allowed clearer lines of communication and a smoother implementation:

- Polytron personnel worked with the manufacturer to document security patching protocols already working on the IT side of the business. That knowledge was then used as a model for security sustainability on the OT side. Relying on what is tried and true in IT helped ensure OT patching protocols were effective.

- Knowledge of the processes that OT applications were running, meant Polytron could recover more quickly from any issues that arose once a patch was applied. For the IT team, it would have been more difficult to recover, since they are not as experienced with or likely to have understood the ramifications of applying an OT patch to line equipment.

- By applying Polytron's OT expertise to the update process, the OT system maintained an effective level of interoperability between the OT network and production lines. The manufacturer didn't have to worry about patches creating performance issues.

SECURING PEACE OF MIND

Polytron established a strategic OT and IT team focused on ensuring the customer's goal of cybersecurity and protecting assets from cyber-attacks.

Results: Polytron Approach Secures IT and OT Networks

Polytron established a strategic team focused on ensuring the customer's goal of cybersecurity. This team used cloud collaboration tools to keep team members in constant real time communication across the multiple sites. This enabled:

- **Flexibility in scheduling**: Polytron was able to accommodate plant schedules, servicing 68 plant sites across North America – and adding virtually no downtime.
- **A cohesive team approach:** Manufacturer had confidence that they were getting consistent service out of every member of the Polytron team.
- **Systematic and manageable deployment:** Issues were either anticipated or resolved without compromising the schedule.
- **Centralize reporting function:** Best practices were shared across the deployment team, creating a clearinghouse for team knowledge and learnings that resulted in faster, smoother implementation. These learnings were then passed on to the manufacturer to have on-hand for future support.

As a result, the manufacturer is reaping the benefits of a fully protected system:

- Unauthorized access risk reduced
- Confidence that employee, consumer and public safety is protected
- IT network is protected from OT system breaches – and vice versa
- Breach detection and procedures in place to detect and recover quickly

Find Cybersecurity Peace of Mind

Polytron helps manufacturers protect their IT and OT assets from cyber-attacks.

To learn more about Polytron, visit us online **(www.polytron.com)** or contact us **(www.polytron.com/contact-us)** to talk to a specialist.

3300 Breckinridge Boulevard, Suite 100, Duluth, GA 30096
Polytron.com | (855) 794-7659

POLYTRON