BELDEN
SENDING ALL THE RIGHT SIGNALS

White Paper

# Cybersecurity Challenges in the Discrete Manufacturing Environment

## Use cases and solutions from the factory floor

Gary DiFazio, Director of Marketing, Industrial Cybersecurity

## Executive Summary

Like other innovative industrial organizations around the world, many discrete manufacturing facilities such as those in the automotive, aerospace and electronics sectors are strongly benefiting from access to real time production data flowing from the plant floor, strategically applying this intelligence to increase yields, improve quality, reduce waste and more. Further, many such organizations are poised to cull even greater benefits as the Industrial Internet of Things (IIoT) continues to evolve, and new and more powerful technologies and subsequent opportunities emerge.

However, with this increase in connectivity comes a resulting increase in risk. Previously isolated control networks are now potentially accessible to outsiders through increasing numbers of touchpoints, including the global Internet itself. This can open up the production environment not only to the danger of hacking attacks and malware of many kinds, but also equipment failures, human errors, malicious internal events and other cybersecurity related incidents that can significantly impede production and even degrade safety performance on the factory floor. Such issues can be especially impactful in the discrete manufacturing environment, where unscheduled downtime can often be calculated at a cost of hundreds of thousands or even millions of dollars per hour or higher—and excessive waste or product recalls can add even more.

## Table of Contents



Be certain.
Belden.

Fortunately, discrete manufacturers have many options to significantly reduce the potential for cybersecurity issues at their facilities, and minimize the possibility of suffering from the type of events that have had huge negative impact on productivity, quality, safety, profitability and even brand reputation in untold production operations around the world.

This white paper is intended to educate the reader as to the true extent and diversity of cybersecurity threats that are being experienced in today's discrete manufacturing environment, as well as introduce the possibilities that exist to limit exposure. These include practicing good cybersecurity hygiene; optimizing the strategic use of smart cybersecurity configurations in existing network equipment; understanding and initiating cybersecurity best practices such as Tripwire's comprehensive three step "Visibility → Protective Controls → Continuous Monitoring" solution; and deploying innovative third party tools specially designed and proven to optimize cybersecurity performance at your facility.

Indeed, today's operations technology (OT) professionals can readily enjoy the best of both worlds: maintaining and expanding the use of data-driven technologies that enhance production goals, while simultaneously proactively protecting against the vulnerabilities that threaten the integrity of the operation.

## Discrete manufacturing facilities are highly vulnerable to cyber incidents

In a discrete manufacturing facility, operations professionals are charged with meeting challenging objectives and quotas, taking a diversity of raw components from a multitude of sources, transforming them, and getting large quantities of finished product out the door on time and in the highest quality, with minimal variation and optimum on-target specifications. To do so, they rely upon the data that they are receiving from networked components at each step of the production process all the way through final quality control inspection. However, what if any of this data has been compromised?

Further, the typical discrete manufacturing plant floor contains myriad dangers to human life and safety, with light curtains, motion detectors, sensors and other technologies ever vigilant to help ensure that everyone gets home at the end of the day. What if any of these fail safes have been compromised? Can we trust them if they are responding inappropriately to data or responding to false data?

## Greater connectivity = Greater profitability = Greater Risk

These alarming scenarios are not uncommon today, with the increased connectivity found in modern discrete manufacturing automation systems clearly creating a double-edged sword. Indeed, industries as diverse as automotive, aerospace and electronics have been highly successful at utilizing diverse automation equipment including controllers, robots, motors, sensors, HMIs, VFDs, I/O blocks and process-specific machinery of all kinds on the production floor. While these vital components had long operated independently, they now often proactively share streams of real time data, communicating in line to allow finer control of processes for accuracy and quality improvements. In addition, many strategically generate and disseminate data for analysis that can allow further fine tuning of processes as well as archival of production data for overall equipment effectiveness, audit, vendor accountability and other purposes. With the continuing evolution of the IIoT, which promises even greater connectivity, utilization and value for connected devices and shared data, this trend can only accelerate, increasing opportunities for greater yields, faster cycles, reduced waste, improved quality, greater safety of personnel and equipment and more.

However, with these benefits comes a very real threat to the efficacy of the production environment. Isolated for years, these control networks are now, potentially, directly linked to the outside world from other areas of the factory to the IT-led enterprise side of the business to the global Internet itself. This creates a new world of threat vectors, opening up the plant to a host of potential cyber-related incidents, malicious and unintended alike. Many of these threats are new territory for OT personnel, including ransomware, malware, employee cyber sabotage, network failure, user error and more. While these issues have been familiar and costly to the IT side of the organization, their accelerating emergence into the OT side can be even more damaging due to the fact that, in discrete manufacturing industries, producing and shipping product is the lifeblood of the business.

## A diversity of dangers to productivity and process integrity

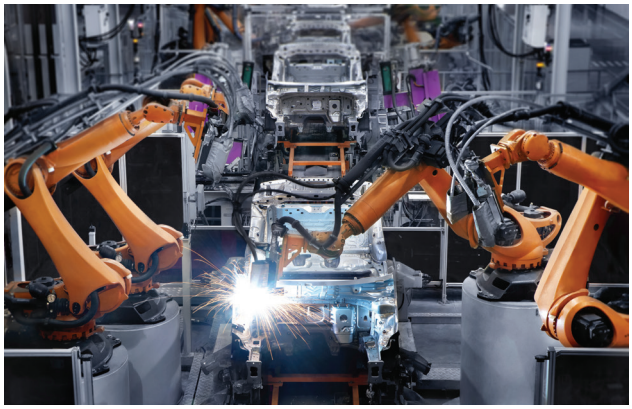
In a discrete manufacturing environment, production lines are often run at maximum capacity, and downtime—with its high costs related to lost yields, increased waste, missed commitments and more—is calculated in many industries at a cost of hundreds of thousands or even millions of dollars per hour or more.

Further, with dozens, hundreds or even thousands of assembly processes that must be in tight specification, there are myriad opportunities for a key subassembly such as a door panel, a motherboard or even a final product to be ruined by a single out-of-spec operation, even something as simple as a bolt or other fastener applied with insufficient torque value. The production instructions for any one of these can be impacted by an inappropriate change in a device configuration or production requirement, whether it comes from an input error, a purposely malicious input change, failing components or other undesired modification to the network. While discrete manufacturers theoretically have the advantage of reworking out-of-spec subassemblies down to component parts, such refabrication is often considered laborious and time-inefficient, with out-of-spec parts often reclassified as scrap, and relegated to the waste stream for costly disposal.

Additionally, for many discrete manufacturers, when out-of-spec products are not caught in time, this can lead to costly product recalls, a degradation in brand reputation or even litigation if there is a product-related injury down the line.

## A wide variety of cyber "culprits," malicious and otherwise

As suggested, cybersecurity incidents are not only those perpetrated by malicious actors, such as hackers and malware developers—although these are more likely to grab the headlines. As incident responders can tell you, a cyber event is considered anything that negatively impacts the network and impedes the ability to view, monitor, control or maintain the availability of an industrial process, including safety systems—whether malicious, accidental or the result of natural wear and tear. This includes hacking attacks such as denial of service, malicious mischief, corporate espionage and more; malware attacks such as ransomware and viruses; innocent human error by otherwise valued employees that can still ruin broad swaths of production; disgruntled employees who can wreak production havoc from inside the network; quietly failing equipment and components that can slow processes or produce operational issues like off-spec conditions—all these, and more, regardless of source or intention.



## Some common cyber incident scenarios and what they look like to discrete manufacturers

As the potential benefits of connectivity increase, and the threat of cyber incidents increases in tandem, it seems timely for today's plant floor network professionals to fully educate themselves on their risks. Operations personnel must begin tapping into available cybersecurity techniques and technologies, many long familiar to IT, in order to protect their OT production environments. Indeed, it may be that the stakes are even higher because threats to the discrete manufacturing environment can strike the integrity of production, the creation of products that are the heart of a manufacturing enterprise as opposed to vital but non-specific administrative functions.

This starts with the basics, which, for many in the OT environment, might not be as second nature as they have become in IT. This includes good cyber hygiene practices such as disabling unused ports, separating the OT and IT environments with firewalls, initiating onboard security settings on all devices so equipped, and, perhaps most importantly, disallowing connectivity between production devices and the global Internet. And, while these are all important, the key to cybersecurity in both IT and OT environments is establishing and continually maintaining optimum insight into network operations minute by minute in real time.

It is important to note that, while cybersecurity in IT can often be viewed as primarily "defensive," proactively driving cybersecurity in the OT environment can actually increase process integrity and improve the ability of personnel to manage processes in increasingly granular ways. Indeed, for controls professionals, cybersecurity is often not just about security; the increased visibility and monitoring capabilities that provide cybersecurity can also be integral to the drive toward process stability and optimizing quality and yields. To better understand how, let's look at a host of common scenarios and how they might manifest in a typical discrete manufacturing production environment. These examples will illustrate how the ability to "see" any of these scenarios as they occur, rather than be blindsided by them, is key to optimizing OT cybersecurity—and OT process integrity as well.

### Unauthorized malicious entry from outside the organization

Hacking is perhaps the most "dramatic" of malicious attacks as it is usually a "hands-on" event. This is opposed to, for example, an actor sending a piece of malware out into the world and being unaware of the locations where it might end up. By contrast, hacks often consist of an actor personally getting into a network, and then spending time in "reconnaissance" trying to see what information and resources might be exploitable. As noted, this is the time that they can be seen and thwarted, if adequate provisions are made in advance to gain the visibility that will immediately reveal their digital footprints and alert network operators to take action.

Hackers take many forms; they could be nation state actors looking to sabotage a strategically important organization, competitors or their agents looking to gain organizational intelligence such as bills of material or production data or plans, or even simply random purveyors of criminal mischief.

Of significant note: the hacking victim might not be the ultimate target. For example, perhaps a hacker enclave wants to ultimately attack a well-protected organization such as a major automotive manufacturer. Small suppliers to that organization are immediately targets because they might have a poorly protected entry into the major company's systems through a billing or ordering link. Further, if the smaller organization has a particular device, such as a specific model of PLC that the larger company also uses, a hacker will often hack that device at a smaller company as a "test bed" to learn about its firmware operation and vulnerabilities before trying to access it and exploit it at a larger company. Another reason for targeting a smaller company is to enslave computer resources, using their captured capacity along with that of others to launch "denial of service" or similar attacks on bigger players.

You should be aware that the IP addresses of many controllers, cameras, machines and other networked devices—perhaps yours—are available right now, on the Internet for anyone who cares to look. Professional research sites such as Shodan provide this information; what might be on the dark web for more illicit purposes is anybody's guess. Anyone can literally use this readily available information to view the inside of factories through the facility's own cameras. It is quite shocking, but enlightening, and effectively illustrates that basic security protections, such as closing ports, installing firewalls and looking for and eliminating these unnecessary and dangerous Internet access points have not been established at these facilities.

### Inside hackers

Even among those OT environments more experienced with cybersecurity protections, much is often done to thwart the outside hacker, but the possibility of malicious actions by an employee—often far easier to implement and more likely to occur—are overlooked and not anticipated or protected against. Building a robust perimeter does little if the attacker is already "inside the gates." Further, employee hackers are already familiar with OT processes and equipment and can be even more damaging than the outside hacker.

Reasons for employee cyber-attacks can run the catalog of lower aspects of human nature—disgruntlement and desire for revenge due to real or imagined company slights; betrayal driven by bribery or monetary gain; becoming reluctantly compromised due to threats or blackmail; cheap thrills; psychosis; boredom; or "just because I can." Goals can be tied in to the above, including sabotaging production by purposely modifying specs or work orders, stealing and providing proprietary information to a third party or selling on the black market, or sabotaging safety systems to cause injury to perceived enemies and the organization.

Another flavor of inside "hack" is that performed by a perpetrator who is spoofing a trusted employee using stolen credentials. For example, even if they are checking the logs, operators may turn a blind eye and not be suspicious of changes made to production specs initiated by the boss, not realizing that the changes were being made by another employee illicitly using his credentials. Even if such changes were flagged, related pieces of suspicious information (Why are these changes being made at 4:00AM? Why is there communication to foreign IP addresses?) are usually not consolidated to create a complete picture unless additional tools are deployed.

Amazingly, people often wonder how someone "knows" their password, the same password written on a sticky note and placed under their engineering workstation keyboard. Common cracking techniques such as password brute forcing, psychographic guesswork (kid's names, birthdays), implanted keystroke emulators, accessing unencrypted password databases, or snooping the credentials off of network traffic are highly effective, but are often not even necessary.

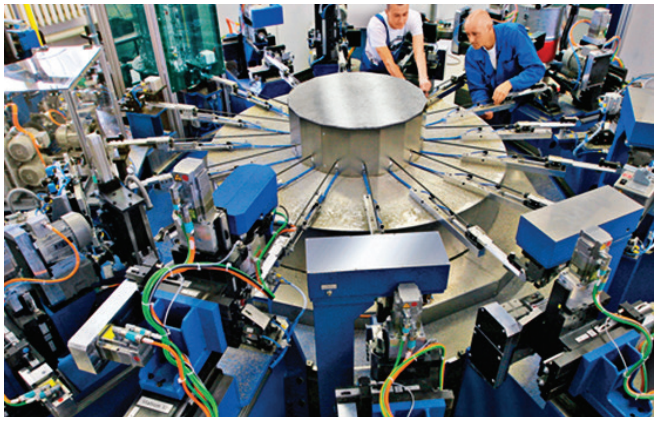
No matter the source, protection against "insider" cyber events starts with visibility. If every time a change is made, an alert is sent to the operator, then every change can be verified to authorized work orders, and unexpected, unauthorized changes, whether with malicious intent or not, can be immediately reverted back to the expected, operational configuration.

### Malware—viruses, trojans, worms and more

Malware describes a number of manmade code-based phenomena that can infect the OT network and wreak havoc on production in a number of ways. The impacts of malware can vary from silly and annoying (announcing "Star Wars Rulez" on every screen) to completely shutting down production indefinitely. Reasons for doing so can include spite, sabotage or even ransom. Ransomware, which first came to light attacking the IT environment, would seem to be an even more effective attack in the OT environment, where downtime is often so much more costly and time sensitive. Unfortunately, with many current ransomware schemes such as WannaCry and (Not)Petya, even paying the ransom does not guarantee that the data or system operation would be returned to user control—and, ironically, it has nothing to do with the relative "honesty" of the perpetrators. Often, authorities immediately shut down the Bitcoin wallet or other electronic payment channel assigned by the criminals, leaving the victims without even this access to a potential "solution." In these cases and others, the only solution is reimaging devices and accepting the process downtime and loss of data.

Malware can include viruses, which are attached to a file and need to be opened by a user in order to spread—hence the constant warnings to never open unfamiliar attachments or files. Worms are more insidious, duplicating themselves and acting behind the scenes, without the need for user "launching." Trojan Horses are perhaps the most insidious of all, often disguising themselves as a useful application and causing damage when opened, locking or deleting files, or opening up a backdoor allowing the malicious actor access to the network.

Malware can be introduced to the OT network in a number of different ways. Infecting user PDF manuals and schematics is a favorite channel, so that when a contractor opens such a file on the plant floor to attend to a device, the malware is launched and spreads throughout the OT network. Malware can enter through an attachment opened in an email—another reason why Internet-connected devices should not be allowed to connect to plant floor devices. Even if correctly unconnected to the outside world, malware can get in through the purposeful or ignorant complicity of inside personnel, through someone connecting an Internet-enabled laptop, or plugging in a found "free flash drive." The latter was reportedly the source of Stuxnet, the malware which infiltrated the supposedly air gapped plants in Iran by presenting false values to PLCs and making centrifuges malfunction. Again, good cybersecurity hygiene best practices would lead one to avoid some of these scenarios through disabling the use of USB ports or denying connection of unauthorized devices to the network.



One highly unexpected source of malware is having it piggyback in on a duly purchased device. Sometimes a device manufacturer's production environment can be infected, and the malware could be riding in the device firmware, infecting the production environment of each purchaser facility it is installed in. Often, visibility saves the day as the proper tools can flag these devices secretly doing things they were not meant to do, such as performing port scans or attempting to phone out.

Of vital note, malware is often not an end in itself, but the first step in a hacking attack, with the malware designed to change configurations, "phone home" captured passwords, disable firewalls or perform some other hidden function to allow a hacker to gain access for their primary purposes. In a proactive, cybersecurity aware operation, it is these changes that are its undoing. Similar to hacking attacks, malware implementation leaves evidence of changes in the network that can be immediately identified and alerts triggered if the proper visibility is put in place.

As noted, many pieces of malware were originally created to compromise the IT environment, and yet are causing "collateral" damage in OT environments due to the fact that there are often IT devices and services—such as Windows, Linux, SQL databases, and web servers—running in plant environments as well. They can be infected independently, and, without proper separations between these environments, infections in the enterprise can spread to the OT production side as well. In recent years, however, more and more malware is being deployed that has been created with OT attacks in mind using protocols specific to the controls environment such as IEC 101, IEC 104 or Step7. One particularly appalling piece of what is suspected to be nation state driven malware—Triton—was written specifically to target Triconex, a market-leading safety instrumented system (SIS) manufactured by Schneider Electric, and seems to have the infliction of injury—rather than monetary gain—as its primary purpose.

### Human error

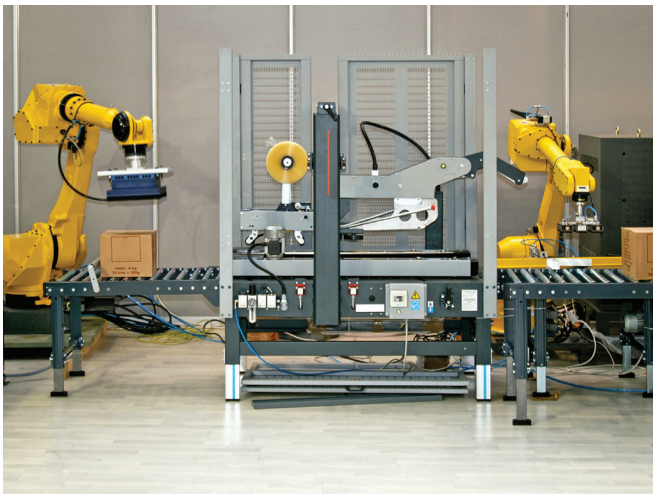
Not all cyber events are malicious—unintentional mistakes play a role in a high percentage of detrimental network impacts in a discrete manufacturing environment. Think how easy it is for a busy operator to type in 60 psi instead of 6.0 psi to a torque value, or accidently set the networked PLC on line 1 with the values for the PLC on line 2, creating huge issues on the line. Consider how often a maintenance worker might weaken firewall rules in order to make a repair or create a testbed—and nobody ever changes them back.

Fortunately no matter what the intention, changes to the network can be flagged using the right monitoring solution—and operators can quickly determine if these changes were appropriate and take immediate action when necessary.

### Failing equipment

Another common, non-malicious scenario that can impact the integrity of the production network stems from an imminent failure in physical infrastructure, such as a cable, a switch or a device like a PLC or HMI. Production instructions can start to become garbled, lost, incomplete, or slowed, causing an impact on quality and yields in the discrete manufacturing environment.

Often, the system might be giving some indication, from measurable changes in response times of robots or conveyors to an increasing amount of cyclic redundancy check (CRC) or other errors or diagnostic information that may be generated in operation logs that are not looked at in timely fashion. Automatically monitoring this diagnostic information and deploying proper alerts is another form of preventative maintenance and is critical to help pinpoint events before they have the potential to impact production process in a negative way.



## Numerous cybersecurity threats - one protective strategy

As suggested by every example above, any change to the network—whether purposeful, accidental or malicious; benign, frivolous or highly detrimental—immediately leaves evidence of its inputting. Problem is, by default, such evidence is often incomplete, isolated and “hidden” somewhere in device logs or not even collected in the first place. If it is not searched out at the exact moments when an incident is occurring, it will continue invisibly and unabated until the damage has been done and the costly impacts on your facility and production are in full swing.

That’s why operators consider implementing specialized solutions that are designed to provide continuous real time visibility into their network operations. Generally speaking, these have a three part strategy—inventorying what you have and what it does, putting in all the protective controls possible, and then monitoring for changes against the baseline, i.e. any abnormal network behavior. In this way you can gain control over everything that you can possibly control.

Although the idea of securing an insecure plant from “square one” can seem daunting, in fact, you can quickly gain a significant amount of protection fairly readily. There are foundational cybersecurity controls that you can begin right now to help reduce operational risk and help you detect and avoid the impacts of all the threats discussed above. These foundational controls are fundamental techniques that provide the most visibility and protection against malicious activity. In fact, they are the basis of most formal industry cybersecurity frameworks, such as IEC 62443, American Water Works Association Process Control Network Guidance, NIST SP–800-82 and NERC CIP. However, whether or not your organization chooses a specific standard to adopt, you can start with fundamental actions such as:

- Asset Inventory and Discovery of Hardware and Software
- Network Segmentation
- Vulnerability Management
- Change Management
- Network Management
- Centralized Log Management

These are all included in the comprehensive three part strategy. The philosophy and driver behind it is, as we often say, “How can you protect something if you don’t know what you have or what it does, or what ‘normal operation’ even looks like?” The strategy remedies that.

## Visibility, Protective Controls and Continuous Monitoring

**Comprehensive cybersecurity in three steps:**

### Step 1. Gain Visibility

Immediately, you can take the guessing game out of the equation. You can know what you have and therefore what you need to secure. When you have holistic visibility into your control network, you can create and maintain asset inventory (vendor, make, model, serial number, firmware version and more), as well as manage communication patterns between devices, see network topology variations, identify rogue assets on the network, outline configuration changes, provide vulnerability context, and other environmental elements—by fact, not guesswork. Visibility capabilities include:

1. Understand and document all network communication between the industrial control network and the corporate enterprise IT network.
2. Understand and document all remote access into the industrial control network, i.e. vendor access with dial-up modems, VPN and cellular connectivity.
3. Create and update asset inventory information for both hardware and software, including vendor, make, model, serial number, firmware version, and versions of installed software.
4. Create and maintain a network topology diagram.
5. Understand what industrial protocols are communicating and between what assets, such as HMIs to PLCs.
6. Understand how assets and devices are configured and if those configurations are changing.
7. Identify what vulnerabilities (weaknesses) are present in the environment.
8. Implement a centralized log management solution.

### Step 2. Implement Protective Controls

Protective controls are controls that help prevent or lessen the impact of cyber events. However, it is often wasteful to implement protective controls blindly. You have to implement the right protective controls for the industrial process you are trying to secure and manage. What may be appropriate for one application may not be appropriate for another. Ensuring network segmentation between the corporate enterprise IT network and the industrial control network is a great first step. This denies all unauthorized network communication through the use of firewalls or access control lists on networking devices.

Another often effective protective control is system/device hardening by which:

1. All services are disabled that are not explicitly needed to run the industrial process, i.e. disable insecure protocols like telnet which does not encrypt traffic;
2. Cybersecurity features such as logging, SSH, SNMPv3 and other features are enabled; and
3. Device/system is checked for proper configurations, i.e. change default passwords and enable password management (length, strength, complexity, etc).

**Overall, fundamental protective controls can include:**

1. Network segmentation
   - a. Between production zones
   - b. Between key mission critical systems/devices such as PLCs and RTUs
2. System and device hardening
   - a. Per an industrial standard or best practice like IEC62443 or NIST SP 800-82
   - b. Include devices like HMIs, PLCs, engineering workstations, historians and industrial networking devices
3. Centralization of all remote access with strong authentication
   - a. Create a separate, protected “DMZ” for all of these connections
   - b. Implement multi-factor authentication for users. Multi-factor is a two-step authentication process having something you know, like a password, and something that you don’t, like a token.

### Step 3. Continuous Monitoring

The third step is to implement continuous monitoring. Just like you have a SCADA to help optimize and control your industrial process, you need a "SCADA"-like cybersecurity solution to help optimize and control visibility to industrial cybersecurity events and ensure the protective controls you have implemented are operating correctly. This is not a one-and-done activity—it needs to be performed continuously, just as threats rear their heads continuously.

Industrial cybersecurity "SCADA" monitoring helps continually answer the "How do I know" questions, such as:

1. How do I know if my device/asset configurations are changing, and do those changes put the device in an insecure state or misalign to my build specification?
2. How do I know if my operational baselines (the configuration of a device or system that is specific to the environment it is running in) are changing?
3. How do I know if one of my devices is at the brink of a failure?
4. How do I know if a rogue asset or protocol is now present on my control network?
5. How do I know if my vulnerability risk profile has changed?

If you are able to answer all of these "How do I know" questions, you will be able to keep your industrial process running without interference from cybersecurity events.

Unfortunately, you do not get to make the decision as to whether you are a target for either an external or internal malicious intent. So know your network. If you don't, someone else with a different motive will. Fortunately, control networks are defendable. Further, as noted, cybersecurity can be an enabler to the key performance indicators of the industrial process: safety, productivity, and quality. The important thing is to take action: Come up with a strategy that is driven by executive management and sets a proactive tone from the very top of the organization.

The time to implement visibility, protective controls and continuous monitoring is now—every minute that you don't is a minute that leaves your network vulnerable to a host of costly threats.

## Conclusion

The production function is the lifeblood of every discrete manufacturing business, with professionals working round the clock to get high quality product out the door on time and within increasingly tightening operations budgets. Advances in operational technologies and factory floor networking are giving OT professionals powerful tools to boost yields and reduce waste, but such tools cannot in good stewardship be implemented without an understanding of the resulting cybersecurity risk they open up. Fortunately, with this awareness—and subsequent action—network, cybersecurity, and automation control professionals in discrete manufacturing and similar operations can work to optimize profitability with the most sophisticated automation solutions driven by the advent of the IIoT, while maintaining optimum, best-in-class cybersecurity levels on the plant floor.

To learn more about Belden's industrial cybersecurity solutions, visit **belden.com/industrial-cybersecurity**



CYBER-SECURITY-DISCRETE-MANUFACTURING_WP00055_INCA_BDC_0919_ENG