WWW.CHEMICALPROCESSING.COM

CHEMICAL PROCESSING

LEADERSHIP | EXPERTISE | INNOVATION

CYBER SECURITY SPECIAL REPORT

Start ▶

Sponsored By

Honeywell

PutmanMedia®

We're Living in Interesting Times!

By Shawn Gold, Honeywell

"MAY YOU live in interesting times", often referred to as the Chinese curse, seems to be a good fit for where we have found ourselves over the past several years. The importance of server- and network-based IT solutions for automation systems has grown rapidly in recent years. Continually increasing technology capabilities – perhaps growing faster than we are able to adapt effectively – present us with ever increasing challenges.

The Information Technology (IT) organizations within most companies of any size are old hands with this evolutionary process, and their best practices have matured and improved over many years. That's not to say that IT professionals don't get surprised – particularly in the areas of network access and the perverse nature of cyber terrorists.

In the control systems environment, we enjoyed a more proprietary, protected environment and considered ourselves immune to security attacks, but the price we paid was in connectivity and information exchange in a timely and controlled manner. As we adopted more open technologies, much as our corporate IT organizations have done, we began to see many of the vulnerabilities associated with the introduction of these technologies. Basically, we have requirements that are quite similar to corporate IT organizations; however, an intrusion in a control system environment carries with it more opportunity for physical harm than is typical in the corporate environment. For this reason, we are now taking the view of an industrial IT approach for control systems.

If we step back and view where we are today with the application of information technology to control systems, we can make several observations:

1. It's no secret that there are increased accessibility requirements. Open technologies invite accessibility, and individuals and groups within the organization want access – to perform their own functions in a more timely and effective manner.

2. There is a tighter linkage between business and process information – associated here with point 1, above.

3. Many tools are available to address a single issue or group of issues. And, there are standards and best practices that have grown up around specific areas (like security), and for certain industries (like power).

4. Cyber threats come in many flavors – from those creating mischief (irritating) to those targeting specific industries with malicious intent (dangerous).

5. There is an increase in industry and government regulations and/or standards. The intentions of the groups generating these regulations/standards are positive; however, the time required to make significant progress is lengthy.

6. From a business perspective, most control systems are driven to provide increased uptime, availability and reliability.

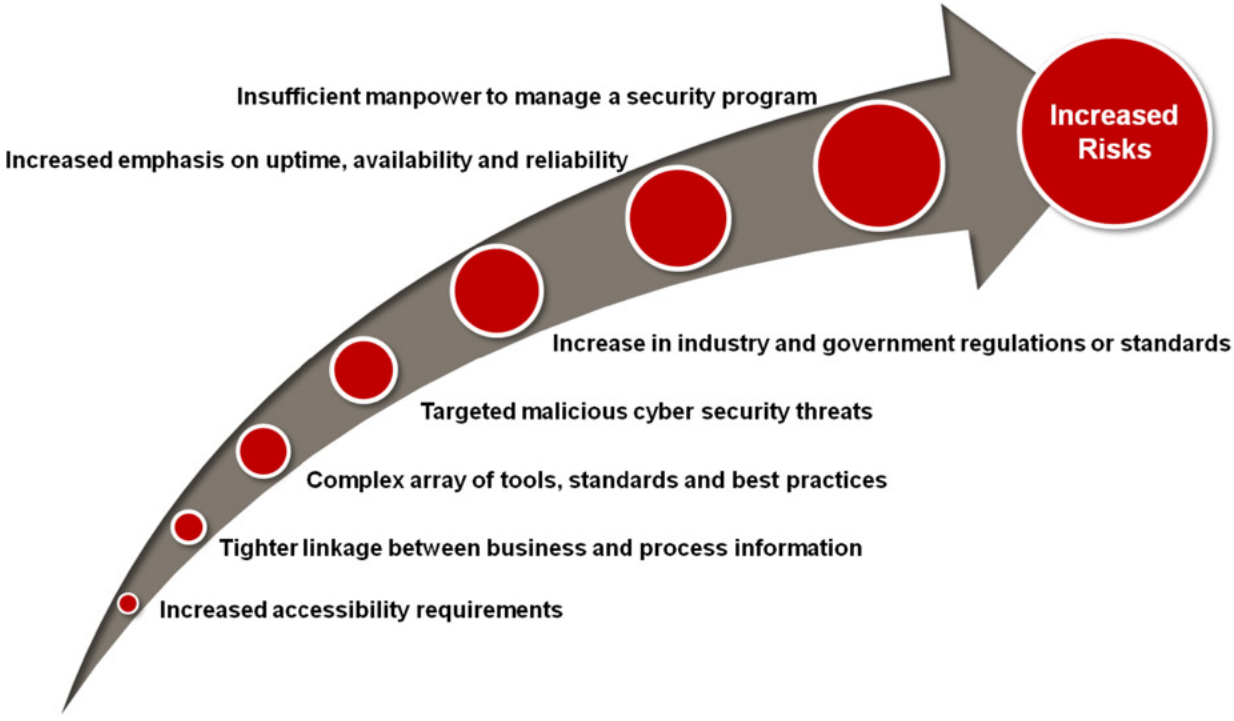
7. In general, there is a lack of IT know-how in the plant – with a view more to availability than confidentiality. Plus, there is insufficient manpower available in many organizations to manage a security program.

All of these points direct our attention to the realization that we are in an environment of increased risk. We can view the risks by type – internal, external, targeted, and non-targeted.

The most likely risk may be internal, non-targeted – for example, an employee inadvertently brings a virus or worm into the control environment using a USB memory stick – a kind of "sneakernet" intrusion.

Perhaps the worst situation is the external, targeted risk – the most hyped in the media and certainly the most dangerous. A recent example is Stuxnet -- designed to attack a specific industrial control system, proving that control systems are not immune to cyber attacks – by highly motivated parties directing the attack.

The Repository of Industrial Security Incidents



Industrial IT – Cyber Security Challenges

(RISI), which records cyber security incidents directly affecting SCADA and process control systems, shows the number of incidents increasing by approximately 20% per year over the last decade.

We have realized that control networks are not built to withstand traditional IT attack or protection methods. We are in a business environment that needs to minimize risk. If we have learned anything from our corporate IT organizations, we are beginning to realize that we need to take an approach that is based on a long-term, sustainable view of our future.

Just as corporate IT organizations have tackled the issues of providing a consistent, proven set of tools across multiple systems, we in the control systems environment need to adopt a similar approach.

Corporate IT organizations have learned that delivering information technology to their users is an ongoing process. And, that's a key point for us in the control systems environment – we need to understand that an area such as security is an ongoing program, not a project that has a defined completion date.

So, let's consider security from the perspective of an ongoing program. Where do you start? A phased model of the security lifecycle will help to clarify and give some ideas on where to start and how to continue.

- Assess your assets and vulnerabilities against industry standard and best practices.
- Remediate your network with a custom-designed security program.
- Manage your network security investment with services and training.
- Assure your security program is functioning as designed with compliance management.

…and continue the cycle!

Assessments help to determine where you are today in securing your critical infrastructure. You need a way to identify overall shortcomings and risk areas compared with a desired status. And, from that point, you would need to formulate and prioritize actionable recommendations focused on better system management. And, of course, you'll need to know how much it's going to cost, how long it's going to take, and how broad a scope you want to tackle initially. You may want to focus on one or more types of assessment, such as:

- Regulatory (NERC CIP, CFATS, etc.),
- Network (security, upgrades, outsourcing, monitoring, etc.),
- Gap analysis (risk and readiness, general best practices),
- Audit (based on a regulatory or corporate checklist).

Remediation is the next phase in the lifecycle – and it is perhaps the most robust in terms of

involvement, process definition and implementation. Realizing that the focus of this effort is overall risk management is key. Remediation is broad in its scope, involving people, process, and technology.

From a people perspective, a security awareness program will focus on helping each individual have a respect and basic understanding of the requirements and the potential impact of a security breach. This area includes security training, plus policy and governance development, and design and implementation resources.

Process includes procedural development for critical areas, such as patch management, secure remote access, anti-virus, backup and restore procedures, change management, and perimeter security.

Technology represents the choices for the network architecture, network topology (including diagrams of the process control network design), server and software (selection, deployment, and configuration), system hardening, and virtualization.

Depending upon the extent of the areas in need of adjustment, as determined in the assess phase of the lifecycle, the corresponding remediation phase can be quite involved. Depending on the severity of the assessment findings, the remediation may require immediate attention, while other areas may be managed over time. The prioritization of these adjustments will be very helpful in the remediation phase.

Manage focuses on the ongoing management of systems and technology and support. This phase is where you would see the implementation of workflow processes, attention to anti-virus and patch management, perimeter management, and testing and change management. Support would include regular tuning of security tools and system health and performance monitoring.

Assure focuses on compliance management and program monitoring. Compliance management ideally would provide an asset-based approach, with complete document management capabilities, including workflows to track document review and approval as per NERC CIP requirements, as an example. In addition, the compliance manager would include integration with Microsoft Windows cyber assets to track and document configuration and user information changes, the ability to integrate with other systems that hold compliance-related data (such as HR, LIMS, SIEM and log management). And finally, the compliance manager would provide accurate, reliable information readily available for audits and spot checks.

And, back to the assessment phase again – remember, it's an ongoing program – not a project! It is important to be as vendor neutral as possible in working through the lifecycle, taking advantage of network and security certified personnel.

Industrial IT helps to unite the best practices of traditional IT with the special requirements of process control systems – to protect and preserve security while delivering maximum performance. ■

SHAWN GOLD is the Vancouver, BC-based global solution leader of Honeywell's Industrial IT Solutions division. Email him at Shawn.Gold@ Honeywell.com.

Build Better Cyber Security

A three-step approach is key to enduring protection.

By Rick Kaun, Honeywell

CYBER SECURITY has received a big boost lately. Unfortunately, it wasn't the type of boost chemical makers were hoping to see.

A 2010 attack by malware dubbed Stuxnet that targeted control systems (see: "Industry Gets Cyber-Security Reality Check,") has thrust the concept of cyber security further into the spotlight of major concerns of manufacturers in the process industries and elsewhere. It has prompted many a chemical maker to ask:

Is my plant vulnerable to attack?

What if my facility is hit with the next version of Stuxnet?

Do we have the appropriate policies in place?

What about Chemical Facility Anti-Terrorism Standards (CFATS)? Are we in compliance?

In short, if a company wasn't already scrambling to research, create and implement an effective cyber-security program, Stuxnet certainly provided the impetus. It underscored that a strong cyber-security program is a necessity for manufacturers today.

Cyber security plays a crucial role in ensuring the reliability and robustness of the networks that a plant's critical applications run on. Implementing a baseline security model across a facility — whatever the industry — increases the likelihood of safe, dependable operations and minimizes potential security incidents. So, cyber security clearly is destined to become as entrenched in the process industries as a "safety culture" has over the last few decades. Like with safety (see: "Make Safety Second Nature"), chemical makers must achieve a cultural change. This requires not just a project but an ongoing program.

The prospect of doing anything — let alone running a cyber-security program — perpetually may seem overwhelming. However, this daunting task is achievable by breaking it into three key steps: inventory, integrate and implement (Figure 1).

INVENTORY ASSETS

The first step in developing any security program — physical, cyber, or both — is assessing a plant's current measures. In terms of cyber security, this means taking inventory of assets.

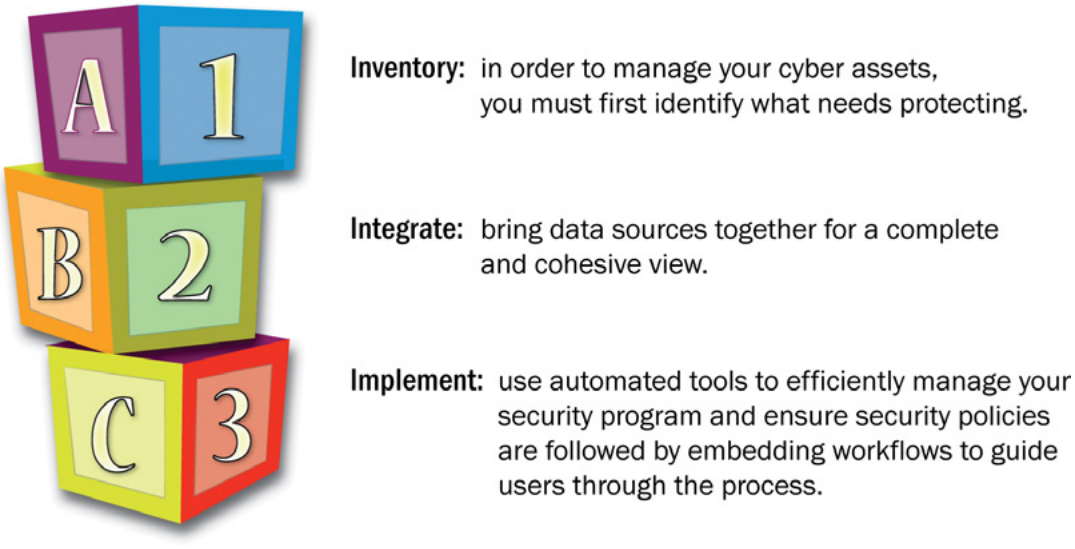
In industries where cyber-security regulations already are in place, operators must provide a list of their critical cyber assets. Getting started on an inventory immediately can help chemical makers ensure they're not left scrambling. CFATS doesn't explicitly call for such a list today — but may as its cyber component evolves.

A cyber inventory provides plants with the information needed to make informed decisions about cyber-security priorities. In addition, regulatory bodies require such an inventory for judging whether a facility is in compliance or not. Finally, a comprehensive asset inventory eases end-of-life planning, upgrades and long-term management of key safety or legacy process control and other systems. So, developing such an inventory is a great place to start.

Most facilities don't know precisely what's plugged in on the plant floor; it isn't always easy to determine. Managing compliance requires a robust inventory, including:

- IT inventory (operating systems, IP addresses, user permission levels, etc.);
- operational inventory (control systems and software, etc.);
- logical inventory (the network locations of assets);
- physical inventory (the real locations of assets); and
- security system inventory (what security solutions are in place, and where they sit).

Performing a physical inventory provides crucial insight into who has access to the asset; it also allows for a visual inspection of the asset, which can lead to important information that isn't available through other means. For example, have some assets on the plant floor been powered down or decommissioned? What about assets that aren't plugged in, or that have



Building Blocks
Figure 1. Three crucial steps underpin effective cyber security.

open ports, switches and modems that are supposed to be turned off when not in use? Does an asset have multiple network cards for accessing different network segments? Laboratory information management systems and centralized data historians are good examples of assets that often connect to multiple networks. Without a visual inspection it would be easy to miss this information, which is an important consideration for incident response plans and backup and restoration programs.

It also is essential to inventory existing security applications, including where they sit and how they function. Most facilities have at least a dozen isolated lists of information provided by various security applications or point solutions — for example, user security settings in Windows Active Directory, an inventory of critical systems in the backup system, anti-virus, intrusion-detection and patch-management applications, network access rules and controls (acceptable paths, what machine can connect to which network), and various sets of documentation ranging from policies to procedures to checklists and technical standards.

A detailed cyber inventory underpins many of the subsequent steps in creating a best-practices compliance program, such as identifying and addressing vulnerabilities and establishing mitigation and remediation plans. The more accurate and complete an inventory, the easier it will be to make thoughtful decisions about a security program, including understanding the impact on operations of rollout of, say, an anti-virus application.

INTEGRATE DATA SOURCES

Once the inventory has been completed, the challenge is tying this information together for a holistic view of the plant's cyber assets. There's no sense in pulling all these data from the various areas and duplicating them in a separate database (doing so would create an information management nightmare). The alternative is to compile a "master list" of all information sources in a facility with links to the supporting data and underlying information. This higher-order database is similar in function to a site map for a complex website, and is really a logical model of a facility. Most plants likely can generate it from the inventories they've already completed. This master list enables sites to keep tabs on their critical information, provided processes are in place to ensure it's kept up to date.

A key aspect of managing a security program is integrating all security data sources and making that information accessible and actionable.

Take the example of an access request. Whether the request is for electronic or physical access, most facilities today would need to go to a host of spreadsheets to cross-reference the user name against training records, electronic access clearance level, and even background or clearance checks. The bits and pieces of the information plants need to determine whether to grant the request reside in various data sources, formatted differently in each. Now imagine a single interface able to display a user and list his or her specific clearances, training and certifications taken (with time stamps).

Tools to automatically monitor and manage the security program as well as document changes are essential to a robust security management program. A tool that interfaces with best-in-class security software, e.g., for protection against viruses, patch management or backup/virtualization, can provide immense value in managing a plant's data and security program — if

it's set up right, that is. A recommended approach is to implement a database with front-end portal capabilities for viewing relationships and interdependencies and reporting on them.

IMPLEMENT WORKFLOWS

The third fundamental aspect of a successful security program is the ability to keep it up to date (and fully documented). The longer plants manage the program, the more difficult and more important this becomes. As many managers can testify, the average employee can become complacent over time. Usually the first areas to suffer are administrative or seemingly unimportant recording and tracking tasks. To combat such lapses, it's imperative to establish and regularly review workflows. Done properly, they guide personnel through each stage and proof point, embedding procedural and policy objectives into day-to-day tasks and providing some form of verification or documentation. Such workflows can play a crucial role in ensuring proper management, maximum security and getting the most value from security spending, while minimizing the "people" risk factor.

In essence, specific workflows reflect the application of corporate or regulatory policies and procedures. One simple example involves ensuring new employees are granted access to critical systems based on relevant clearances and certifications spelled out in various programs such as CFATS, the Transportation Worker Identification Credential, etc.

Let's take a closer look at the request-for-access example. By extending the framework to include training and personnel data, plants can add a workflow to manage and automate such requests.

The application could submit the user name to a process that grants user access to specific workgroups or roles within the facility. If the role and clearance required already are defined, the application now can manage — automatically and without error — whether or not to grant access.

Further, workflows can monitor the time stamps associated with various clearances, training and certifications, automatically notifying users when these are about to expire. Similarly, removing users who no longer require access (due to employment termination or retirement, for example) from all information systems becomes simple, either by providing a comprehensive report or by automatically disabling accounts. A plant also can apply automated workflows and management of information to log review, patch evaluation and deployment, general change management, etc.

To the extent possible, all policies and behaviors should have a corresponding workflow with some form of verification or documentation. This can range from a simple key sign-in/sign-out sheet to a full-fledged change-management regimen for patch evaluation or upgrades.

To properly reflect an organization's policies and procedures, workflows must be dynamic. If, for example, an application upgrade is high risk due to the systems involved, the workflow must manage additional levels of approval and consultation. A dynamic workflow should accommodate reassessment, extra information, and reassignment of tasks or reporting. Of course, it also must capture any and all additional actions taken. This is especially true for key process control and safety instrumented systems, etc., that are critical to safe and reliable plant operation.

An additional necessary aspect of workflow is the ability to tie the changes and reports back to the

systems to verify the data. If a user can mark a task or change complete without having done it and this isn't caught, the omission may go unnoticed. So, a loop-back mechanism, whether electronic or manual, is an important element of any workflow tool.

Implementation using electronic tools essentially involves embedding specific reporting and tasks into a step-by-step workflow that then verifies the particulars against the end-system data, effectively enforcing the policy. In turn, this ensures consistency of reporting, content and workflow across different people, shifts and locations within the organization. As an added bonus, the plant gains an effective change-management tool. If the system is hooked into existing corporate communication tools like instant messaging or Active Directory (for access review, revocation, control, etc.), the processor has the building blocks of a dynamic security-management program.

CHANGING THE CULTURE

The three-step process of creating/managing cyber inventories, integrating data sources and implementing workflows essentially forms a blueprint for establishing a strong cyber-security program.

But one crucial element — corporate culture — ultimately will determine whether this program is maintained effectively. A successful security program depends upon ongoing buy-in by people at all levels in an organization.

In light of the unrelenting move toward increased regulation, putting off implementing cyber security really is just postponing the inevitable. And delay can have serious repercussions for the success and cost of a security program.

In the chemical industry, it's fair to say that physical security now matches worker safety in priority. In the U.S., CFATS certainly has spurred increased emphasis on effective physical security measures. Cyber security, though, is a different story. Often, it falls below other priorities such as alarm management, process improvement and environmental controls.

Processors must think beyond the mechanics of compliance and realize that cyber security really is about ensuring safe, reliable and expected system behavior.

And chemical makers, like manufacturers in all industries, must view cyber security exactly the way they do safety — as a permanent program, not just as technologies that are part of a finite project. ■

RICK KAUN is the Edmonton, AB-based manager of Honeywell's Industrial IT Solutions division. Email him at Rick.Kaun@Honeywell.com.

Industry Gets Cyber-Security Reality Check

Stuxnet attack points up vulnerabilities of control systems.

By Seán Ottewell, Editor at Large

IN EARLY March the Security Incidents Organization (SIO), Sellersville, Pa., released its annual report on industrial control system (ICS) malware incidents. "This report shows the details of the continuing threats to manufacturing and infrastructure security around the world. As the Stuxnet malware showed in 2010, the threat continues and has become even more complicated and mature," says SIO executive director John Cusimano.

The emergence of the Stuxnet worm, which apparently targeted Siemens control systems at an Iranian nuclear-enrichment facility, certainly exposed serious knowledge gaps in how cyber security is implemented and maintained by process companies.

A new white paper, "How Stuxnet Spreads -- A Study of Infection Paths in Best Practice Systems," aims to help bridge those gaps. Published in late Feburary, it's co-authored by a trio of cyber-security experts: Eric Byres, chief technology officer, Byers Security, Lantzville, BC; Andrew Ginter, chief technology officer, Abterra Technologies, Calgary, AB; and Joel Langill, chief security officer, SCADAhacker.com, Lantana, TX.

The authors describe a hypothetical industrial site that follows the high security architecture and best practices defined in vendor documents. They then show the ways the Stuxnet worm could make its way through the site's defenses to take control of the process and cause physical damage.

While speculation continues as to the creators of Stuxnet, the worm underscores that ICSs now are the target of sophisticated attacks, note the authors, who add that owners and operators must adjust their security programs accordingly. In particular, stress Byers, Ginter and Langill, security programs must:

- Consider all possible infection pathways and have strategies for mitigating those pathways rather than focusing on a single pathway such as USB keys;
- Recognize that no protective security posture is perfect and take steps to aggressively segment control networks to limit the consequences of an incursion;
- Install ICS-appropriate intrusion detection technologies to spot attacks and raise an alarm

when equipment is compromised or at risk of compromise;

- Deploy, operate and maintain at maximum effectiveness ICS-appropriate security technologies and practices. These include firewalls, antivirus technology, patching systems and whitelisting designed for supervisory control and data acquisition (SCADA) and ICS, to make attacks by sophisticated malware much more difficult;
- Look beyond traditional network-layer firewalls to firewalls capable of deep packet inspection of key SCADA and ICS protocols;
- Focus on securing last-line-of-defense critical systems, particularly safety integrated systems (SISs);
- Include security assessments and testing as part of the system-development and periodic maintenance processes followed by correction of identified potential vulnerabilities, thereby decreasing the likelihood of a successful attack, and;
- Work to improve the culture of industrial security among management and technical teams.

"These changes to improve defense-in-depth postures for industrial control systems are needed urgently. Waiting for the next worm may be too late," they say.

CHANGES NEEDED

Byers highlights two requirements in particular as being essential. The first is culture: "On the macro level you need upper management to really develop a security culture: enthusiastic engineers are not enough."

He points to the safety culture that has emerged in the chemical industry over the last 20 years as a model for how this could happen. "Security needs to follow along the same lines now: it must become a top-to-bottom culture with programs that are both technical and procedural. Nothing works unless this is in place first."

BP, Exxon and Shell in the oil and gas sectors and Dow and DuPont in chemicals exemplify how a safety culture can become a security culture, he says. "The management of these companies really understands the security challenge because they already have sophisticated risk-management cultures. So they have concepts in place that allow them to measure and predict risks far better than other companies."

Byers also cites the findings of a major oil company that recently evaluated the risks and consequences on an offshore oil platform associated with a serious fire versus those of a cyber attack. It determined they were almost identical in terms of cost and loss of life. Yet, the company was spending $50 million/yr on platform fire suppression but only $1million/yr on cyber security. "This spend was instantly increased. This is a level of risk sophistication that is lacking in many other companies."

Such a lack of sophistication was evident at a distributed control system (DCS) vendor's users' conference he attended shortly after Stuxnet appeared last June. While delighted to see operating company managers there treating malware as a serious problem, he was shocked that one proposed solution involved filling USB ports with silicone. "I realized how badly these people were missing the point. Use as much silicone as you like, it won't make any difference. The next attack will come via a pdf or some other source."

Byers' second priority is to firewall-off mission critical systems such as safety ones. "Remember that Stuxnet only had to attack one system because both control and safety were bundled together in the

system it infected -- all the eggs were in one basket," he cautions.

Once the low-hanging fruit such as safety systems have been tackled, you must start to work back. "You need what I call multiple prongs: the people and their culture; then mission critical systems; then standards. The new ANSI/ISA-99 and IEC 62443 standards are concerned with dividing plants into different security zones, so that no worm gets a free rein."

STEPS TOWARD SOLUTIONS

Byers emphasizes that the white paper really focuses on problems rather than solutions. However, a number of papers on solutions currently are being developed.

The first concerns OPC and related protocols for open connectivity. With input from Matrikon (now part of Honeywell), Edmonton, AB, the paper will propose solutions to ensure that OPC gets through but a worm cannot, says Byers. It is due to be published this month.

The second paper involves work with an as-yet-unnamed software company to help operating companies better understand network traffic on the plant floor. "Most companies suffer from a lack of visibility about what is going on in their networks. If people had been watching the network that Stuxnet infected they would have seen all sorts of new traffic: pieces of equipment talking to each other that had never done so in the past, for example." This paper is due to appear in the spring.

Also due out then is a third paper, on managing Modbus traffic. By creating deep-packet-inspection capabilities for firewalls that look inside Modbus messages, Byers says users will get very fine-grained control over exactly what they want a human/machine interface or workstation to be able to do over the network to a DCS, programmable logic controller (PLC) or safety integrated system (SIS). He cites the new Honeywell Modbus read-only firewall for SIS (see www.tofinosecurity.com/article/honeywell-selects-tofino%E2%84%A2-modbus-read-only-firewall-secure-critical-safety-systems) as an example of this.

Meanwhile, Rick Kaun, Matrikon's manager, industrial security and compliance, warns of a future fraught with risk. "Stuxnet proves the concepts of: (1) targeted attacks, on (2) control systems using (3) zero day exploits [those in which there's no time between when the vulnerability is discovered and the attack]. Add to this the recent revelation of Chinese hackers infiltrating oil and gas companies and the release of Stuxnet code to the public and you have a whole heap of potential risk. A perfect storm is coming."

Like Byers, he believes cyber security must be treated as an everyday plant issue -- just like safety. "Security isn't about being bulletproof. It's about operating facilities in a safe and secure way. So security needs to have the same philosophy or culture as safety. Security is about how quickly you can detect, contain, recover and learn lessons from an incident."

The U.S. chemical industry is giving increased attention to security because of the Chemical Facility Anti-Terrorism Standards (CFATS). However, Kaun feels a lack of emphasis on cyber security in CFATS has led to an overly strong focus on managing physical security. "There are notable exceptions, but still many in the sector have focused almost 100% on physical security and have done little or nothing yet with cyber security."

Matrikon's cyber-security philosophy has three aspects: people, process and technology. "You must

address all three to be secure -- and people is the toughest one to nail down," says Kaun.

To show how challenging this can be, he cites the example of a security firm that went back to check on how a client was implementing a new and very rigorous cyber-security program. The security firm left a selection of USB sticks containing hidden data mining tools around the client's parking lot, reception area and cafeteria. "Within a day the tools were on the network. It's human nature to pick a USB up and plug it in. So if a customer doesn't really get what it's trying to do -- and enforce it -- then it is dead in the water," he warns.

He also points out that if the authors of Stuxnet hadn't used a USB stick as a key method of distribution, the attack would likely have taken much longer to detect. Siemens' web-based Simatic security update still is advising against use of any USB sticks or other mobile data carriers (Figure 1).

Cyber threats are impacting how Matrikon does business. For example, the internal risk-assessment group at one major industrial client has called in the company to assess the cyber security of specific control systems and networks. Matrikon is doing this through a combination of interviews, document reviews, physical login/inspections and control penetration testing. Using a system of likelihood and impact findings, Matrikon then will be able to provide a priority list for remediation.

This sort of assessment also appears as a new trend within Matrikon's own cyber-security projects. The last three customers all have requested that Matrikon return to assess whether their new security measures have been implemented properly and are being run effectively. "People are much more concerned now to know that everything is working properly. And this is important because, for example, a customer might have left the firewall ports open to conduct a vibration analysis and forgotten how to lock them down again," he says.

Figure 1. Web-based security updates recommend a range of actions including not using USB sticks. *Source: Siemens.*

For chemical operators overall, Kaun emphasizes two basic vulnerabilities that must be tackled to improve cyber security: awareness and enforcement.

BETTER STANDARDS

In early March, the International Society of Automation (ISA), Reseach Triangle Park, NC, announced that its ISA99 standards committee on industrial automation and control systems security has formed a group to conduct a gap analysis of the current ANSI/ISA99 standards with respect to the rapidly evolving threat landscape.

The purpose is to determine if companies following the ISA99 standards would have been protected from such sophisticated attacks and to identify needed changes, if any, to the standards being developed by

the committee. A technical report summarizing the results of the group's analysis may come out by mid-2011.

Last November, the International Instrument Users' Association, The Hague, The Netherlands, launched Version 2 of its "Process Control Domain Security Requirements for Vendors," which it calls the first international standard that outlines a set of specific stipulations focusing on cyber-security best practices for suppliers of industrial automation and control systems.

Led by major companies such as BP, Dow, DuPont, Saudi Aramco and Shell, dozens of other end-users, as well as leading vendors such as Invensys and multiple government agencies, the group spent two years developing and piloting the program that culminated in Version 2.

"Not only do the requirements provide current-state measures, they allow us to continue to improve and adapt to the ever-changing security landscape. From our perspective, this program is a major shift, not only focusing on tactics, but one that puts into place strategic elements that address operational change," says Ernie Rakaczky, portfolio program manager control systems -- cyber security for Invensys Operations Management, Dollard-des-Ormeaux, QC.

"This document provides the common language we need to communicate our expectations around security to our suppliers and the framework to work together to help improve the overall security posture for our critical systems," adds Peter Kwaspen, strategy and development manager, EMEA control and automation systems at Shell Projects & Technology, The Hague, The Netherlands.

"We've now come to a truly functional cyber-security standard based on the needs of end-users and it is now up to us, the end-user, to take advantage of this effort and insist that our vendors are certified," stresses Jos Menting, cyber-security advisor with GDF Suez Group, Paris. ■

SEÁN OTTEWELL is Chemical Processing's Editor at Large. You can e-mail him at sottewell@putman.net.

detect threats

Threats can be deceptive.

Cyber security is a critical issue for our industries, and finding a manageable response to security is difficult, especially with the myriad of technical solutions and false prophets offering bulletproof security tools. Honeywell's Industrial IT Solutions can help protect your process control network by providing DCS-independent, unmatched expertise and services to give you scalable, affordable security solutions across the security lifecycle. As a trusted advisor to our clients, we have solutions that not only detect and avoid immediate threats but also help manage security while meeting production, uptime and regulatory requirements.
Don't get the wool pulled over your eyes.

Honeywell

For more information on Honeywell's cyber security solutions, visit **BeCyberSecure.com**.

PREVIOUS PAGE