# CYBER SECURITY

## AND THE INDUSTRIAL INTERNET OF THINGS

## MAINTAINING DATA SECURITY IN A DIGITAL AGE

Today's distribution and fulfillment operations are reaching the point where they have to take chances to succeed, thrive or even survive — especially those competing in the hyper-competitive, fast-paced world of commerce. As a result, many are making a digital transformation to more automated processes and connected facilities, both made possible by the industrial internet of things (IIoT).

But there are risks in these transformations, whether it's a simple transition to connecting key pieces of automation equipment — in response to labor challenges and the shortage of skilled technicians — or the transition to the fully connected and automated distribution center (DC), complete with IIoT-enabled infrastructures and cloud-based data analytics.

Wherever connectivity and data are exploited, there is risk: a growing potential for cyberattacks. Once a relatively minor risk compared to that faced by other industries, denial of service (DoS) and ransomware attacks are increasing rapidly in the supply chain and distribution space. The potential for security breaches and costly business disruption is forcing operators to implement appropriate cybersecurity protection measures to ensure that sensitive operations and data are protected in the DC.

### A GROWING THREAT IN THE DC

When internet-facing tools enter a business equation, security concerns follow immediately. In fact, they've always gone hand in hand. The first global denial of service (DNS) attack was in 1988 — four years before the introduction of the personal computer (PC) or the invention of the World Wide Web[1]. Since then, the internet has matured and grown far more sophisticated — as have hackers (aka threat agents), who are always trying to stay one step ahead.

Although IIoT is a relatively new subspecies of the internet, it is quickly becoming an emerging target for hackers[2]. A recent study detailed the top 20 cyberattacks against industrial control systems in hopes of better formalizing defense strategies[3], A 2018 survey of 1,300 global manufacturers reported that 66 percent have experienced a cyberattack on their supply chains — and half of those attacks occurred in 2017 alone. Many of these attacks focused on operations rather than data theft and ransom demands:

34 percent saw their operations disrupted and 32 percent experienced downtime, costing an average of $1.1 million per attack[4]. There's simply too much value in the distribution and fulfillment of goods for threat agents to ignore.

The attacks on distribution and fulfillment operations are growing larger and more audacious. A malicious attack on U.S. newspaper distribution centers on December 22, 2018, halted delivery of many papers, including the Los Angeles Times and New York Times[5]. A global ransomware attack crippled supply chain operations worldwide, including FedEx, in April 2017[6]. And the largest cyberattack to date, the NotPetya, shut down shipping operations and data centers in 130 countries on June 27, 2017 — with damages of $10 billion[7].

Given the nature of e-commerce and the dynamics of increasingly connected DC operations, threats to a DC can be very different than the data- and service-focused cyberattacks on the global internet. Across the DC and the IIoT, attacks are often focused on disruptions to connected equipment, instrumentation and algorithm-driven decision making[8].

## WHAT'S AT RISK?

Cybersecurity is crucial everywhere in the digital economy, one that threat agents know well. Any news source can tell you about the size and scope of a cyber event, compromising the security of hundreds of millions of people at a time. According to the World Economic Forum, cyberattacks are ranked among the top three treats in the world; 92 percent of the top U.S. manufacturers cite cybersecurity as a significant concern for their business.

From novice script writers to sophisticated nation states the open internet is fair game to those with nefarious intent. They want money. They want data. They demand ransom. Some simply want economic disruption for the sake of disruption.

A massive cybersecurity industry has grown over the decades in a race with threat agents for the upper hand, each striving to stay one step ahead.

In the meantime, one new corner of the internet is now appearing on threat agents' radar: the supply chain and the growing adoption of the IIoT-based technologies that manage the data that keeps it moving.

These threat agents (or bad actors) seek data, access to money, access to consumer information and access to value. Distribution centers have all of that. And threat agents put it all at risk:

- Costly disruption of fulfillment operations and resulting downtime
- Disclosure of sensitive or regulated data — i.e., operational, business confidential or Personal Identifiable Information (PII)
- Introduction of malware to system and equipment controls
- Inventory theft
- Compromised IIoT sensors and wireless systems[9]

IIoT is still being experimented with and understood by attackers (potentially including some of your own employees, knowingly or unknowingly, in that their PCs and smart devices are connected directly to your IIoT for direct access[10]). The IIoT is different from the internet in some regards: it's more isolated and often linked to edge computing devices and a proprietary data storage cloud. Since the adaptation of the IIoT is far smaller in scope than the global internet and web, there are relatively easier targets for threat agents to pursue. And as you connect your high-value assets to the IIoT, your DC will likely become a more attractive target. That's a problem in itself. Because the DC is only now beginning to face IIoT attacks.

## IS YOUR DC PREPARED?

In most industries, IT teams are used to seeing and fighting different types of cyberattacks over the internet. Cybersecurity has always been at the top of their priority list. With the IIoT, cybersecurity is only now becoming a major issue. That's because, until fairly recently, DC operations had limited connectivity to internal, enterprise computing, and were isolated from the

**A 2018 survey of 1,300 global manufacturers reported that 66 percent have experienced a cyberattack on their supply chains.**

outside world. Now, connected to the internet and the cloud, your IT people may see types of cyberattacks never encountered before.
In many cases, the security systems to protect them from these new types of attacks are simply not in place or IT teams aren't aware of them, because there are very few dedicated IIoT cybersecurity resources to call on. However, the small community of IIoT experts is growing as attacks increase.

architectures, solutions and services to reduce cyber risks for the specific vulnerabilities of distribution centers.

Today, there are only a handful of experts in supply chain cybersecurity. Honeywell Intelligrated has a unique lead in this field: our experts have a long history of reducing cyber risks across control networks in numerous industries, and have enabled the connected DC from the ground up. As a result, they continuously survey and develop innovative industrial cybersecurity technologies to protect your data, assets, operations and people from digital-age threats.

## THE RISE OF SUPPLY CHAIN CYBERSECURITY EXPERTS

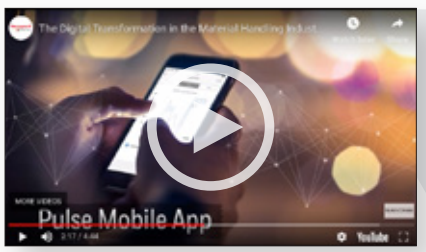
Cybersecurity for the IIoT-connected DC consists of known and unknown risks as the systems become increasingly complex — and important. The new benefits from plant connectivity and data analytics are industry-critical: your future depends on them, and cyber threats must not interfere with digital transformations that are underway. Fortunately, companies driving the connected DC and IIoT solutions, such as Honeywell Intelligrated, are tightly focused on building security

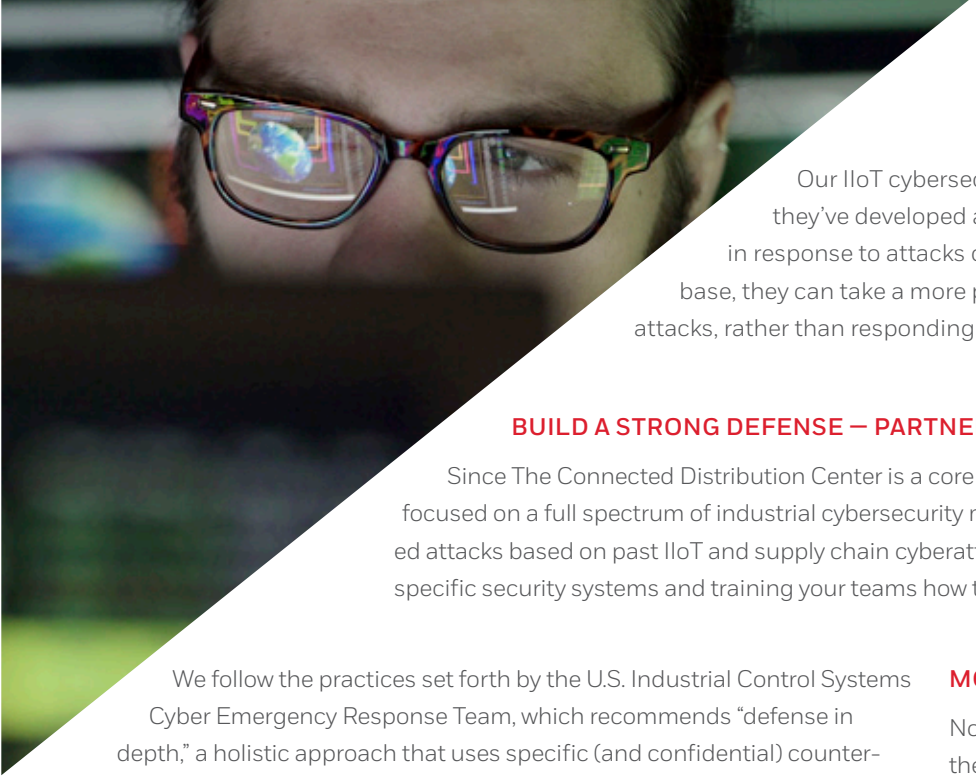
**Threat agents seek data, access to money, access to consumer information and access to value.**

# ON THE MOVE Video Series

*Featuring the OTM Video Series from Honeywell Intelligrated.*

Hear from experts in the field as they discuss issues that impact the industry and how Honeywell Intelligrated is finding solutions to customer challenges.



Our IIoT cybersecurity experts have an experiential advantage: they've developed and implemented internet security measures in response to attacks over the last 40 years. With that knowledge base, they can take a more proactive, predictive approach to potential attacks, rather than responding with protective measures after the fact.

## BUILD A STRONG DEFENSE — PARTNER WITH AN EXPERT

Since The Connected Distribution Center is a core offering for Honeywell Intelligrated, we're focused on a full spectrum of industrial cybersecurity measures, including: testing against simulated attacks based on past IIoT and supply chain cyberattacks and methods; conducting trials of your specific security systems and training your teams how to prevent and respond.

We follow the practices set forth by the U.S. Industrial Control Systems Cyber Emergency Response Team, which recommends "defense in depth," a holistic approach that uses specific (and confidential) countermeasures implemented in layers to defend against security threats and vulnerabilities[11]. This approach is a particular advantage for DCs integrating legacy equipment into newly connected architectures, as security measures can be implemented at each point of connection. And for turnkey installations, the security layers are integrated from the ground up.

When connected to the internet, you want your operations invisible to threat agents, but fully visible to management and IIoT cybersecurity. By partnering with our Managed Security Services, you'll be able to monitor and manage your cybersecurity operations around the clock. Our consultants can enter the process at any time, whether you have no cybersecurity measures of any kind in place up to managing a fully optimized security program.

Threat agents always look for new ways to penetrate your operations, and our cybersecurity services always seek out ways to improve your protections. You should expect the provider of your connected DC systems to adapt with your evolving cybersecurity needs, providing specific expertise on control systems and other issues critical to the DC and the IIoT. For example, almost half of connected distribution and fulfillment companies utilize edge computing in their IIoT infrastructures, where virtual servers provide an interim gateway to the cloud. But this may introduce cybersecurity risks of its own which must be addressed[12].

## MOVE FORWARD WITH SECURITY

No company in any industry has abandoned the internet because of the potential of cyberattacks. It is at the heart of the global economy. Its offshoot, the IIoT, is at the heart of the modern distribution and fulfilment center. DC connectivity enables advanced control of your operations, providing the visibility and insights needed to maximize reliability, utilization and productivity. It is the only way to stay ahead of the intense pace and volume of modern commerce. Thus, concerns about cybersecurity risks should not outweigh your objective to implement the connected technologies that drive efficient DC operations.

Fortunately, IIoT experts at Honeywell Intelligrated are dedicated to addressing these security concerns, building in requisite security measures and providing full-time security services. When it comes to connectivity in the DC and the IIoT, your benefits should far outweigh your concerns.

FOOTNOTES

1. https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history
2. https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-ccinnovation/cybersecurity-industrial-internet-things
3. https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_DEC_17/Waterfall_top-20-attacks-article-d2%20-%20Article_S508NC.pdf
4. https://www.cips.org/en/supply-management/news/2018/july/supply-chain-cyber-attacks-hit-two-thirds-of-companies
5. https://www.reuters.com/article/us-cyber-latimes/cyber-attack-hits-u-s-newspaper-distribution-idUSKCN1OT01O
6. https://www.supplychain247.com/article/massive_cyber_attack_hits_countries_worldwide
7. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world
8. https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/#Cybersecurity_and_data_security
9. https://supplychainbeyond.com/7-supply-chain-security-concerns-to-address-in-2019
10. https://now.avg.com/point-of-entry-how-hackers-could-get-into-your-business
11. https://ics-cert.us-cert.gov/Abstract-Defense-Depth-RP
12. https://ieeexplore.ieee.org/document/8026115