PACKAGING WORLD®

packworld.com

PLANT FLOOR CYBER SECURITY– Two part series

Part One pgs. 2-6: On your agenda?

Part Two pgs. 7-10: Turning discussion into action

PMMI MEDIA GROUP

Reprinted from *Packaging World* July and August 2015

Part One, reprinted from the July 2015 issue of *Packaging World*

Plant floor cyber security—is it on your agenda?

What is the cyber landscape for Consumer Packaged Goods companies? How great is the risk of getting hacked? Maybe it's time we took a closer look at cyber security.

Keith Campbell, Contributing Editor

Plant floor cyber security is among today's most serious threats facing our individual manufacturing enterprises and our collective national security. Yet the potential of the Internet to radically and constructively transform our businesses is undeniable. The key will be to strike appropriate balances between security and productivity and between risk and revenue streams. The decisions to be made in this regard are C-suite decisions, to be overseen by boards of directors. As engineers and managers, if we are to be recognized in the C-suite of our company, it had best be as part of the solution and not as the cause of the problem. We cannot allow the hype over the industrial Internet of things (IIoT) to lure us into positions of vulnerability. We must be certain that plant floor cyber security has been adequately addressed, before we do anything that may expose our operations.

This two-part article is not intended as a how-to guide, but rather a why-should guide. This month we will dig deeply into why should a reader of *Packaging World*—whether a packager, an equipment supplier,

Plant floor cyber security

or a material supplier—be actively engaged in cyber security discussions at the highest levels of their company? Why should educators, professional organizations, lobbyists and others who work with these industries be part of the discussion? Next month we will suggest some of the areas that should be considered, some strategies that could be employed, and some resources that can be drawn upon in the process of turning discussions into action.

The cyber landscape for CPGs

Consumer Packaged Goods manufacturers (CPGs) in particular, and hybrid manufacturers in general, are being largely overlooked in cyber security oversight. Major sections of the process industries, as part of our critical energy infrastructure, are required by law to address cyber security. Discrete manufacturers, especially those involved in manufacturing parts for small arms and major weapons systems, are being coached and prodded by the Departments of Defense and Homeland Security to close cyber security loop holes. The 19th annual ARC Industry Forum held this past February included a day of standing-room-only workshops on cyber security conducted by The Automation Federation and Department of Homeland Security (DHS), and the topic was on the agenda throughout the remaining 2½ day conference with speakers from DHS, the FBI, NIST, Chevron, Shell, MIT, 3M, major utility providers, and a variety of technology providers. But scanning the attendee list shows that the conference was significantly under-represented by packagers, small process operators, and process and packaging machinery builders.

Hybrid manufacturers and their packaging and processing equipment suppliers are being left largely to their own devices to recognize and address the plant floor cyber threat. My research suggests that only the largest among them are actually taking adequate steps to address the problem. Best practices would include those whose boards have directed steps be taken to secure the shop floor, provided funding to do so, and set their internal audit departments about the task of testing and reporting on progress. To execute these directives, one CPG company has established an engineering function with the term "security" in its charter and name, and one has been working jointly with the nuclear industry to develop world-class protections and processes.

At PACK EXPO Las Vegas 2003, the OMAC Packaging Workgroup sponsored a paper on the topic of plant floor network security. That paper presented one leading CPG company's plan for securing its plant control networks while allowing for remote access by employees and vendors. Twelve years later, most manufacturers have yet to achieve the levels of security described at that time. But given today's threats, those levels are no longer adequate. The fundamental difference between then and now is that 10 years ago, we were still focusing on protecting our shop floors from the mistakes or oversights of our own well-meaning but perhaps uninformed employees and trusted vendors. We did not wish to risk the safety of our products, machines or workforce to some accidental intrusion across our networks that might cause our systems to temporarily go out of control. Fast forward now past the Stuxnet, Target, and Home Depot breaches; the state actors who have breached Sony and the White House; those who use cyber intrusion as a means of terrorism or war; and the 3 billion Internet users around the world, some of whom may simply choose to allay their boredom by trying to disrupt one of the world's branded icons—and we find ourselves looking at "network security" in a whole new light.

There has been no more important time in history for CPGs to interact with power, water, wastewater, oil & gas, chemical, nuclear, and defense industries to share best practices; but unfortunately, CPGs seem to have leaned out their manufacturing technical staffs to the point that there are few left to do this, and the industry has largely stopped sponsoring the kind of multi-vendor and multi-sector events that historically provided developmental and informal benchmarking opportunities for engineers and managers. One exception may be *The Automation Conference* (TAC), sponsored by the publishers of this magazine and growing in popularity among a variety of segments. I am convinced that the web does not adequately replace face-to-face opportunities to interact across disciplines, sectors, and levels of experience to help people understand that they don't know what they don't know.

In February of this year, President Obama signed an Executive Order entitled "Promoting Private Sector Cybersecurity Information

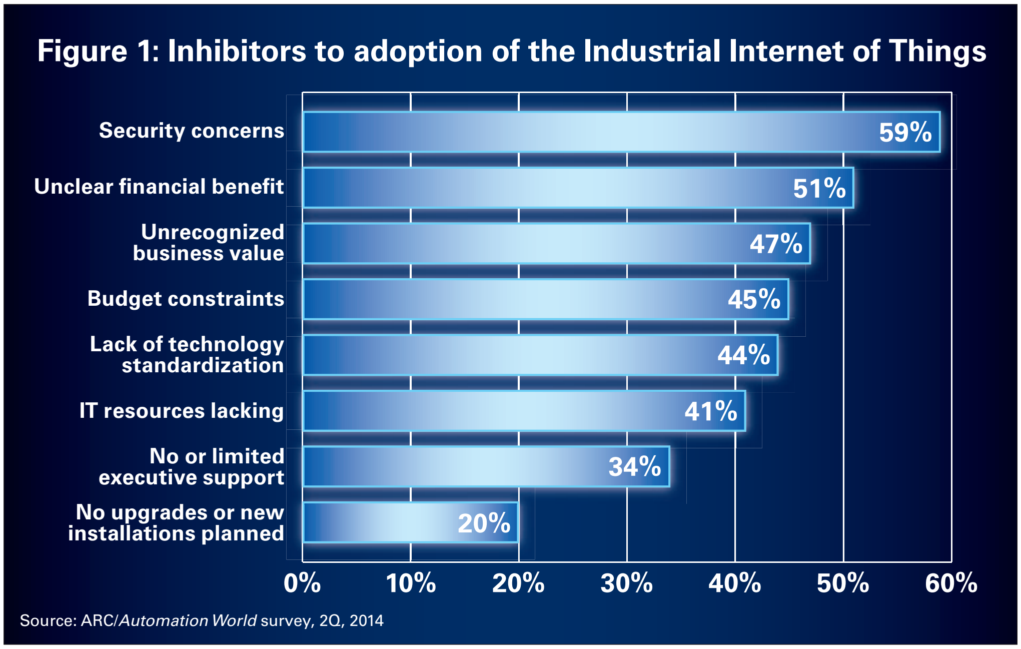

Figure 1: Inhibitors to adoption of the Industrial Internet of Things

Source: ARC/*Automation World* survey, 2Q, 2014

Survey results. When asked about factors that were inhibiting them from adopting IIoT, 59% of respondents in this survey cited security concerns as their number one concern.

Plant floor cyber security

Sharing." Companies don't like to share the fact that they are being targeted, and they certainly don't want to talk about having been breached. They don't want to share how they are protected, because knowing a target's defenses can be a key to defeating them. And in a world where sharing the tiniest bit of information with the public can open you up for patent trolls to come knocking, such as occurred when CPGs were drawn into the well-known Solaia law suits a decade ago, maintaining total silence seems the least risky action. But is it? I can say that the president's executive order did not make my research for this article any easier.

Why worry about shop floor systems?

A white paper published by the National Defense Industrial Association (NDIA) cites a number of reports and statistics about the persistence of cyber attacks on manufacturers, including this statement from McAfee's *2012 Threat Predictions*: "Attackers tend to go after systems that can be successfully compromised, and industrial control systems have shown themselves to be a target-rich environment. The NDIA report cites three categories of concern for manufacturers; 1) Theft of confidential technical data 2) Alteration of data affecting process and product integrity and 3) Impairment or denial of process control, reducing manufacturing availability. These 3 make up the C-I-A concerns of plant floor cybersecurity.

Innocuous devices? Even the most everyday devices, such as smart phones or flash drives, can be the means by which sensitive information that resides on the plant floor winds up in places it doesn't belong.

In testimony before a Senate committee, a National Association of Manufacturers (NAM) spokesperson said, "As holders of the world's leading intellectual property, including designs, patents, and trade secrets, manufacturers are consistently targeted by cyber thieves." Cyber attacks have been documented to have blown up a pipeline and to have disabled a steel mill, preventing the blast furnace from being shut down. Over 500 breaches were recorded by Verizon against manufacturers in 2014, probably far fewer than actually occurred.

As our factories have transitioned from analog to digital, as our controllers have become self-documenting, as our process flows have become available at-line, and as our operator interfaces have become fully graphic, perhaps the most complete sets of product specifications and formulations actually reside within our shop floor control systems. While the information in the corporate product data management (PDM) system contains the master specifications, those specs and the real-life specifications about how the product is really made reside on the shop floor, in digital format, that can be transferred on to a USB drive, someone's smart phone, or a message over the Internet. The same can be said for equipment suppliers' intellectual property that resides in their machines, often IP beyond that which is actually being used for a particular application. Security experts have pointed out that there is no point in a criminal attacking the PDM system when the same information is available in much softer targets, where confidentiality may be breached. This scenario represents the C in the C-I-A concerns.

One individual I spoke with in preparing this article linked cyber security with the Food Safety Modernization Act (FSMA) and Food Safety Defense Plans. Processors must ensure the safety of their foods, requiring security of the facilities and supply chains, which must include cyber security. Someone bent on adulterating an ingredient or a finished product no longer need be physically present to do so. What about hacking the HVAC or refrigeration systems to cause spoilage over a weekend? Or perhaps that network needn't be hacked at all, because an employee of the company monitoring your utilities needs a little extra income and lives in a culture that finds no issue with accepting a bribe. Since many factory floor cyber security plans ignore device networks, could someone easily gain access to yours to change the calibration of a sterilization loop or a canning process? One temperature transmitter may supply data to both the process control and the quality control system, and by recalibrating it for an hour every week, a factory might turn out a couple pallets of unsafe material every week without anyone ever taking notice. These examples point out loss of integrity, the I in C-I-A.

Machinery suppliers are increasingly offering to provide remote diagnostics for their machines. A production line may consist of adjoining machines supplied by competitors, all of which are connected to a single local area network. Each supplier has been given proper secured access to this LAN and has protected their individual machines with user names and passwords that have been entrusted to the field service technicians. Suppose that one of these techs leaves his company under unpleasant circumstances and joins a competitor. Knowing that a big project is coming up to be won by either his current or former employer, the service tech decides to take some revenge on his old employer and influence the outcome of the new project. Over a period of several weeks, using his new employer's legitimate access to the customer's LAN and his old employer's username and passwords, he begins to slowly detune the servo drives on the machines, resulting in steadily decaying operational performance. This example points to loss of availability, the A in C-I-A.

These examples have been fabricated. Resources found in next month's installment will point to real examples, often through recommended practices that have been developed based upon actual intrusions. These examples also point to the reality that entrusting cyber security to your IT department alone, or to the IT contractor that many small companies depend upon, may not be an adequate strategy. Do

Plant floor cyber security

they even know what a temperature transmitter is?

Many sources have cited differences between plant floor and IT systems and how these differences define a different set of security circumstances. This is an important realization when developing a cyber security strategy. Plants have 10's to 10's of thousands of network-connected devices to be concerned with. The nature of these devices is that many of them work 24-7-365 for upwards of 25 years. Their operation has been painstakingly tested. Their software may have evolved over decades. They cannot be subject to weekly patching and bi-annual obsolescence. A security plan cannot possibly be put in place to make each of these devices individually secure. What must be secure is the information that flows to and from them, especially if the source or destination is outside of the physical boundaries of the plant.

Going even deeper, the NDIA report cites differences that apply *between* manufacturing segments. For example, for discrete manufacturers, every new job (order) may bring new executable code into the manufacturing control system. This would rarely be the case for process industries where new orders, at worst, entail a recipe change; and this would be unusual for hybrid manufacturers. However, CPGs have their own new product programs, most of which will entail both the introduction of some new code and new network connections.

Is there a real threat to my company?

We all know in our gut that the threat is real, but it is easy to pass it off as someone else's threat. It's easy to reflect on Y2k being perceived as much fuss about nothing and thinking "here we go again." But have we adequately assessed how real of a threat plant floor

Can we learn from a security culture of an earlier time?

It wasn't many years ago that consumer products companies had incredibly effective security around their intellectual property (IP). Our digital age now poses an incredible threat to IP.

➲In my last post, we opened a discussion on plant floor cyber security that was expanded upon in a feature article in July issue of *Packaging World* and will be further developed in the August issue due out soon. I often find it useful to reflect on circumstances from a historical perspective to provide context and a sort of benchmarking for current issues. The value and control of intellectual property is an issue that can benefit from some reflection as we deal with the new threats of cyber crime.

I started my CPG engineering career about the time that 4 function calculators were becoming affordable. We didn't have computers on the factory floor, but we did have a security culture. Our engineering documentation was kept in a bank vault in the plant's engineering office and our product documentation in a similar vault at headquarters. Both were backed up with microfilm stored in cave in another part of the country. Only a few select people were allowed into that vault, and all copies leaving it were transferred from hand to hand between parties known to each other. The most confidential of information (such as process flows that would today routinely be built into HMI screens) was available only over the signature of an executive, who would not approve that for everyone. As a young engineer, I was on multiple occasions told that I was too young, too new, or too inexperienced to have this information. This was really about taking time (years) to build trust. If one was granted permission to take a truly confidential drawing, it was forbidden to make additional copies and the copy that you were entrusted with was tracked until being returned and destroyed. Periodic inquiries were made as to the document's whereabouts.

Control rooms were also part of our security culture. They were off limits to outsiders, sometimes even to the outside engineers who built and supplied the equipment in them. In one, a complex teletype-like machine caused us lots of headaches. When the service technician arrived, he stayed in the lobby and the machine was taken to him. After some adjustments, it would be returned to use, and if not working correctly, the process repeated itself. Service techs were allowed into some parts of the plant, but never without a full time escort. Pathways to and from the worksite were carefully planned and approved in advance and sometimes it was necessary to erect temporary walls along the way. We reserved the right to inspect briefcases and toolboxes in and out, so no documentation was going to leave.

Compare this with today's online P&IDs, formulations in PLCs, service techs walking in and out of plants with laptops and jump drives, employees taking confidential files home or accessing them from their home PC, and on and on. Then throw in the fact that hackers from any part of the world can breach our plant security perimeter without our even knowing it! In those days-gone-by, did we place too much value on our intellectual property, or do we today place to little on it? Has manufacturing become so simplified and commonplace that we no longer need protect our designs, processes and formulations? If we really think about it, I believe we will come to the conclusion that we need to protect our IP today as much, if not more, than we did before the digital age. But it is hard work, and maybe it is just easier and cheaper to pretend that it doesn't matter. It was easy for managers to control flow of people in and out of a vault, but it is complicated for managers, who may not have any real technical training, to control flow of data across their networks. The old adage goes that we manage what we understand.

I think we need a digital security culture that compares to our older security models. Can we do it? Watch for some tips in the upcoming August issue of *Packaging World*.

Plant floor cyber security

cyber is to us, no matter how small or how low tech or how off the grid we think that we may be? Have we thought about how large the potential consequences are should our systems be hacked, our products compromised, or our customers' intellectual property be stolen from us? What is the potential that our customers' or suppliers' systems could be penetrated using our systems or our people as a gateway?

We have all heard that the Target breach came through an HVAC contractor. Two stories seem to float around: one that the attack came through a project management system connection and one that it came through an equipment monitoring connection. It really doesn't matter which is true, because both vulnerabilities provide us with something more to ponder. If your HVAC systems or packaging machines are being monitored by a vendor, how far does their network extend? How secure is it? Where are the people that can access it? How are they vetted? Are they in a culture that would find nothing wrong with accepting a bribe to turn your HVAC or packaging information over to a competitor who might use it to calculate your production rates? How much are you actually saving by having that vendor monitor your equipment? The facilities department may have saved a few thousand dollars, but how big is the risk? And who gets to decide? And if you are the company doing the monitoring, ask yourself all the same questions. How big is your risk if someone on another continent, your employee or not, uses or hacks your network to steal information from your customer? Could one of your customers use your system to spy on or infiltrate another of your customers? Could you be accused of stealing proprietary information from a competitor if their machines are connected to machines that you are monitoring? Forget about the criminal aspect, what would be your civil liability in any of these situations?

The White House believes that the cyber threat to America is real enough that on April 1st, the president declared a cybersecurity national emergency. But evidence from an informal survey of machine builders that I conducted at PackExpo East in Philadelphia convinced me that far too few have really thought about this problem. I asked a number of suppliers, who obviously had equipment capable of being on a factory floor network, if they had thought about cybersecurity, and if so, what have they done to address it. The far most common response was a "deer in the headlights" look.

Whether you work for a large or a small CPG company, a packaging or processing machinery supplier, a technology supplier, or some other manufacturing-related company, the risks of plant floor cyber security affect you BOTH as a provider and as a consumer of products and services. The security of your network is of the utmost concern to your customers as should the security of their network be of the utmost concern to you. This is an issue as you look both upward and downward in the capital equipment supply chain, the materials and products supply chain, and the services supply chain. And by network, we don't just mean the enterprise networks, but also the plant networks that connect to the enterprise, the process control and automation networks within the plants, and the device networks within the automation systems. Cyber security has been called a multi-dimensional problem requiring customized solutions for conventional IT, automation & control systems, intelligent network-connected devices (sensors, cameras, point of sale terminals), mobile devices, and the cloud.

Preparing for exponential growth

The concerns about plant floor cyber security are juxtaposed against the predictions for the Industrial Internet of Things (IIoT). Pundits tell us that if we do not embrace IIoT as manufacturers, we will be putting ourselves out of business. Others tell us that there can be no implementation of IIoT until security is established. Peter Holicki of DOW Chemical made a clear statement at the ARC Industry Forum reporting that DOW believes that it owes it to the community to guarantee that the systems that ensure plant safety are completely disconnected from the Internet. But keeping systems separated may be easier said than done. Today computer technology is so inexpensive that it creeps into our plants sometimes with little if any conscious planning; so it takes conscious planning to keep it out. One supplier told me of a case where a European plant was shut down for a day because someone hacked into the WiFi link on a conference room projector that was also connected to the plant's Ethernet. Who would have planned for that threat?

In 1995, fewer than 1% of the world's population was connected to the Internet. It took 10 years for the first billion users, 5 years for the second billion, and 4 years to bring us to where we are today with 3 billion users, almost half of which are in Asia. Projections are to hit 5 billion in the next 10 years (growth is slowing). Cisco claims that there are currently over 15 billion things connected to the Internet, with a projection of 50 billion by 2020. Some say that 40 billion of those connections will be wireless, with much of the growth coming from sensors, many of which will be in our factories.

The *Symantic Internet Security Threat Report 2014* included this headline within the executive summary: "Attackers are turning to the Internet of Things." It went on to say, "Today the burden of preventing attacks against IoT devices falls on the user .... Manufacturers [IoT device makers] are not prioritizing security..."

Last year, in conjunction with our sister publication *Automation World*, ARC conducted a web survey to gauge industry perspective on the adoption of the Industrial Internet of Things (IIoT). This survey sampled a wider manufacturing audience than CPGs and packagers and resulted in over 200 responses. The survey targeted those who were current or potential users of IIoT solutions or providers of such solutions, a rather well-informed group. When asked about inhibitors to adoption of IIoT, the number one concern of respondents was security (**Figure 1**).

More connected users (2 billion more), more connected devices (35 billion more), and a lack of prioritization of security would seem to be the ingredients for a perfect storm, substantially increasing the means, motive, and opportunity for those who may wish to attack our plants. While my colleagues and I often quip that technological advances in manufacturing should be measured in "dog-years," a dog-year mentality will not prepare manufacturers for this explosive growth! We had best plan accordingly.

Next month we will suggest some of the areas that should be considered in that plan, some strategies that could be employed, and some resources that can be drawn upon in the process of turning discussions into meaningful action. **PW**

Plant floor cyber security—turning discussion into action

Last month we explored why plant floor cyber security should be on your agenda. Here in Part 2 we focus on how to establish a serious and open dialog, develop strategies, and tap outside resources.

Keith Campbell, Contributing Editor

As we continue our exploration of plant floor cyber security, we need to develop strategies that work for our particular situation and seek guidance from a variety of outside resources. We can then turn discussion into meaningful action. This month's concluding segment on plant floor cyber security is intended to provide some suggestions to facilitate this process.

It may help to begin by familiarizing ourselves with some new terms. The “actors” are those individuals who take part in creating a cyber security attack or breach. Actors may be nation state agents, organized criminals, lone wolf criminals, bored teenagers, disgruntled employees, or paid informants. Many of these are hackers. There may be “white hat hackers” who seek out “vulnerabilities” in systems for the purpose of protecting against a breach, referred to as ethical hacking. The “black hat hackers” will seek out and exploit vulnerabilities for malicious purposes. “Grey hats” may seek out the same vulnerabilities to sell them to the highest bidder or to claim bragging rights. Each of these groups may be “probing’” our systems and our people as they seek to find and exploit these vulnerabilities.

Not all actors are hackers however. Some may simply be individuals who have obtained legitimate access to systems and use it for malicious purposes. Often such people are not intending to do harm, but are duped by “phishing” or “spear-fishing” attacks where the bad actors seek accomplices who unknowingly provide information that may be used in a more damaging attack. Manufacturers are among the most frequently targeted by spear-fishing attacks. Bad guys go after the weakest link in the chain—the people. Criminals will follow your employees home to steel information that will allow them access to your systems.

It has been said that cyber security requires the integration of psychology and engineering, because understanding the motivation of the people trying to infiltrate our systems is critically important. Too often we make our plans assuming that we operate in an honest and ethical society. When it comes to cyber security, we can no longer assume that. Just because our plant sits in a valley of tranquility, those seeking to do us harm may be anywhere in the world where the values and mores are beyond our understanding. Motives may include terror, espionage (national, industrial, commercial, or private), hactivism (activism motivated by social, political, or ideological beliefs),

Plant floor cyber security

financial gain, revenge, notoriety, or vandalism.

Our "attack surface" is the amount of area we expose to an actor. The more network connections we have, the more internet connected devices we have, the greater our attack surface and the more likely it is that there will be vulnerabilities. In years past, we could secure all of our assets, both physical and intellectual, by creating a security perimeter around our plant. Only people trusted to enter or leave that perimeter were permitted to do so. We could physically lay eyes on every person, and if we chose, on every document, that crossed the physical perimeter. We could send security personnel to patrol that perimeter and validate its integrity day or night. We could look for holes in the chain link fence or for fire doors left ajar. We could monitor everything with cameras and motion sensors if deemed necessary. Today if we have a network connection, our perimeter is much different. It is not without meaning in this regard that the term "perimeter" implies only two dimensions while the term "surface" implies three.

An "attack vector" is the means or path that an actor uses to gain access to his target. By finding a vulnerability on the attack surface, he exploits that as a means to perpetrate his attack. He might use a receptionist to obtain a legitimate username and password. He (or his robot) might dial thousands of mobile numbers until he finds a broadband modem attached to a piece of factory equipment. He might have an employee attach a cell phone to a network plug that was relocated to the outside of a control panel for safety reasons. He might piggyback on a VPN connection. He might infect a service technician's USB drive, knowing that it will be plugged into a machine that can later become the attack vector.

Nature of solutions

As was stated earlier, this is not intended as a how-to guide. But in the process of developing this article, some general strategies emerged. Here are some of them.

Peter Holicki of Dow Chemical in an ARC Industry Forum keynote address affirmed that technology requires strategy, business alignment, and business ownership. Dow does not let companies that own the technology control them, DOW controls the technology. This is a tenet that I strongly support, especially as it pertains to the security of our intellectual property, our operations, our people, and our products. Manufacturers should have shop floor technology plans that align with their business, financial, marketing, HR, and security plans.

In that same session, Brigadier General (Ret) Gregory Touhill of the US Department of Homeland Security explained that cyber security is misunderstood as a technology issue for discussion in server rooms when in fact it is a risk management issue for discussion in classrooms, lunchrooms, and boardrooms. It is a matter of risk for everyone in our society.

Cyber security is a team sport. We need our plants to be safe, secure, and resilient. The first thing to do is to put it on the agenda, and keep talking about it until it permeates every part of the company. Help your employees with security not only in the office, but at home. Then discuss with your partners up and down your supply chain.

Cyber security needs to be raised to the level of safety in our plants. A safe work environment is a condition of doing business (a license) in today's world. A cyber-secure environment should also be a requirement. As we are required to report lost time accidents to OSHA, we should be required to report cyber security incidents as the Germans are already doing. One CPG representative told me that they were treating cyber security like safety and like sexual harassment awareness, where every employee is required to attend training and retraining. We need to create a cyber security aware culture in our plants. This is probably one of the most important steps to be taken.

Realize the impossibility of protecting all of your information to the same level. Moltke the Elder taught that in warfare, he who defends everything defends nothing. Identify where the really important data is (maybe in the process control system, not the office) and apply more resources there.

Realize that you can't harden everything. There are still tens of thousands of systems in the plants running unsecure-by-design systems such as Windows 98 and XP. These aren't going away anytime soon. Think of a turtle. These soft structures can be surrounded by a hardened shell of hardware and software that monitors all of the assets and controls any information flow to or from them. While you cannot hope to keep software up to date on all of the connected devices, you can apply daily patches to the system comprising the shell to keep it as secure possible. This will require dedicated staff who understand both IT and control systems. And, this is not the long term solution. In parallel with this approach, we need to take a 'secure by design' approach for new systems.

Planning should be multi-dimensional including plans for protec-

Plant floor cyber security

tion, prevention, mitigation, response, and recovery. Our systems must be both safe and, when things to go wrong, resilient.

If you allow external connections, make everyone come through a common and closely managed access point. It is like having only one entrance to your plant.

Establish, communicate, and enforce strict policies regarding who can authorize the addition of ANY device onto a network or the addition of any communications access to a machine. Is your landlord or your building management department making connections that your process control or IT departments don't know about? Is the cafeteria or the lab having their equipment monitored remotely? If so, chances are good that there are cross connections to your internal networks.

Establish, communicate, and enforce policies regarding visitors, especially service technicians bringing computer technology into your plants and attaching it to their equipment in your systems. Keep in mind that big corporate equipment suppliers may resist allowing you to scan their laptops or USB drives just as much as you may insist, resulting in a standoff while production is down. Plan and agree in advance.

Remove and prohibit vulnerable technologies unless you can prove your system keeps them secure. These would include DHCP, dial-up modems, broadband cellular modems, tablets, and smart phones. In municipal systems such as water and wastewater, the concept of bring your own device has emerged whereby plant operators use their own cell phone as an operator interface. What a vulnerability that makes!

You will need to know about every digital device in your plant and have up to date network and data flow diagrams. In 1999 you probably had these things in preparation for Y2k, but that inventory has long since gone out of date. When you complete this one, establish procedures to keep it current. Learn from other mistakes of Y2k.

Think about secure-by-design, but realize that every design will eventually be compromised. Security needs to be part of every design going forward.

Cyber security activities need to be both measured and tested. Have cyber security key performance indicators (KPIs) as part of your plant and corporate balanced scorecard.

Use industry and government standards and practices as part of your solution, but don't mix up minimum recommended practices with what you really need to do.

Resources

There are a great many public and private resources available to help you get started on the journey of protecting your factory floor assets from malicious cyber activity. Presidential Policy Directive 21 issued February 12, 2013 addresses Critical Infrastructure Security and Resilience and clarified the roles and responsibilities of cabinet level departments with respect to physical and cyber security. The key areas of responsibility include overall coordination by Department of Homeland Security (DHS), national defense by the Department of Defense (DOD), enforcement by the Department of Justice (DOJ) and the FBI, and research and development of tools for improving security by the Department of Commerce (DOC). Other departments such as the NRC, FCC, FDA, GSA, etc. have specific responsibilities within their sectors. All of these departments have established teams who support cyber security efforts.

The FBI has cyber security squads, referred to as GeekSwats, in each of its 56 field offices that work within 16 identified segments including critical manufacturing and food & agriculture. The FBI has established a partnership with the private sector called **InfraGard** (www.infragard.org) for the sharing of information and intelligence to prevent cyber crime. There are 80 chapters of InfraGard that meet across the United States with 350 of the Fortune 500 represented.

DHS operates the National Cyber Security and Communications Integration Center (NCCIC), the U.S. Computer Emergency Readiness Team (US-CERT), and the Industrial Control Systems Computer Emergency Response Team (ICS-CERT). Each of these agencies has extensive information, tools, and resources available on their websites with the ICS-CERT focusing specifically on the topic of factory floor

Cyber Security - That deer in the headlights look

A survey on plant floor cyber security brings many blank stares

➲In preparing a Packaging Controls & Automation feature for *Packaging World*, I took the opportunity of Pack Expo East to walk around and ask exhibitors about plant floor cyber security. The most common response to my informal survey of machine builders to the question "Have you thought about factory floor cybersecurity, and if so, what have you done about it?" was a deer in the headlights stare. But to be fair, there were other thoughtful responses that can be paraphrased as:

1) Some of our machines are on the customers' factory LANs, but we have no external access.

2) Some or our machines are on the customer's factory LAN and we have external access when the customer permits it through their firewall.

3) Some of our machines may or may not be on the customer's factory LAN, but we have remote access through a broadband SIM card that we put into the machine.

4) We used to use dial-up connections to our machines, but as far as we know, all of our customers have removed those.

5) We have really thought about this and we use secure cloud services with our customer's involvement.

To learn more about why plant floor cyber security should be on the agenda of every manufacturer and every link in the supply chain, read the article Plant floor cyber security - Is it on your agenda? Follow up next month with tips on creating a plan, strategies to employ and resources to draw upon.

Plant floor cyber security

security. They provide alerts, advisories, assessment, training, standards, conferences, and a host of tools, case studies, and best practices. Among interesting documents offered by ICS-CERT is one entitled *Cybersecurity Questions for CEOs*.

The National Institute of Standards and Technology (NIST) falls under the Department of Commerce. Last year NIST issued the document *Framework for Improving Critical Infrastructure Cybersecurity* to guide businesses in applying a systematic process for identifying, assessing, and managing cybersecurity risk. NIST operates 60 Manufacturing Extension Partnerships across the US that can make resources available to apply this framework, especially for smaller manufacturers.

Professional and trade organizations such as the International Society of Automation (ISA) provide tools, assessment, training, and certifications in cyber security. ISA focuses on factory floor systems, and has created a series of ANSI and ISA consensus standards on *Security for Industrial Automation and Control Systems.*There are 13 parts envisioned in the series, which has been under development for 13 years by groups of volunteers. Find information at isa99.isa.org .

Industries closely related to manufacturing, especially those that are being driven to implement protective measures by regulation, have developed much useful information. For example, the North American Electric Reliability Corporation (NERC) has developed 81 Critical Infrastructure Protection Standards, the so-called NERC-CIP Standards. Unlike ISA standards that are copyrighted and available for a fee, the NERC-CIP's are available at no charge at www.nerc.com.

Educational institutions are gearing up to prepare cyber security professionals. Gary Beach in an article in the *Wall Street Journal* made the claim that lack of talent is America's most challenging cybersecurity challenge. One step in addressing this was a $23.2 million Department of Labor grant to establish the National Consortium for Mission Critical Operations (NCMCO), a group of community colleges partnering to create programs and curriculum to address the needs for a skilled workforce that can anticipate, prevent, mitigate and respond to cyber security breaches. Strategies being used in this effort are well aligned with the strategies outlined in *The Manufacturing Workforce Development Playbook* available at www.packworld.com/workforce. These strategies have also been extensively used to build capabilities for industrial maintenance and mechatronics. Universities are also engaging in the cyber fight with, for example, Carnegie Mellon (CMU) establishing the CyLab partnership with industry and the CERT Division, which is part of the Software Engineering Institute at CMU.

Communications and software companies with a vested interest in cybersecurity collect information and provide reports, training, and information for the public. Verizon and McAfee publish annual reports such as the *Verizon 2015 Data Breach Investigations Report* or the McAfee Labs quarterly *Threats Report*.

Hardware, software, and service suppliers have made a great deal of information on cyber security available. These include white papers and blogs such as those offered by Tofino Security. New security hardened products are being offered by vendors. Despite the ongoing shakeout of PLC platforms, even a completely new security and electro-magnetic pulse hardened PLC platform has been introduced by Bedrock Automation. Five years ago, I think no one would have imagined a new entry into the PLC marketplace, but security is deemed to be that big of a deal that entrepreneurs thought it worthwhile.

In preparing this article, I made use of Chantal Polsonetti's LinkedIn discussion group Industrial Internet of Things where I posted the question, "Is anyone concerned about the security aspects of having our factories connected as part of the IIoT?" This resulted in a number of thoughtful responses, as have many of the other threads in the group. You may join this group on LinkedIn.

These are by no means all of the resources that are available or that will become available as the battle continues. The FDA has taken limited steps in its areas of control, focusing on medical devices and healthcare facilities. Other food and pharmaceutical entities need direction just as do the larger CPG and hybrid industries and their equipment suppliers. It would be worthwhile for manufacturers in these spaces to encourage their industry associations to help them wade through the vast quantities of information that are available and to help develop guidelines for their particular segments. In the long run, this could arguably obviate the need for forced government regulation and produce superior results. NAM prefers a voluntary system, while others point to the safety success of the nuclear industry as an example of forced regulation that works. In my experience, hybrid manufacturers have not heretofore shown enthusiasm for participating in the development of standards, bringing them to a timely conclusion or adopting them in a timely fashion. But in this case, it seems to me, there are only three viable choices: 1) everyone takes on this gigantic task on their own; 2) manufacturers work together to create and adopt robust standards; or eventually 3) government attention will turn to these additional industry segments and force regulation upon them.

It's a new world

It is a new world, in which whether we like it or not, cyber security is a real threat. It's not just the financial sector's problem or just a problem for nuclear plants, pipelines, and defense contractors—they are the tip of the iceberg and the areas that need to be addressed first. A broader manufacturing industry undergirds our society and our economy and cannot be allowed to become the soft underbelly to be attacked by cyber criminals. And within our manufacturing enterprises, our factory control systems may hold the most confidential of our confidential information. They are critical to process, people, and product safety.

Our factory systems contain the widest variety of digital systems, in age, source, and function, making it the hardest part of our infrastructure to secure. We should not put our businesses at risk for loss of confidential information, loss of product integrity, loss of availability, or loss from civil claims if our systems or employees become the vector used to attack a customer or supplier. We need to discuss this at the highest levels of our companies, plan for it, fund it, and create a security culture that encircles the threat.

As CPGs and hybrid manufacturers, we should band together through appropriate associations to assure that we aren't left behind as government focuses on process and discrete "critical" industries, and to obviate the eventual transfer of regulations created for those industries onto us. We need to support education and employee development and cross-pollination with other industries. And we need to plan carefully and act prudently as the Industrial Internet of Things comes upon us, to be sure that we balance security, productivity, risk, and revenue. **PW**