Securing Industrial Control Systems in the Chemical Sector

Roadmap Awareness Initiative – Making the Business Case

Developed by the Chemical Sector Coordinating Council in partnership with
The U.S. Department of Homeland Security
November, 2012

Through the Chemical Sector Coordinating Council, the chemical industry is working in partnership with the Department of Homeland Security to address industrial control system (ICS) security. Government and industry partners alike recognize that the justification for ICS security improvement and enhancement starts with developing a business case that explores the financial risks and consequences of a cyber event[1]. While a detailed business case is beyond the scope of this document, below is a plausible scenario of the consequences that a company may suffer should control systems be improperly secured.

What Is the Impact to Business?

Chemical companies are not immune from cyber attacks. Both targeted and non-targeted attacks can cost companies millions of dollars in lost business and proprietary information. Yet many companies are woefully unprepared when it comes to protecting their industrial control systems from viruses and other cyber intrusions. Is your company one of them? Read the fictional but realistic testimonial below and ask yourself, "Could this happen to my company?"

> **Cyber Incident Testimonial**
>
> I work at a medium-sized specialty chemical manufacturer developing a variety of proprietary materials for individual customers. We develop specialty chemicals using our unique array of high pressure, glass-lined, and solids handling and distillation equipment. Processes typically require toxic and corrosive materials, as well as those that are air and moisture sensitive. Most of the specialty chemicals are difficult to synthesize and are developed only upon customer request for just-in-time delivery. Pricing and availability are highly variable.
>
> On the security side, we take advantage of many resources from the government and industry to stay on top of threats to our process control systems. We noticed a United States–Computer Emergency Readiness Team (US-CERT) alert that indicated a few new exploit tools had been released that specifically target programmable logic controllers (PLCs) supplied by the major manufacturers. One tool targets the Ethernet/IP protocol deployed by numerous PLC vendors. The payloads can affect any device that uses the protocol, allowing attackers to crash or restart affected devices. We employ a number of these devices, and our entire internal corporate network uses Ethernet connections. Additionally, our ICS devices do not directly connect to our corporate network; they are located behind a process control firewall for security protection. This greatly reduces exposure for ICS incidents. If remote access is necessary, we use Virtual Private Networks (VPNs) to do so, and we have strong password and account lockout policies in place as well as monitoring of administrator-level accounts by all of

[1] For a more detailed discussion on creating a cyberecurity business case, refer to the *Cross-Sector Roadmap for Cybersecurity of Control Systems*, Sponsored by DHS and the Industrial Control Systems Roadmap Working Group, September, 2011, http://www.us-cert.gov/control_systems/pdf/Cross-Sector_Roadmap_9-30.pdf.

our third-party vendors. However, given the nature of this ICS threat, we felt compelled to perform system-wide updates and install operating system patches on all of our ICS computers.

We noticed some problems with a patch that would not install properly on one machine and asked for assistance from our ICS vendor. We have worked with this vendor for several years and they have a deep knowledge and understanding of our system. Our regular support engineer, John, informed us he would need to log-in at the system administrator level in order to identify the problem and troubleshoot the device. We made arrangements to allow John remote access for a limited time, after which one of our IT staff members was instructed to close the connection. After several hours of removing and reinstalling several patches, the vendor was finally able to get the software patch to load properly, and we got ready to resume production.

While the system was down in order to install the new patches, we received an order for a specialty chemical from a relatively new customer. Although it would be a challenge to meet the new customer's delivery date, we felt we could do so without missing any ship dates to our existing customers. Unfortunately, midway through the production process for this new customer, we started having problems maintaining the temperature and pressure required for the chemical reaction. Upon completion of the batch, Quality Control indicated that the physical properties were outside the tight specification required by this customer. We quickly halted production, and began to systematically troubleshoot the problem.

We diverted the off-spec product to the proper waste collection stream and re-cleaned and re-sterilized our equipment per our standard operating procedures. The operators and equipment maintenance mechanics conducted a thorough check of all hardware and electrical connections to make sure that none of the electrical heaters were burnt out. The equipment seemed to be functioning normally. Having lost nearly two shifts worth of production time, we resumed production to meet the tight delivery schedule.

The process seemed to be running properly during the early reaction steps; however, the control room operator noticed some sluggishness calling up alarm displays and silencing the audible alarm warning that the temperature was dropping off in the reactor just as the reaction required additional heat. Further examination indicated that the booster heaters were not cycling properly to sustain the reaction temperature. Overall, the control system seemed slow responding to operator commands.

We contacted our ICS vendor and requested John's assistance in tracking down the problem. John noticed that the error logs on our operator stations indicated abnormally high central processing unit (CPU) utilization levels, indicating the process control network was saturated. The advanced control programs running on the batch server appeared to be stalled, because the controllers were not responding. Further analysis revealed an unknown process running on these computers that was consuming high levels of CPU time and memory. Internet searches revealed that this was a recently detected malware program for which the anti-virus vendor had released a virus signature update file the day before. This update file had not been installed during the chaos of dealing with delayed production startup after the patching problem and then the process problems with off-spec material.

John researched the problem with the anti-virus vendor and consulted the US-CERT Web site to see if there was any guidance and suggestions for mitigation. It was determined that the only safe way to get rid of the malware was to re-image our entire system, so no traces would remain and the chance of re-infection minimized. At this point, nearly 48 hours had passed since our first problem surfaced. Luckily, our company has a comprehensive disaster recovery plan that requires us to create an image of our system on a regular basis or when there are major changes made to the system. We re-imaged the first ICS computer and made a back-up copy of the infected system to aid in the subsequent investigation.

This was our worst-case scenario. We had to call our new customer and tell them their order would be delayed. Our production lines typically gross tens of thousands of dollars per day. The combined opportunity loss and cost of working our staff around the clock to rectify the measure would reach the six-digit range. This cost doesn't even take into account the loss of consumer confidence and embarrassment after our other customers heard what happened.

At this point we were still left wondering where the malware originated. Once we confirmed the presence of malware, we reviewed the logs from the back-up image we made to determine the last administrator level log-in before our problem surfaced. We determined the last person to log-in was John when he helped us with the difficult patch installation. We asked him to check his system for the malware. With John's help, we concluded a virus was introduced into our system from his computer. The vendor eventually traced the virus to a computer system John worked on immediately before working on our system.

Our company learned a couple of tough lessons. We were glad we had a management of change policy in place to help us troubleshoot the problem and confirm how the malware infected our systems, but we had to re-learn that we must continuously monitor our cybersecurity program—not just the technical components, but the human component as well.

Our corporate policy requires each facility to have a disaster recovery plan directing us to image our control systems on a regular basis. This requirement saved us valuable time enabling us to get back on-line much faster than we would have otherwise. The image back-up, which is also required in situations like this,

> will be immensely valuable to the investigators we will be working with to dissect the malware.
>
> While we considered our vendor a trusted vendor, it is our responsibility to verify that trust. We must work with our vendors to understand how their systems work. We are planning to visit their offices to make sure they provide secure, remote support when we need it, but we also plan to work with them to develop processes that increase security for both companies.

Could This Happen to My Company?

This scenario is one of many possible scenarios illustrating the consequences and business costs of compromised control systems. Most companies are familiar with advanced persistent threat activity and the threat this poses to proprietary data and intellectual property. In contrast, the scenario outlined here is a non-targeted attack that could happen to any company, irrespective of company size. Loss of control system integrity due to cyber attacks is on the rise, suggesting that the probability of successful attacks on companies increases every year.

The availability of open-source computer search engines such as SHODAN, WireShark, or MetaExploit, makes the world a more dangerous place for control systems. These tools allow hackers to find Internet-facing supervisory control and data systems (SCADA) that use potentially insecure mechanisms for authentication and authorization. Vulnerable systems can include control system interfaces designed to provide remote access for monitoring system status,[2] as illustrated in the testimonial above. Cyber hackers might also use these tools on smaller control systems for reconnaissance purposes before attacking higher-profile, more complicated control systems.[3] In addition, protocols and software that were once proprietary are now open-source, making it even easier for hackers to attack some targets.

Relying on security of ICS through obscurity no longer holds true. Thanks to international headlines covering the Stuxnet virus, control systems have higher visibility than ever, and new search tools make it easier than ever for hackers to find systems that are connected to the Internet.

What Can I Do?

The chemical industry must work together to ensure that a control systems security breach does not occur. This requires increasing awareness, education, and communication between the engineering, security, information technology, process safety, and manufacturing operations communities. The ultimate responsibility for ensuring a secure ICS environment lies with the owner/operator. Look through the information provided, bring it to your company management, ask key questions about how your company is addressing ICS security, and become an advocate in your company on this important issue!

Companies should do the following:

[2] ICS-ALERT-10-301-01 – Control System Internet Accessibility. Alert can be downloaded at: http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf

[3] Cyber Warfare and the Control Systems Community: What Must the Control Systems Community Do to Adapt to the Threat of Cyber Warfare?, Robert M. Lee, http://www.controlglobal.com/articles/2011/cyber-warfare-control-systems-community.html.

- Ensure one person takes ownership of ICS security and is accountable.

- Open the lines of communication between engineering, security, IT, process safety communities, and manufacturing operations communities within your own company.

- Conduct an audit of current ICS security measures and implement obvious fixes.

- Follow up with an ICS security vulnerability analysis (risk assessment) for a complete identification of vulnerabilities and recommendations for corrective action.

- Implement an ICS security management program that is integrated with existing company management systems for security, safety, quality, etc.

- Email chemicalsector@dhs.gov for more information.