WWW.CHEMICALPROCESSING.COM

CHEMICAL PROCESSING

LEADERSHIP | EXPERTISE | INNOVATION

SPECIAL REPORT:

CYBERSECURITY RESILIENCE

Sponsored by

ABB

PutmanMedia®

CONTENTS

Industrial Cybersecurity: How Much is Enough?

New threats and complex consequences raise the bar for security management

By Sheila Kennedy, Contributing Editor

If cybersecurity wasn't already a household word, the recent Equifax data breach surely narrowed the gap. Chemical processing companies have long been confronting cybersecurity concerns and may be farther along than most industries in protecting and defending against the risks. Unfortunately, the complexity and urgency of the task keeps increasing, while the costs of doing nothing, or too little, are becoming more severe.

Too often we see new reports of failure. Now, public disclosure rules are helping to uncover the risks and consequences. The repercussions of an incident can be brutal — not only financially, but to reputations, security, competitiveness, efficiency, downtime, and human and environmental health. It could even put a company out of business.

In chemical processing industries, any breach, loss, or disruption is unacceptable — even more so in around-the-clock environments. Ensuring maximum readiness requires a clear understanding of the risks and a well-formed strategy that protects the complete, fast-growing digital footprint. This includes treating operational technology (OT) and industrial control systems (ICS) with the same care as information technology (IT).

ENDLESSLY EVOLVING THREATS

Cybersecurity is a journey with no end. It involves understanding, avoiding, and mitigating wide-ranging threats from both internal and external sources, including targeted hacks, opportunistic malware, accidental data releases, and even the loss of computers and storage media. Old-school threats such as distributed denial of service and email phishing have been joined by watering hole attacks, man-in-the-middle attacks, DLL injection, exploit kits, legitimate but infected software, and even drone threats.

In the past, cyber threats were less sophisticated, less persistent, and easier to recognize and address. IT malware and "script kiddies" (persons who use scripts or programs developed by more skilled hackers) were the primary threats, says Eric Byres, senior partner at ICS Secure (www.ics-secure.com).

"Now we see very complex, multistage cyber attacks from professional attackers who have the capability to perform long-term reconnaissance operations and manage sophisticated attack strategies," notes Byres. "They have the ability to maneuver and deploy a new pathway into their victim if someone detects their initial probes. And, they are patient."

A good example is the Crash Override attacks on the Ukrainian power industry's ICS systems. Built specifically to disrupt physical systems, the malware twice knocked out power to a portion of the Ukraine. The 2015 attack involved manually switching off power to electrical substations, while the 2016 attack was fully automated, quicker, and required far fewer people.

Though catastrophic sabotage of ICS systems is a prominent fear, most attackers prefer to stay under the radar. Stealing intellectual property (IP) is more lucrative for them, explains Byres. Chemical processors don't want their competitors (especially nation-state competitors) to get the IP in their control sys-

"Now we are seeing that the risks and financial consequences are real."

tems because losing it can have a terrible long-term financial impact.

For instance, the Nitro Attacks of 2011 were used to steal secrets from the chemical industry such as designs, formulas, and manufacturing process details. One victim, The Dow Chemical Company, reported to the BBC that the company "engaged internal and external response teams, including law enforcement, to address the situation. As a result, we have no reason to believe our operations were compromised."

Dragonfly (aka Havex) was a more persistent cyberespionage campaign against U.S. and European energy companies in 2013 and 2014. It used remote access tool (RAT) malware to gather system information and data over a long period of time, and it bears the hallmarks of a state-sponsored operation, according to Symantec. "This malware was used to gain access to industrial control systems and establish remote 'command and control.' It is believed that this malware was installed and used for exfiltration of information," says Walter Sikora, global manager cyber security services at ABB's Industrial Automation Division (www.abb.com).

There were at least two instances of alterations to water treatment chemicals and flow when hackers breached an unnamed water utility's aging AS/400-based operational control system, according to Verizon's 2016 Data Breach Investigations Report. The public health consequences could have been great, but alert functionality allowed the utility to quickly identify and reverse the changes.

Business interruption is another goal of hackers. In 2012, 30,000 workstations at Saudi Aramco were forced out of service for 10 days by a malicious virus implanted by political activists, or "hacktivists." The oil company's exploration and production operations were unaffected, but the management of supplies, shipping, and contracts became paper-based, and the corporate email and office phones went down.

Ransomware such as WannaCry and NotPetya are broad, opportunistic malware campaigns. In June 2017, NotPetya encrypted entire hard disks of computer systems in wide-ranging industries around the world. As of mid-August, pharmaceutical manufacturer Merck was still feeling the effects and had not fully measured the impact on its manufacturing operations or bottom line. Snacks manufacturer Mondelez International estimated its NotPetya costs at just over $150 million in lost sales and incremental expenses. Shipping giant A.P. Moller-Maersk reported that system shutdowns and business interruption triggered by NotPetya will cost it as much as $300 million.

"These are real examples we imagined and talked about for years — and now we are seeing that the risks and financial consequences are real," says Sikora.

EXPANDING DIGITAL FOOTPRINTS

Rapid digitalization of chemical processing assets and supporting automation, maintenance, and process control systems has enabled a tremendous convergence of formerly standalone technologies. It has broadened the scope that a risk manager has to take into account, but many organizations have not caught up to the technology, suggests Marty Edwards, managing director at Automation Federation (www.automationfederation.org).

"If your control system was islanded, it is now being connected to your business network, which is in turn connected to the internet, and it certainly exposes these legacy types of infrastructures to present-day threats. In many cases, you've got the control

"Digitization has broadened the scope that a risk manager has to take into account."

system environment utilizing old or in some cases obsolete operating systems, which now have been interconnected to the threat landscape," adds Edwards.

PATHS TO OPTIMAL PROTECTION

People in the industrial space who finally decide to spend money to solve a cybersecurity problem often get frustrated when every six months another problem pops up that needs fixing. Management sees this as a "whack-a-mole" approach, says Sid Snitkin, vice president of cybersecurity services at ARC Advisory Group (www.arcweb.com).

Too often, companies end up buying solutions that they can't use or maintain. "Not only will they not get the benefit of the technology, but the staff will become overworked and unable to do even the very basic tasks, such as updates and patches, and known risks may not be acted upon," explains Snitkin. "As a result, plant managers may think they're secure when they really aren't."

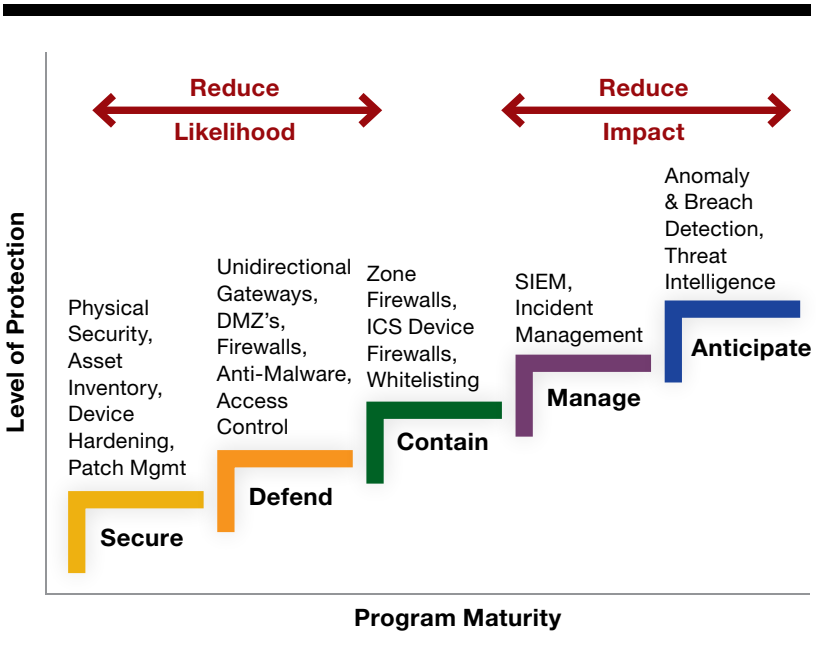
There are multiple avenues to ensuring a more effective cybersecurity program:

Understand the risks. Companies will plan for a health epidemic or a natural disaster, but not necessarily a cyber event. The most senior executives need to recognize that cyber risks can be as big, or bigger, than any other risk they are managing, says Edwards.

Expand asset awareness. If digital devices on the factory floor don't show up on the corporate IT inventory list, the corporate information security officer may not realize there's a risk or a liability on their hands, he adds. OT/ICS and IT systems and devices should be managed with similar diligence.

Establish a strategy. To better understand the relationship between cyber risks, strategies, tactical technologies, and human resources, ARC Advisory Group developed the Cybersecurity Maturity Model. It is a framework for deciding what level of risk to assume, and how to manage to that level most effectively. ARC recommends working from the bottom up — do each step well before moving to the next step.

Build a capable team. "The number-one problem is not the technology; it's the people, both in the number needed to do the basic tasks, and also in expertise that's needed for the more advanced tasks," says Snitkin. Hire the right people and empower them to do a good job. Buy a cybersecurity management solution to improve the efficiency of your current



ARC Maturity Model for ICS Cybersecurity Programs

"Too often, companies end up buying solutions that they can't use or maintain."

staff, and offer more training if feasible. Supplement the team by hiring additional resources or engaging third-party services.

Start with the basics. The scope of ransomware victims is telling; had they been able to reinstall everything from their most recent backup, it would have been business as usual within a few hours. Become diligent about performing backups, updates, and patches. Apply user and access controls, end-point protections, network segmentation, and system hardening. Make sure your antivirus protection and firewalls are turned on. Don't leave PC ports open.

Monitor the environment. "Dragonfly, Stuxnet, and BlackEnergy were all pretty obvious on the ICS network once you looked for them, but sadly few companies did. Even sadder still, few really have a means of monitoring their ICS network traffic in a meaningful way today," observes Byres. Consider a solution designed to simplify ICS network monitoring.

Translate observations into immediate actions. Waiting for the morning shift to sort out a patching strategy isn't good enough. "If network activity is detected indicating someone is scanning for ICS devices using a given protocol, then the security team needs to know exactly which devices use that protocol, and which might be susceptible to the scanning. They also need to know exactly what version of firmware software is on these devices, and what possible vulnerabilities the attackers might exploit next. Finally, the company must have a way to immediately triage those devices," suggests Byres. An integrated platform for real-time device management can help you understand the context in your ICS and act on issues immediately.

There is no single, correct approach to cybersecurity, but steps should be taken to enhance your readiness and minimize the effects of a successful attack. Resist the tendency for fear, uncertainty and doubt, and make cybersecurity a priority in your organization. ◻

Cybersecurity Q&A with Walt Sikora

Walter (Walt) Sikora is global manager of cybersecurity services at ABB's Industrial Automation Division. Here he shares his views on today's cyber risks and responsibilities.

How does today's cybersecurity landscape differ from in the past?

The threats have changed in ways that we never imagined — just look at all the different ICS-specific malware now. In addition, cyberattack tools have become a big business within the criminal underground on the dark web, and nation-states have recognized the importance of building cyber armies and weapons. We have made great progress in the last ten years, but there is still a lot of work needed to protect against all the new cyber risks.

How has digitization heightened the challenge?

Back in the early days of control systems, the systems were closed and proprietary. Now that modern automation systems are interconnected to enterprise business systems, the cyber risks have increased dramatically. However, operating system owners have not increased their spend to mitigate these risks across their full fleet of assets. Organizations need to accept that there is a cost of using digital technology, and that cost needs to be factored into their business plan such that security is a top priority.

What are the implications for chemical processing?

Chemical processing plants are quite familiar with managing hazardous operations, but cyber risks are different. Many organizations are still learning to incorporate cybersecurity into their hazard and operability (HAZOP) process. The logistics can be difficult; in a 24/7 processing operation, even a simple machine reboot following a security update requires significant preparations and planning.

What solutions, services, and strategies can help?

There are no technology solutions that will reduce all the risks or offer 100% security. Doing the basics well, before investing in advanced cyber technologies, is the key. I recommend having a solid security policy and mapping out a three-to-five-year journey to achieving adequate security maturity. Some effective tactics to consider are hardened perimeters, defense-in-depth, whitelisting, network intrusion prevention, air gapping, and security awareness training for all employees. Also, make sure to include specific contractual language about cybersecurity in your OT/ICS requests for proposals. To execute your plan, leverage your IT and OT teams, but also look for OT vendors who can offer comprehensive cybersecurity services.

What are industry leaders doing to help?

The Global Technology Forum, universities, and standards bodies such as Platform Industrie 4.0 and Industrial Internet Consortium are among those working to strengthen cybersecurity. ABB and several other system vendors recently completed a collaborative effort drafting the recommended practice for "Cybersecurity in the oil and gas industry based on IEC 62443." ABB also has an active Group Cyber Security Council, and our Safety Execution Center (SEC) is a TÜV-recognized Functional Safety Management System. But, we all need to do a better job of using simple language to explain the cyber landscape in common-sense business language, so the average person running a company can understand it and make intelligent investment decisions.

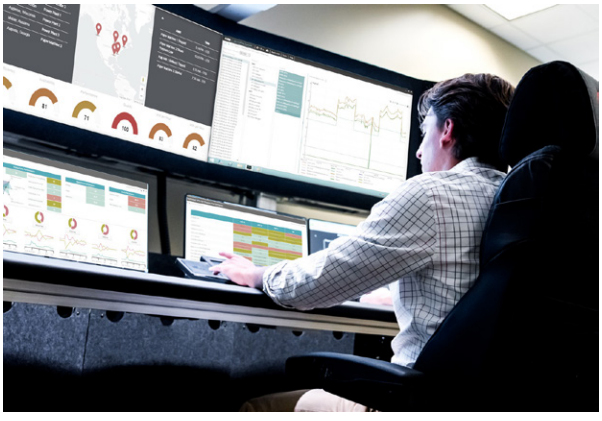
Pay Attention: WannaCry and NotPetya Demand a Cybersecurity Strategy

By Walter Sikora, Global Manager Cyber Security Services, ABB

The need for a solid cybersecurity strategy has been discussed and debated for almost a half a century now, and yet the basic worm-type attacks first documented back in 1972 are still with us today. Why? Because even the most basic measures to protect control systems from these types of attacks are still not systematically employed.

It's hard to believe that there are still thousands of systems in operations today without any basic security controls in place. If you own a car, or a house or a boat — just about any "big-ticket" item that would be expensive to replace — you protect that asset with insurance. And even though you can't see it or feel it, you know, instinctively, that it's worth the money. You sleep better at night knowing you have it, and it would be a high-priority item to re-acquire if you lost it — especially if it contributed to your livelihood. But, when it comes to control system cybersecurity, this thinking, for some reason, often is not applied. Cyber experts are still struggling to convince senior management that they need to spend money to protect their control system assets. But recent events from early 2017 should be setting off alarm bells in board rooms across the industrial world. Two viruses, WannaCry and NotPetya, have wreaked havoc on companies that were running older Microsoft Windows operating systems, but failed an entry-level cybersecurity test: keep your systems patched and up-to-date.

Both of these viruses were destructive. WannaCry was standard ransomware, but NotPetya was a wiper bug that masqueraded as ransomware. Its purpose: cause maximum damage to the systems it infected. It forced thousands of large complex operations in many industries to halt production by scrambling data, and offered no way out to its victims, such as paying for the decryption keys.



Industrial control systems are increasingly coming under attack by common viruses aimed at Windows operating systems.

Companies that were impacted are just now disclosing the financial impact of these attacks. It's not pretty:

- One of the world's largest container shipping companies, with substantial oil & gas assets as well, will wipe as much as US$300 million off its books in the third quarter of 2017
- A skin-cream maker said that NotPetya cost it US$41.5 million in first-half sales
- A French building materials manufacturer said it would lose about €250 million in sales this year
- The worldwide pharmaceutical production of a major drug producer was disrupted and the total financial impact is still unknown
- A major international package delivery company announced the loss of about US$300 million

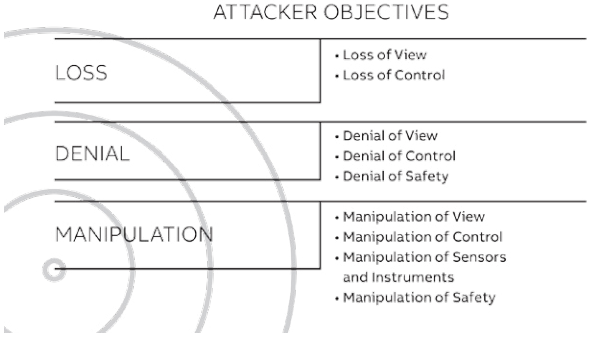
That is a lot of money — money that could have refreshed legacy systems, acquired new assets, invested in R&D, paid employee bonuses, delivered stockholder dividends, etc. Certainly some of it should have been spent hardening these organization's systems against such events. So why wasn't it?

WHY COMPANIES DON'T INVEST IN CYBERSECURITY

Part of the answer is pretty simple: it's hard to convince companies to spend money on something that has no measureable return on investment (ROI). Basically, it's hard to put a dollar value on an event that may not happen.

Of course, everyone knows that cybersecurity is important and that it falls into the general category of risk management. But, as an event such as the massive oil spill in Alaska's Prince William Sound in 1989 proves, the cost of doing nothing is far greater than the cost of being proactive (super tankers are now made with double hulls to prevent a repeat of that ecological disaster). It isn't that control system owners don't deploy cyber and security solutions; they do. They are aware of the problem and take actions to avoid risks. But many in the industrial world are still too focused on the big attack or hack — the nation state that blacks out an entire region or shuts down the water supply to a city — when the bigger risk is common malware that impacts a control system because it is running older, unprotected, and unpatched operating systems.

Detected in 2016, Petya is ransomware targeting Microsoft Windows-based systems, causing master boot record infections.



Attackers often look for a return on their investment in the form of a ransom but not always. Some attackers simply seek to disrupt and destroy critical control systems.

This risk exists even if the system is "air-gapped" from the business's network. People going about their daily routines often introduce data and software using removable media such as USB drives to make changes to their systems, introducing the potential for viruses along the way. And, as these air-gapped systems become more interconnected to enable integration with business applications, they become increasingly exposed to the internet. This is why it is far more likely that common malware is the threat that will cause the most damage in the long run — just as we've seen with WannaCry and NotPetya.

This is because there is a fundamental disconnect in securing operational technology (OT) vs. information technology (IT). But as OT becomes more exposed to the internet, it faces the same cyber security threats as any other networked system because operators have adopted the same hardware, software, networking protocols and operating systems that run and connect everyday business technologies, such as servers, PCs, and networking gear.

At the same time, many machines and legacy systems are so old and so proprietary, no self-respecting cybercriminal would ever write malware to attack — because there just aren't enough of these systems

around to make it profitable (typically the main motive of hackers everywhere today) or notorious (if they have more harmful motives). That leaves control system operators in a tough position. If they try to deploy the same security measures as IT then a) they may not work or b) they may actually shut down a running production process. This could be more harmful for the business than the cyber-attack.

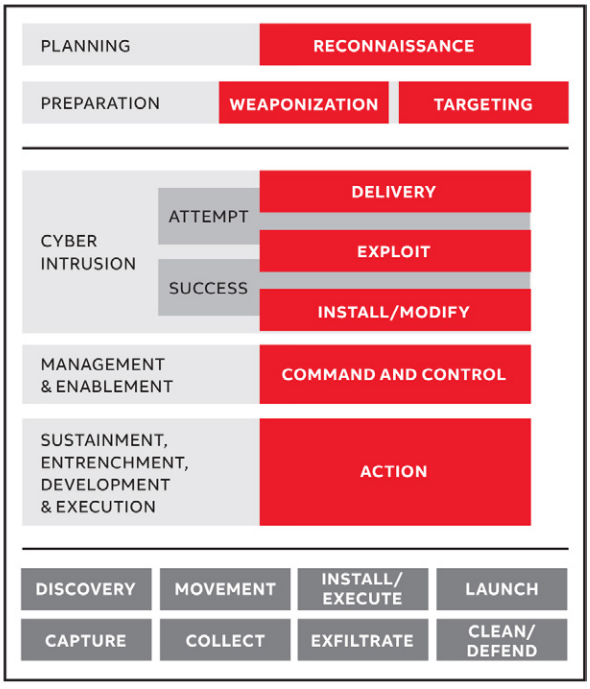
The problem is that IT cybersecurity solutions tend to focus on locking down data when there is a threat. That makes sense if it's a credit card database, but it doesn't work out so well if a firewall blocks programmable logic controllers (PLCs) from opening and closing valves in an oil refinery or pulp mill.

LUCK IS NOT A STRATEGY

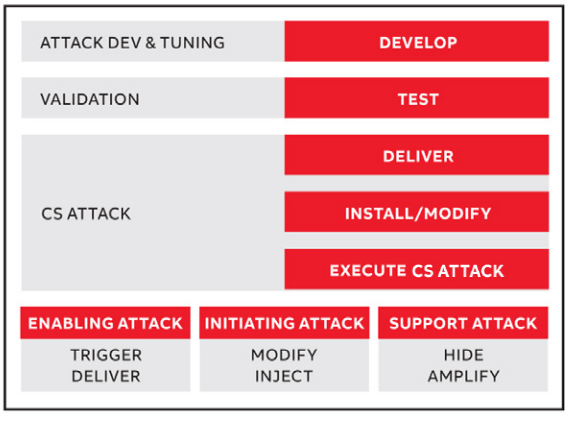
And then there is just human nature. Many operators simply rely on wishful thinking that goes something like this: "We haven't had an incident, therefore, we must be doing the right things." Well, not really. If you assume that not having been attacked or hacked means that you are doing enough, think again. You could just be lucky. Being lucky is great, but you should not rely on luck as a strategy. Talk to a professional gambler and they will tell you the same thing: eventually your luck runs out.

So how do you know the difference between luck and "doing the right things?" Ask yourselves the following questions. If you answer "no" or "don't know," then perhaps you should consider yourselves "lucky" and start taking a hard look at your cyber security posture and policies:

1. Do you regularly train your employees on cybersecurity best practices?
2. Do you have a comprehensive list of cyber assets?
3. Have you performed an operational risk assessment?
4. Have you performed a cybersecurity risk assessment?



Stage 1: Cyber Intrusion Preparation and Execution



Stage 2: CONTROL SYSTEM (CS) Attack Development And Execution

5. Have you implemented proper network segmentation?
6. Have you implemented end-point malware prevention and do you update the signatures on a daily basis?
7. Do you patch your systems on a regular basis (minimum quarterly, ideally monthly)?
8. Are you monitoring your system logs and network traffic?

9. Do you have a backup of all your assets such as switches, routers, firewalls, programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices (IEDs) and every other digital control asset with a configuration file?
10. If your system were compromised today, do you have a recovery and response plan ready?

If you answered "no" to one or more of these questions, you are not alone. Most control system owners do not employ this level of cybersecurity readiness. But, at a base level, if you do not have proper network segmentation, updated system software, end-point protection and hardened systems, then you are probably lucky that your system hasn't been compromised.

GETTING UP TO CYBER SPEED

When thinking about how to get started, don't just look for some new technology that claims to mitigate all your risks — it doesn't exist. Doing the basics well before investing in advanced cyber technologies is the key. To minimize your risks and get the most protection in the least amount of time, you first need to plan and develop a cybersecurity program that:

1. Identifies what assets you are trying to protect
2. Determines how you are going to protect those assets
3. Enables intrusion detection and monitoring
4. Defines incident response process and procedures
5. Verifies mechanisms to restore and recover assets

These five steps follow well-trodden ground. All of the security frameworks can be distilled into these basic steps: identify, protect, detect, respond, and recover.

For example, putting in a firewall to separate your control system from the corporate/business network is a great idea. But, if you don't have an inventory of critical assets and applications, you may still be vulnerable to risks from employees and contractors who use laptops and removable media. Developing strong security policies and practices and mapping out a 3-to-5 year journey that leads to security maturity is also highly recommended.

Some effective technology tactics to consider are hardened perimeters, adopting a defense-in-depth approach, whitelisting, investing in network intrusion prevention (IPS), air gapping control system, and security awareness training for all employees. Also, make sure to include specific contractual language about cybersecurity in your OT and control system requests for proposals (RFPs). To execute your plan, leverage your IT and OT teams, but also look for OT suppliers who can offer comprehensive cybersecurity services.

CONCLUSION

The list of things you should do to protect your operational technology is long and beyond the scope of this paper, but if you continue to do nothing, pretending that your systems are safe from attack, it is only a matter of time before you won't be pretending. Eventually, your luck will run out and maybe it will be your systems that go down this time, and your company that ends up in the headlines. ◻