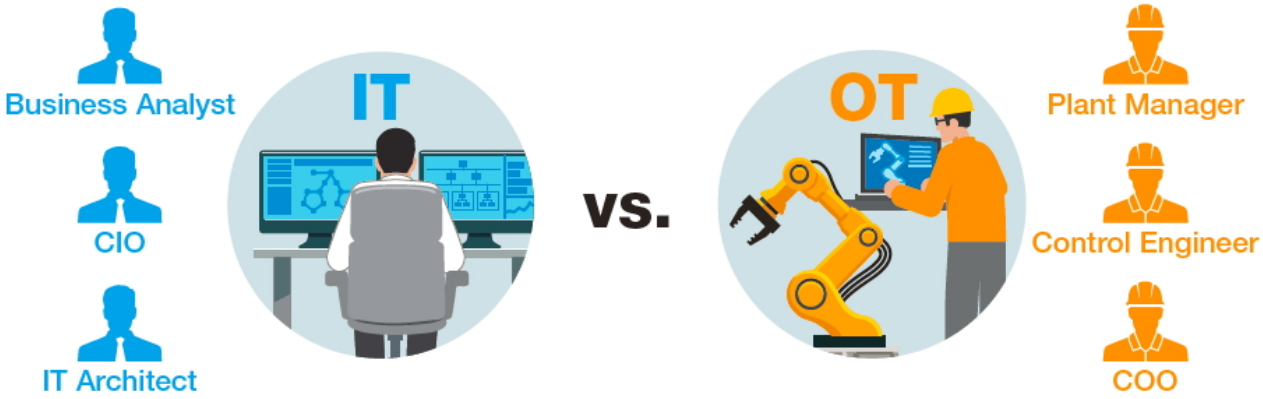
Do You Think Your Industrial Networks Are Secure?

Industrial networks are continuously evolving: new devices are being added to hem constantly, and they are now being connected to the Internet to increase accessibility and visibility. Unfortunately, cybersecurity measure do not always keep pace with this evolution. As cyberthreats become more common, it is important that network owners mitigate these risks. In this aricle, we consider some of the obstacles to deplyoing secure netwroks and the solutions to overcome them



No. 1 Priority	Confidentiality	Availability
Focus	Data integrity is key	Control processes cannot tolerate downtime
Protection Target	Windows computers, servers	Industrial legacy devices, barcode readers
Environmental Conditions	Air-conditioned	Extreme temperatures, vibrations and shocks

In order to realize the benefits of the Industrial INternet of Things (IIoT), industrial netwroks are increasingly being connected to IT networks and the internet. As a result of this changing landscape, industrial cybersecurity has become a major concern for business owners, as there is a real possibility that cyberattacks will significantly impcat business operations and thereofre profits. Despite this, a significant number of peaople are still under the misapprehension that industrial networks are secure because hackers do not understand ICS, PLCs and SCADA systems or believe that their facilities will not be targeted because they are runnning a medium-sized

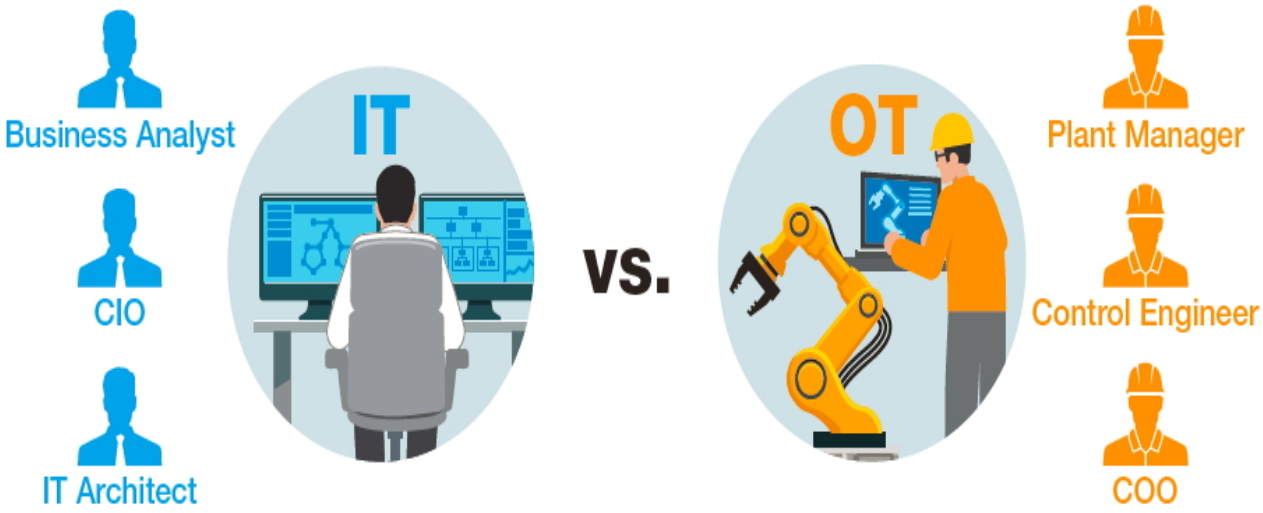
business. However, this is an outdated belief that is no longer true for modern industrial networks

A Wake-Up Call

Since 2010, there have been several sophisitcated cybberattacks, such as Stuxnet and Industroyer that targeted ICS networks. These incidents have served as a stark reminder to owner of critical applications, such as power plants, taht their facilities cannot endure downtime for even a few seconds, as it can have a tremendously negative impact on their business operations. Furthermore research by the U.S. Government organization ICS-CERT has shown that the energy and critical manufacturing industries are the most vulnerable to cyberattacks. This research is finding its way to the top management, where they are beginning to launch company-wide initiaives to enchance their cybersecurity solutions and assign both IT and control engineers to commence research and deploy security measures that will keep their industrial networks secure.

A Slew of Challanges

Several challanges need to be overcome before an effective security policy can be implemented. Many years ago, when IT personnel first defined cybersecurity policies for companies and started deploying firewalls between network zones, control engineers quickly discovered that their critical control commands could not be delivered to their destinations because the firewall blockes network traffic. This issue occurred because IT networks were not built with the correct type of infrastructure to support the industrial cybersecurity measures that are becoming essential for modern-day networks. For communication across industrial networks, the emphasis is very much on high-quality performance and availability, which is in contrast to the seucirty requirements from IT personnel that focus on confidentiality. Typically several industrial protocols are implemented simultaneously in industrial networks making it difficult to meet the minimal latency requriements for machine-to-machine (M2M) communications. Another obstacle that has to be overcome is that the equipment at field sites and the software running on devices are different for Ot and It engineers, making the task of implementing security measures even more frustratin and troublescome. Therefore, it is essential to have a full understanding of industrial cybersecurity requirements in order to build and deploy secure indsutrail networks.



No. 1 Priority	Confidentiality	Availability
Focus	Data integrity is key	Control processes cannot tolerate downtime
Protection Target	Windows computers, servers	Industrial legacy devices, barcode readers
Environmental Conditions	Air-conditioned	Extreme temperatures, vibrations and shocks

Things You Should Know When IMplementing Industrial Cybersecurity

1. Availability Is The Number One Priority

   Control processes cannot expierence downtime. If a control engineer has not experienced a cyberattack, the engineer will ofte be
   hesitant to deploy enhanced industrial cybersecurity feature for their network as it involves addiional time and effort, such as
   developing security patches, updating or adding new networking devices such as firewalls, and rebooting devices. All of these require
   operations to be temporarily stopped, which is somehting that control engineers want to avoid at all cost.

2. Multiple Vulnerabilities in Industrial Network Legacy Devices

   Some industrial networks were built ten or even twenty years ago, and they did not incorporate security feature into their design. A large

number of instudrial networks have not had their security features updated since initial deployment, making them more vulnerable to
cyberthreats than other networks.

3. Industrial Networks Include Different Operating Systems and Devices

   Two main problems are often encountered b organizations when trying to secure industrial networks. The first stems from the fact that
   network operators are unaware of how seucre the devices are when they are about to be deployed on the network. The second is that
   small and medium-sized enterprise (SME) vendors often do not adhere to the best cybersecurity practices, whcih can lead to several
   significant problems. Furthermore, within these organizations there are often mulitple indsutrial networks that use different operating
   systems and devices, making it difficult to take a unified approch to enhancing security

4. Industrial Network Devices Need to Work in Harsh Environments

   Enterprise networks are usually installed in air-conditioned environments: however, industrial networks are often located in harsh
   environments with extreme operating temperatures and vibrations. Thus it is required to have industrial networking devices that can
   endure electircal interferences andd pass vibration or shock tests.

Best Pracitces

There is no method or approch that offers 100% guaranteed protection against cyberattacks. However, several best pracitse can be followed
to significant decrease the chance that your network will be infiltrated by a cyberattack. First make sure your stakeholders are aware of the
risks and provide them with policies, tools, and equipment to help them reduce those risks. Business owners shouldmaake every effort to ensure
that IT personnel fully understand the importance of cybersecurity and how to protect their industrial networks. With the possiblitiy of
cyberthreats happening at any time, it is of paramount importance that ever manufacturer of indudstrial infrastrucutre solutions has a robust
approch to dealing with cyberthreats