Overcoming the Industrial Cybersecurity Skills Gap Facing the Process Industries
Table of Contents

- Security Skill Set in Age of Digitization: Editor’s Note
- Demand Not Slowing Down
- All Along the Watch Tower: Managed Security Services
- C-Suite Not Confident in Cyber Protection
- New Cybersecurity Center Adds to Global CoE Lineup
- More Automation MeansBoosting Security, Training
- IIoT, Security: Business Enablers
- Honeywell Industrial Cybersecurity
Security Skill Set in Age of Digitization: Editor’s Note

By Gregory Hale

Here we are in the age of digitization where a changing business model provides new revenue and value-producing opportunities, connectivity keeps growing, business benefits are through the roof and fresh cyber attack vectors abound.

With an abundance of data, manufacturers keep learning new ways to hit markets with their products and develop ideas to creatively produce products to save more money and energy while increasing profits. Those are all great things that will keep the company scoring high in a globally competitive market.

The idea that cybersecurity presents an impediment into those rich global plans should be easy enough to fix, right? Just hire a team of security folks, and they will take care of it.

Sorry, there are not enough to go around.

“There are some who just want to purchase a security solution and say, ‘OK, I am done.’ It has to be more than that. Cyber needs to eventually become like safety. A program where everyone clearly understands what their responsibility is and what needs to be done each day to maintain a secure environment.”

— Mark Littlejohn

The numbers back that up: The cybersecurity workforce gap has increased since last year, primarily due to a global surge in hiring demand, according to (ISC)2 Cybersecurity Workforce Study, 2019. Using the workforce estimate of the 11 global economies in the report, there is a global workforce gap of 4.07 million. Also, in the study, 65 percent of organizations represented have a shortage of staff dedicated to cybersecurity. That lack of skilled/experienced cybersecurity personnel is the top concern among survey respondents. In addition, 51 percent of cybersecurity professionals said their organization is at moderate or extreme risk due to cybersecurity staff shortage. In addition, cybersecurity job forecasts have been unable to keep pace with the dramatic rise in cybercrime, which is predicted to cost the world $6 trillion annually by 2021.

This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. Any descriptions of future product direction, intended updates or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release or timing of any such products, updates, features or functions is at our sole discretion.
OT Security Shortage

“Just in cybersecurity in general, there are a massive amount of jobs open and posted. And if you want to make it worse, in the OT environment, multiply that times four in terms of severity with a combination of cyber skills and some knowledge of the process industries,” said Mike Spear, director of global cybersecurity operations, Honeywell Industrial Cybersecurity. “We have done a lot of hiring around the globe, and it is difficult to find them, and once we do, we get them up to speed as quickly as possible.”

Why is there such a big problem?

“In the U.S., we simply don’t have people coming out of school with technical degrees at the rate we used to,” said Mark Littlejohn, global leader, cybersecurity managed services, Honeywell Industrial Cybersecurity. “I think that is an issue. Thirty years ago, unless you were in banking, companies didn’t even have a cyber person. Twenty years ago, companies had one or two cyber jobs available. Today, you have many thousands of openings out there; there is no way to keep up with the rapidly growing demand.”

Does that mean we wing it without a cybersecurity team? Do we spend all our time working on cybersecurity, which takes us away from what we do best? How about outsourcing? Can we hire one company to handle all our sites? Can anybody manage our cybersecurity issues from a remote location?

Security Confidence Low

On top of all the questions, few organizations remain highly confident in their ability to manage the risk of a cyber attack, new research found.

That revelation comes despite companies viewing cybersecurity as a top risk management priority, according to a survey conducted by Marsh and Microsoft.

Cyber risk became even more firmly entrenched as an organizational priority in the past two years, according to the Marsh Microsoft 2019 Global Cyber Risk Perception Survey. Yet at the same time, organizations’ confidence in their ability to manage the risk declined. One good aspect is 79 percent of respondents ranked cyber risk as a top five concern for their organization, up from 62 percent in 2017.
However, companies’ confidence declined in each of three critical areas of cyber resilience. Those saying they had “no confidence” increased: From 9 percent to 18 percent for understanding and assessing cyber risks, from 12 percent to 19 percent for preventing cyber threats, and from 15 percent to 22 percent for responding to and recovering from cyber events.

All those questions and survey data with no real answers. That could add up to a disaster, correct? No, not for the organizations that understand their next move and remain on top of their game.

As the industry is learning, security is not a single project you implement and then move on to something else. Rather, it is an ongoing program that needs understanding and nurturing. What works today, may not work tomorrow and definitely will not work one year from now.

Program, Not Product
“I think customers see it as a product they can buy,” Littlejohn said. “However, there are a few who see it as it should be—as a program. There are some who just want to purchase a security solution and say, ‘OK, I am done.’ It has to be more than that. Cyber needs to eventually become like safety. A program where everyone clearly understands what their responsibility is and what needs to be done each day to maintain a secure environment.”

Manufacturers need to adopt a more comprehensive approach to cyber resilience, which includes the C-Suite and covers the gamut of risk prevention, response and mitigation.

So, creating a program and having everyone understand their role is great, but finding the expertise that can help thwart an intrusion is vital.

Until more cybersecurity experts come on board, outsourcing to experts that have the proper skill set could be the way to go in this age of digitization.

Gregory Hale is Editor/Founder of Industrial Safety and Security Source (ISSSource.com).

Program, Not Product

This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. Any descriptions of future product direction, intended updates or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release or timing of any such products, updates, features or functions is at our sole discretion.
Demand Not Slowing Down

By Gregory Hale

This is the age of cybersecurity awareness with manufacturers understanding there is potential for a problem at quite a few different levels, but with an increase in connectivity and attacks becoming more abundant, demand for security is just not slowing down.

The catch is, though, what is the best way to go for a security solution? Does the end user hire their own security team or do they use managed security services and not have the provider focus on the issue?

In the U.S., the cybersecurity workforce gap is nearly 500,000, according to (ISC)² Cybersecurity Workforce Study, 2019. By combining U.S. cybersecurity workforce estimates and this gap data, it is possible to calculate the cybersecurity workforce needs to grow by 62 percent in order to meet the demands of U.S. businesses today.

“The demand is not slowing down. The more awareness everyone is getting around the world, the more demand there is,” said Mike Spear, director of global cybersecurity operations, Honeywell Industrial Cybersecurity. “We have customers now looking for security resources, whereas in the past, they were looking for chemical engineers or process engineers.

“When it comes to cybersecurity, industrial operators are realizing they just can’t reach the levels of productivity and efficiency they need with their existing resources. They also need new types of analytical tools because their industrial risks have changed, sometimes in ways they don’t yet understand,” Spear said.

Services Model
That is where a managed security service provider could come into play.

“I have quite a number of people around the world that are full time on customer sites because (end users) didn’t want the problems and challenges of hiring one or two of these people with unique skills that are fairly expensive and they don’t fit into the demographics with what they have. So they come to us and partner
with us, and we worry about all of that. That is also why we can leverage the back office to help them to lessen the demand for on-site level people. They can do some stuff from the back office with multiple resources that are skilled that will keep the customer from hiring one of each of these: For example, a domain expert, a firewall expert, a SIEM expert. Those are three different resources and three different people. We have customers trying to do it themselves, but it is so far away from their core business, they are looking for partners.”

“We recognize the fact that customers have a very hard time, even if they can get approval to hire a security person, trying to find one can be very difficult,” said Mark Littlejohn, global leader, cybersecurity managed services, Honeywell Industrial Cybersecurity. “We can bring in expert cyber resources that know their environment.”

The issue of bringing in qualified personnel to handle security issues has gone all the way up to the White House.

**Government Weighs In**
There needs to be “immediate and sustained improvements” in the country’s cybersecurity workforce, according to a United States government report.

The report, called for by the “2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” includes findings and recommendations that address public- and private-sector needs.

“Ensuring the security of our interconnected global networks is one of the defining challenges of our era,” said Secretary of Commerce, Wilbur Ross. “A skilled cybersecurity workforce is necessary for our nation so that we can fully reap the benefits of the 21st-century digital economy.”

By 2022, the global cybersecurity workforce shortage has been projected to reach upwards of 1.8 million unfilled positions, according to a Frost & Sullivan report.

In addition, according to CyberSeek, an initiative funded by the National Initiative for Cybersecurity Education (NICE), the United States faced a shortfall of almost 314,000 cybersecurity professionals as of January 2019. To put this in context, the country’s total employed cybersecurity workforce is 716,000.

Executive Order 13800 directed the secretaries of commerce and homeland security to “assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future,

---

“This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. Any descriptions of future product direction, intended updates or new or improved features or functions are intended for informational purposes only and are not binding commitments on us or the sale, development, release or timing of any such products, updates, features or functions is at our sole discretion.”

---

“Security is not one single thing, rather, it is a collection of different things depending on your risk tolerance and risk appetite.”

— Mike Spear

---

This document is sponsored by Honeywell.
Security Skill Set in the Age of Digitization: Editor’s Note
Demand Not Slowing Down
Along the Watch Tower: Managed Security Services
C-Suite Not Confident in Cyber Protection
New Cybersecurity Center Adds to Global CoE Lineup
More Automation Means Boosting Security, Training
IIoT, Security: Business Enablers
Honeywell Industrial Cybersecurity

including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education.”

The U.S. is not alone in focusing on improving cyber improvements. The United Arab Emirates drafted cybersecurity guidelines, while Singapore is focusing on increased cyber training, and the Netherlands created a new cybersecurity national agenda as did Denmark and Luxembourg.

Start with Basics
The assessment found significant opportunities to expand the pool of cybersecurity candidates by retraining those employed in non-cybersecurity fields and by increasing the participation of women, minorities and veterans, as well as students in primary through secondary school. It also found an apparent shortage of knowledgeable and skilled cybersecurity teachers at the primary and secondary levels.

“We are starting to see some of the universities around the world where they are starting to create curriculums around industrial cybersecurity and cybersecurity in general, where before they had generic computer science degrees,” Spear said.

“Security is not one single thing, rather, it is a collection of different things depending on your risk tolerance and risk appetite,” Spear said. “Users struggle with doing something, but they are not quite sure what that something is. We tell them there is a base level tier one security controls that every plant, regardless of risk tolerance, has to do. Things like patching, antivirus, segmentation, firewall rules. There is a core base foundation of controls and policies you need to do. Beyond that, there are specifics of the industries and regulatory issues.”

The demand continues.

Honeywell Forge Software
New multi-site solution to proactively measure, monitor and manage the cybersecurity risks that matter most.

Know more
All Along the Watch Tower: Managed Security Services

By Gregory Hale

No one can deny there is a cyber skills shortage throughout the manufacturing automation industry. With the potential for attacks becoming stronger and sophistication levels becoming more intense, manufacturers need to find an answer.

That is where managed security services come into play.

“Instead of hiring people, which is difficult to do, they simply bring us in,” said Mark Littlejohn, global leader, cybersecurity managed services, Honeywell Industrial Cybersecurity.

Through managed security services, Littlejohn said, a provider is able to monitor systems, patch systems, offer remote access and provide multi-vendor security, encrypted remote access and support, patch and anti-virus automation, security and performance monitoring, security device management and threat detection and vulnerability identification.

That may end up being a more viable solution since there has been a continuing increase in the amount of organizations suffering from incidents and the hike in the level of sophistication of attacks.

In the past, the Department of Homeland Security’s ICS-CERT continued to see a rise in attacks year over year. That only makes sense, as attackers stop at nothing in their efforts to find weaknesses throughout critical infrastructure environments.

Big or small, organizations continue to be the object of attacks, whether intentional or unintentional. The WannaCry, NotPetya and Triton attacks over the past few years have shown how attackers can gain access to networks and cause huge issues.

The following are weaknesses security researchers say are major issues:

1. **Boundary Protection**, which included undetected, unauthorized activity in critical systems and weaker boundaries between ICS and enterprise networks.
2. **Identification and Authentication (Organizational Users)**, which included a lack of accountability and traceability for user actions if an account is compromised and an increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access.

This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. Any descriptions of future product direction, intended updates or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release or timing of any such products, updates, features or functions is at our sole discretion.
All Along the Watch Tower: Managed Security Services (cont.)

3. **Allocation of Resources**, which included no backup or alternate personnel to fill a position if the primary is unable to work and a loss of critical knowledge of control systems.

4. **Physical Access Control**, including unauthorized physical access to field equipment and locations, which provides increased opportunity to:
   - Maliciously modify, delete, or copy device programs and firmware
   - Access the ICS network
   - Steal or vandalize cyber assets
   - Add rogue devices to capture and retransmit network traffic

5. **Account Management**, which included compromised unsecured password communications and password compromise, which could allow trusted unauthorized access to systems.

6. **Least Functionality**, which included increased vectors for malicious party access to critical systems and rogue internal access established.

**Solution to Issues**

Sometimes there is a good technology solution to help take care of the people and process issue, which makes it one less thing for the manufacturer to worry about.

The goal is to make it easier to bring experts to problems, making it easier, cheaper, and more effective to get an expert in the room.

“End users need to understand their pain points,” said Seth Carpenter, software architect, Honeywell Industrial Cybersecurity. “They know they need to do something. It is rare we have a customer in denial. I don’t think there is anyone that would deny the problem.”

In many cases, it can turn into a productivity issue.

“You want to make your people more effective instead of sending Steve the Intern around to find things,” Carpenter said.

Managed services help manufacturers lessen the demand to have people on site.
Skilled Workers
Workers back at the managed services site have multiple skilled resources at their fingertips, which can keep end users from hiring one of each of these. This way, they can reach out to a person with domain experience, or a firewall guy or a SIEM person. Those are three different resources the end user would not need to hire on site.

“We recognize the fact that end users have a very hard time; even if they can get approval to hire a security person, trying to find one can be very difficult,” Littlejohn said. “We can bring in expert cyber resources that know (the end user’s) environment. We can help them implement new solutions, harden their systems, fix configuration issues, patch their systems, manage their firewalls, and monitor things 24/7.”

It used to be at the point where end users did not worry about security because there was a lack of understanding about the issue, but today that is not the case.

“Every customer we talk to wants to address their security issues,” Littlejohn said. “Ten years ago, customers would say we have firewalls or we are air gapped so we don’t have to worry about security. Now people recognize there is a threat. There are things they have to do to make sure their systems are secure. At the end of the day, it is about availability. Several have had malware infect their systems and cause a loss of view or a loss of control, and they recognize by not plugging these holes they are vulnerable to avoidable downtime. Security doesn’t necessarily mean a breach; it could also be an outage, and an outage is unacceptable. They all recognize this, and they are addressing it one way or the other.”
C-Suite Not Confident in Cyber Protection

In this day and age of security awareness, but not total security program adoption, it may not be a big surprise to find few organizations are highly confident in their ability to manage the risk of a cyber attack, research found.

That revelation comes despite companies viewing cybersecurity as a top risk management priority, according to a survey conducted by Marsh and Microsoft.

In a global poll of senior executives, 79 percent of respondents ranked cyber risk as a top five concern for their organization, up from 62 percent in 2017, according to the Marsh Microsoft 2019 Global Cyber Risk Perception Survey.

The survey found cyber attacks/cyber threats was the top business threat at 22 percent, followed by economic uncertainty at 15 percent and brand/reputation damage at 11 percent.

Unplanned Downtime

“Three years ago, I was sitting in a committee meeting and the question was asked what is your worst cybersecurity fear and one person said getting ransomware on my control system,” said Mark Littlejohn, global leader, cybersecurity managed services, Honeywell Industrial Cybersecurity. “That is not a typical security breach. That is something that takes control and shuts the system down. Customers recognize their worst-case security scenario is things going down, things not operating correctly, loss of view, loss of control. Every meeting we have with our customer advisory board, that is what they are talking about. They are not talking about loss of data, the conversation has changed from I am going to make a headline because of a security breach to I have got to keep my stuff operating, and security is important to that.”

Despite this heightened awareness and rising concern, the level of confidence in the ability to understand, assess and measure cyber threats dropped to 23 percent in 2019 from 29 percent the previous year, according to the Marsh Microsoft study. The same was true in respondents’ confidence to be able to mitigate and prevent cyber attacks dropped to 18 percent.
from 20 percent, as did their ability to manage and respond to cyber attacks dropped to 18 percent from 20 percent.

“Cyber risk is an escalating management priority as the use of technology in business increases and the threat environment gets more complex,” said John Drzik, president Global Risk and Digital, Marsh. “It’s time for organizations to adopt a more comprehensive approach to cyber resilience, which engages the full executive team and spans risk prevention, response, mitigation and transfer.”

In a world of interdependent digital supply chains, cyber risk is an issue. Along those lines, 2-in-5 Marsh Microsoft survey respondents said they thought their supply chain posed a risk to their organization. At the same time, respondents were more than twice as likely to say they faced risk from third-party partners as they were to say that their organization posed a risk to those in their supply chains.

Owning Security
Responsibility for cyber risk management continues to lie primarily with the IT department, with inconsistent involvement of other stakeholders across the enterprise. According to the survey, of the three functions responsible for cybersecurity, 88 percent of respondents pointed to IT as a primary owner and decision-maker for cyber risk management, compared to 65 percent who cited the president/chief executive or the board of directors, and 49 percent who cited the risk management function.

“While technology is the foundation of any good cybersecurity strategy, companies can benefit from investing in non-technology solutions like risk management as part of a holistic approach,” said Matt Penarczyk, vice president and deputy general counsel, Microsoft. “Through advanced technology, tools and training, for example, companies can better protect the data in their networks and be ready for the business interruptions and reputational risks associated with cyber attacks.”

Honeywell Forge Software
Implement connected operations while minimizing cybersecurity vulnerabilities with Honeywell’s Honeywell Forge Software.

Know more
Honeywell opened its first industrial cybersecurity center of excellence (CoE) in Singapore to join a growing roster of centers around the globe to help provide deeper learning on OT security issues.

Developed with the support of the Singapore Economic Development Board (EDB), the center was designed to help the region’s industrial manufacturers defend against evolving cybersecurity threats.

“The only way manufacturers can reap the benefits of digital transformation, such as increased uptime and reduced maintenance, is if their industrial environments are cyber secure,” said Jeff Zindel, vice president and general manager Honeywell Industrial Cybersecurity. “The center’s state-of-the-art capabilities and managed security services improve cybersecurity protection, detection, management and response for customers, which are key enablers for successful digital transformation in the industrial sector.”

The cybersecurity center will be used to conduct proprietary research, develop new security technologies, provide hands-on training and certifications, and test and validate actual solutions deployed at customer sites.

The cyber center is in Singapore’s Changi Business Park and is the third Honeywell facility of its kind in the world. Earlier this year, the company opened a new center in Dubai that serves end users in the Middle East and Europe. Honeywell’s original cybersecurity center is in Atlanta, Georgia, USA.

In addition to serving as a research and development lab, the Singapore center also provides managed security services to help users reduce the risk of security breaches and proactively improve their security posture. Services include continuous security and performance monitoring and alerting, threat detection and risk management, security device management, and incident response with 24-hour expert support 365 days a year.

“Cybersecurity is vital not just for the technology industry, but also our industrial sector and critical infrastructure, which are being increasingly digitalized,”
New Cybersecurity Center Adds to Global CoE Lineup (cont.)

said Gian Yi-Hsen, executive director, cities, infrastructure and industrial solutions, EDB.

The centers of excellence work well with Honeywell customers, but also provide a solid source of cybersecurity training.

“In our Atlanta center of excellence, we have built out the capabilities for training. That means not only training customers but also bringing in less experienced people so we can have focused training and get them up to speed,” said Mike Spear, global operations director for Industrial Cybersecurity at Honeywell. “In the U.S. alone, there are 250,000 jobs open, and we are not going to fill them tomorrow.”
More Automation Means Boosting Security, Training

As manufacturers rely more on automation, they will need more robust tools to be able to communicate with the disparate systems and protocols throughout the manufacturing enterprise.

To automate to a higher level and get the most out of any system, it becomes more important to have software—and connections—that allow for greater communication.

By taking a more proactive approach to predictive analytics, predictive maintenance, and preventative maintenance rather than being purely reactive, automation allows a manufacturer the visibility to become more productive and more informed about a dynamic, evolving manufacturing enterprise.

Allowing for a manufacturer to go ahead and communicate from different software and hardware platforms—and to be able to connect them—is becoming bigger and bigger.

That means systems and tools will need to be more intelligent. It also means technology will take a higher share of the work load so the new generation coming in dealing with the new manufacturing paradigm will feel more at ease with proper training.

But building in greater automation and connectivity creates potential for a cybersecurity incident.

"I can remember a time several years ago when a customer would say, there is no way you are going to bring open systems in my environment," said Mike Spear, director of global cybersecurity operations, Honeywell Industrial Cybersecurity. "Now, fast forward five years and everything is Windows-based. In the past, there was no way in the world you would virtualize an environment at the process level, and now everything is virtualized. For remote access, we started seeing that 12 years ago, and eight years ago acceptance really started. The use case was just so compelling and once you started to address the security levels, it is now almost a given. Now we are talking about the cloud. At each of these levels, security is becoming a bigger and bigger component. It has a fantastic use case and business case, but you..."
More Automation Means Boosting Security, Training (cont.)

have to have the security addressed. I am finding the process industries are slow adapters, but they are now getting into the middle of the pack.”

Access at Any Time
Security has come to the forefront of everybody’s mind because businesses are demanding access to data at anytime from anywhere. Anything that can have an influence on the control system, an end user needs to monitor. That changing level of visibility and access also means there has been a shift on control system exposure.

There are automated facilities connected to the Internet and not very well protected and attackers are licking their chops poised to attack. That is where the industry is trying to figure out a solution on how to protect itself without losing out on its investment in automation and its rich level of new data.

Automation and modernization, which industry analysts say could be a $65 billion market, is more than just updating a system, it is all about taking ancient legacy technology installed before cybersecurity was ever a thought and understanding what that system should look like today and how it will look in five years.

Understanding the landscape and looking to the future, with any new automation project, security and awareness through training is a vital part of any installation.

Cybersecurity is fundamental and it is not something that can be fixed in a patchwork kind of way; it is a sustaining application, not a one-time thing. No one can buy cybersecurity, install it, and forget about it. It needs to evolve because bad guys create new techniques and methods and come out with inventive ways to attack.

Awareness Means Training
That means automation and cybersecurity are all about change management and having the three-legged security stool of people, process and technology within the organization clicking on all six cylinders.

Training and creating a security culture are becoming more paramount for manufacturers.

“I think we see challenges on all three legs, especially on the environment we work in,” said Mark Littlejohn, global leader, cybersecurity managed services, Honeywell Industrial Cybersecurity. “There are challenges out there. There are very few customers out there with maturity to the point where they have got all the technology in place, all the processes in place and the people. We see the people issues, and that is more apparent than the others.”

This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Honeywell and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Honeywell. Any descriptions of future product direction, intended updates or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release or timing of any such products, updates, features or functions is at our sole discretion.
More Automation Means Boosting Security, Training (cont.)

A solid security program can help offset an assault on a control network.

“The people part is not just the skilled people. It is everybody in the plant,” Spear said. “Are they all aware of security? In safety, if anybody in the plant sees someone without a hard hat or a broken ladder, they know what to do. On a flip side, if they see a USB stick on the floor that has a label marked ‘salary levels’ on it, I am not sure they know what to do. They might just plug it in. They don’t know who to take it to. The whole awareness is not there.”

Adding greater automation capabilities means more than just adding technology. It means boosting training and awareness of security.

“They all have to evolve at the same time,” Spear said.
IloT, Security: Business Enablers

By Gregory Hale

With the industry headed into digital transformation via smart manufacturing and Industry 4.0 and the Industrial Internet of Things (IloT), company leaders look at these initiatives as opportunities they need to jump on—and fast.

They truly can gain a competitive advantage through new service-enabled business models, disruptive new products, a more agile supply chain, and efficient operations.

The catch is, though, systems built to be the backbone of the manufacturing enterprise, the control systems, were not built with security in mind.

But on the other hand, a more secure system can mean a hike in productivity, which means greater profitability.

A survey released by Honeywell and conducted by LNS Research entitled, “Putting Industrial Cybersecurity at the Top of the CEO Agenda,” polled 130 strategic decision makers from industrial companies about their use of industrial cybersecurity technologies and practices.

Moving Forward with Security

Slow or low adoption of security could mean either manufacturers will move forward with the digital transformation and remain insecure, or they will end up delayed in their movement forward, thus losing valuable time and potential revenues, until they adopt a security program.

Either way, it appears companies at the vanguard of employing security already have a leg up on any potential competitors. It can also mean more companies are still at the beginning of creating a security program.

“I think everyone knows they have a problem now, but they are not quite sure where to start,” said Seth Carpenter, software architect, Honeywell Industrial Cybersecurity. “There is a long way to go. Awareness is a good first step. We can’t do anything unless there is an agreement that something needs to be done. The next step is putting funding behind these programs. Sometimes it is not throwing money at it, it can really be building up the culture in the organization where

- Security Skill Set in the Age of Digitization: Editor’s Note
- Demand Not Slowing Down
- Along the Watch Tower: Managed Security Services
- C-Suite Not Confident in Cyber Protection
- New Cybersecurity Center Adds to Global CoE Lineup
- More Automation Means Boosting Security, Training
- IloT, Security: Business Enablers
- Honeywell Industrial Cybersecurity
Among the findings of the survey were:

- More than half of respondents reported working in an industrial facility that already has had a cybersecurity breach.
- 45 percent of the responding companies still do not have an accountable enterprise leader for cybersecurity.
- 37 percent are monitoring for suspicious behavior.
- Although companies are conducting regular risk assessments, 20 percent are not doing them at all.

“One of the things I found interesting was when they were asked if they had a breach at their plant, most people normally didn’t want to talk about it, but here quite a few people admitted they had a breach,” Carpenter said.

The survey found there has been low adoption of cybersecurity measures, however, awareness is through the roof, and the question remains about when manufacturers will establish a timetable for adopting a security program.

“It is a combination of things,” Carpenter said. “We know we should brush our teeth and take our vitamins, but sometimes you just say, ‘I will go to sleep right now.’ It is hard without that driving factor or a really good business case behind it. We are at a point where there is a lot of awareness of what is happening. We see attacks in every industry like healthcare, banking, financial institutions, the awareness is there. I think that is the first part, where people recognize something needs to be done. They might not know where to start. So, they say we need to do something about it, but that can be daunting. It is like eating the elephant, you have got to figure out the little bite you can take on this.”

Assessment Step

One of the first steps a manufacturer can take is conducting an assessment to see where you stand.

“There are really good cybersecurity maturity models...
users can map their processes to so they can get started,” Carpenter said. “Sometimes the hardest part is taking the first step and think here is what we are going to get and here is where we want to be and putting together that plan.”

Traditionally, security has been seen as a cost center, but in reality, it can end up viewed as a business enabler that keeps systems up and running by eliminating unplanned downtime.

“That is one of the trickiest parts of security,” Carpenter said. “When I invest in a manufacturing line, I see I am producing 20 percent more product. That is tangible and I can put a dollar value on that. If I spend the same amount of money on a cybersecurity program, how do I measure success? How do I show my boss and my boss’ boss, ‘hey, we did a really good job here.’ We know this is complicated, we are talking systems that have been up and running for years and years, let’s face it, if it is not broken, don’t fix it. So, getting visibility into the assets can be difficult, but in the end, you have to know what normal looks like.”

Any discussion about increasing uptime and operational stability is something that resonates with business leaders very quickly. If a plant is down for one week because of a cyber-related incident, it is easy to understand the cost.

Indeed, when talking about security, users need to consider metrics such as improving the efficiency of operations, reduction in time to detect incidents and return on prevention.

Part of the issue is making sure users understand they are not just looking at the risk model and figuring out the probability. With cybersecurity, as numerous research reports have pointed out, it is not a matter of if, but a matter of when. The challenge becomes at some point, when are you going to have an incident and how much is it going to cost you?

**Best Practices**

The report issued some recommendations:

1. Use an operational excellence model of people, process, and technology capabilities to enable
1. Security Skill Set in the Age of Digitization: Editor’s Note
2. Demand Not Slowing Down
3. Along the Watch Tower: Managed Security Services
4. C-Suite Not Confident in Cyber Protection
5. New Cybersecurity Center Adds to Global CoE Lineup
7. IIoT, Security: Business Enablers
8. Honeywell Industrial Cybersecurity

2. Focus on best practices adoption. Start with the basics like firewalls and access controls; over time move to more advanced topics like network architecture, risk management, and activity monitoring. Build a roadmap based on increasing people and process maturity that considers risk and equates safety with security. If people capabilities are limited to start, consider augmenting with external professional services that have IT and OT experience.

3. Focus on empowering leaders and building an organizational structure that breaks down the silos between IT and OT. A common approach across these disciplines is critical for success in industrial cybersecurity and it can only be done by investing time and energy in the soft skills of change management.

“I think there needs to be a mindset shift to see this isn’t a problem where we are dumping our money into it because we have to,” Carpenter said, “instead this is helping us maintain our machines and giving us the uptime numbers we need.”

Click here to register to download the Honeywell report conducted by LNS Research.

What Are the Financial Savings from a Refinery Cybersecurity Program? Download your copy to Know more
Honeywell Industrial Cybersecurity

Honeywell is the leading provider of cybersecurity solutions that helps protect industrial assets, operations and people from digital-age threats.

With more than 15 years of cybersecurity expertise and more than 50 years of industrial domain expertise, Honeywell combines proven cybersecurity technology and industrial know-how to maximize productivity, reliability and safety. We provide innovative cybersecurity software, services and solutions to industrial and critical infrastructure customers around the world that helps protect industrial assets, operations and people. Our complete portfolio leverages Honeywell’s industry-leading expertise and experience in process control and cybersecurity. Years of providing industrial cybersecurity solutions have resulted in proprietary methodologies, best practices, and a comprehensive understanding of cybersecurity requirements for the process control domain.

We’re foremost in the automation industry in our investment in cybersecurity technology for process control systems, including our state-of-the-art Cybersecurity Centers of Excellence around the globe.

To learn more about Honeywell Industrial Cybersecurity, visit www.becybersecure.com.
Honeywell

To learn more about Honeywell Industrial Cybersecurity, visit www.becybersecure.com.