GRANTEK

Cybersecurity Challenges Facing Manufacturers:

Can Your Facility Go Beyond Compliance To Withstand Today's Threats?

The days of manufacturers avoiding cyberattack through isolating production systems from corporate systems and even the internet, are over. Convenience and efficiencies are achieved by networking production systems, which were formerly part of a closed environment, with a facility's business systems. Doing so, however, increases the risk of cyberattacks which not only compromise data, but threaten the bottom line.

Advantages of Working with a Systems Integrator

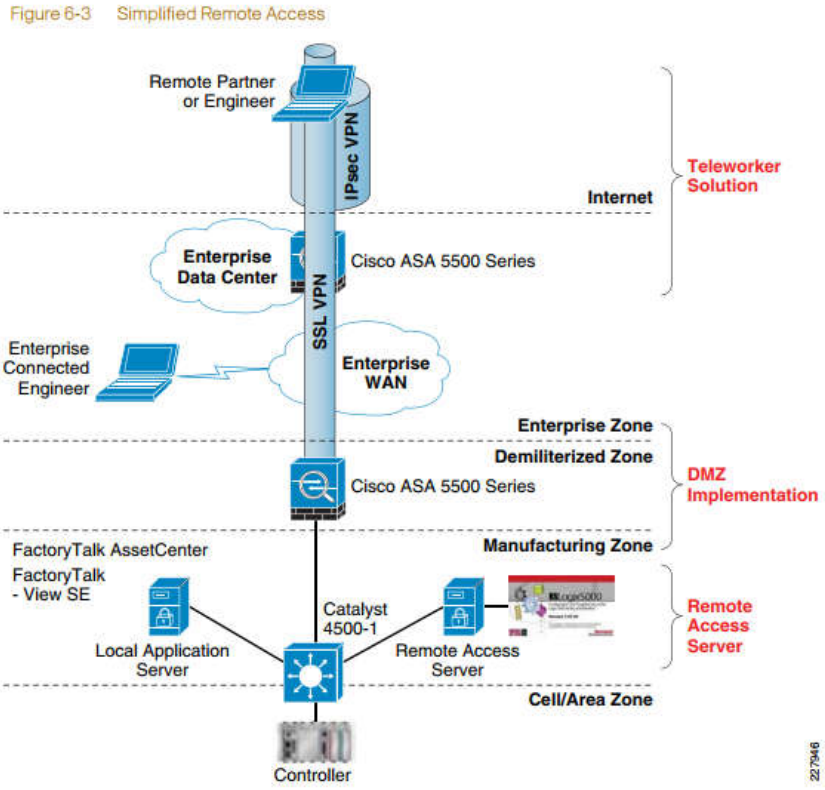
Compared to other cybersecurity analysts, a systems integrator with experience and recognized expertise uniquely positions a company like Grantek to perform cybersecurity assessments and recommendations for manufacturing facilities. Grantek has in-depth knowledge of potential gaps and vulnerabilities in manufacturing systems that most IT and network analysts have little familiarity with. In many ways, manufacturing systems differ from the usual IT networks and business systems that are most often targeted by malicious actors. A manufacturing system may have Programmable Logic Controllers (PLCs) and other control systems that are 20 or more years old and were designed with no security protection in mind. These once-isolated devices may now be remotely accessible as production systems are integrated with business or monitoring systems on the manufacturer's internal network, or in the cloud.

Grantek's knowledge of production systems and manufacturing equipment, in addition to our cybersecurity expertise, allows us to develop and implement cybersecurity methodologies in accordance with the "defense in depth" approach recommended by the International Society for Automation (ISA). This approach covers all vulnerabilities, including physical plant security and available emergency response capability, in addition to network security. Other cybersecurity companies tend to focus on IT and business systems and may not have the manufacturing knowledge Grantek offers.

Grantek applies the Defense in Depth approach that helps prevent cyberattacks, viruses and worms from spreading by segregating systems into other zones. We factor cybersecurity into every project as

part of our general methodology. We perform assessments of facility infrastructure and systems connectivity, for the Industrial Control Systems (ICS) network and the enterprise network, making recommendations to minimize risk of potential intrusions. Typically, our cybersecurity experts work as part of the Grantek team when an expansion or integration project is initiated. We provide recommendations for maintaining the security of the new equipment or systems and how to integrate them at the enterprise level, without compromising security.

Grantek helps our clients develop proactive plans to prevent or minimize the impact of attacks by as-yet unknown threats. Our Test and Security groups can develop strategies to test the company's ability to withstand attack and the ability to respond, isolate, and recover from attack. We help companies find vulnerabilities before attackers do.



Because we are a systems integrator, Grantek can effectively assess the vulnerabilities of an ICS network. Even if a company has disparate networks, or little Ethernet infrastructure today, it is likely

that they are quickly developing migration plans from legacy protocols and islands to meet the demands of increased connectivity and replacing legacy equipment. We assess the ICS components and their connections to other company systems such as Enterprise Resource Planning (ERP). As part of an integration project Grantek assesses all systems to help ensure end-to-end security, scalability and access.

The nature of manufacturing expansions, which often result in “organically grown” networking constructed on an ad-hoc basis, can open the door to cyberattack. The control systems running the production equipment are typically installed as a closed system not connected to Ethernet, and often lack basic security measures.

Manufacturing controls sometimes utilize proprietary protocols that inherently protect them from attack. In the connected environment of the 21st century, any device with an IP address poses a risk. Formerly closed systems are now exposed and must be protected to help prevent costly shutdowns or defective products and recalls. Plant engineers who are experts at programming and installing PLCs may not give adequate consideration to the additional risks created by placing these once-isolated devices onto the IP network.

The proliferation of wireless networking and the Internet of Things (IoT), where devices may transmit data unbeknownst to the user if not configured properly, demands that all devices, even PLCs, HMI (Human Machine Interface) systems, printers, and building monitoring sensors must be protected from unauthorized access, as access to one may allow access to all. Grantek’s longtime expertise with production control systems makes us ideally suited to help decrease the risk from a company’s network, from the oldest PLC-driven machines to the top-level enterprise network exposed to the internet.

Security Maintenance: Patching

Once an integration project is complete, Grantek has a thorough understanding of our client’s

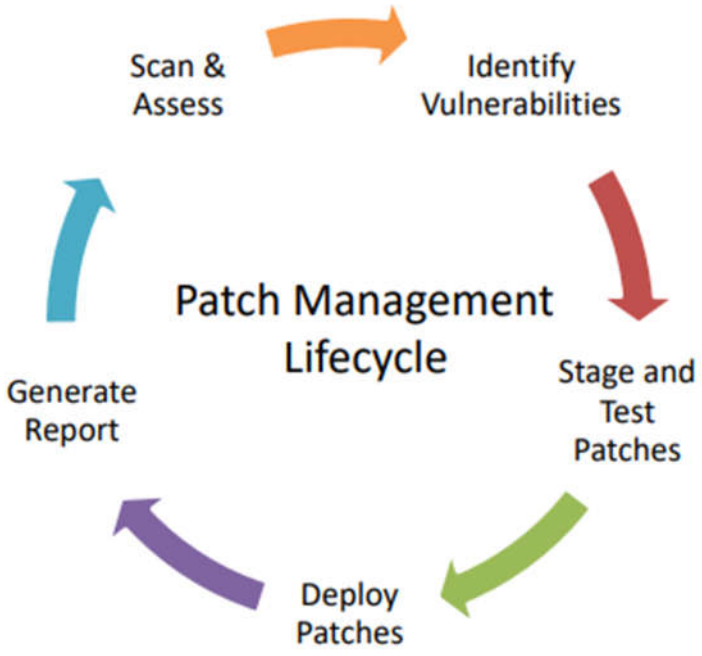
production system. Grantek's Service and Support group can develop and maintain system patching regimens to keep antivirus software up to date and maintain the latest security enhancements to the operating system software. For the Pharmaceutical industry, it is critical to work with validation teams and regulatory bodies to provide a safe, current and stable validated environment. Today, the FDA generally considers patches to be non-functional changes that can be made without revalidation.

Our support team can implement a program of scheduled and tested antivirus and OS patch installation to minimize system disruption, but we can also complete immediate application of critical patches – with the appropriate support, testing and rollback policies to ensure system uptime. We strive to work with our clients to develop a Security Maintenance Program that minimizes downtime and the risk of unexpected consequences of patch installation. Typically, Grantek can test the patches in-house or at a test site to ensure they don't break existing software before rolling patches out across customers' systems.

For antivirus and security patching to be effective and efficient, updates must be tested on a control structure to ensure compatibility. Grantek's Service and Support team can test patches as they come out, and then install them at a predetermined time that minimizes disruption. Grantek's team routinely monitors ICS-CERT alerts and is well poised to advise customers on the risk and potential impact to their specific systems, firmware versions, and implementations.

For facilities that wish to handle antivirus and patch maintenance internally, we offer instructions and guidance to help maintain security. As an integrator, we can also help maintain controller firmware updates. Our approach is to augment, not replace, our clients' capability to ensure they are receiving best in class support and minimizing risk in the most cost-effective manner.

We can push antivirus updates and OS patches to networks remotely or provide on-site installation. Alternatively, the client's IT group can stage the patches and ready them for deployment, and at preplanned intervals, Grantek ensures all required patches have been downloaded and are available for installation at the facility, then deploys them.



Maintainers of systems unique to manufacturing sometimes opt out of receiving patches as they fear unexpected impact on production systems, or the need for revalidation testing. Our experience with production systems gives us the knowledge to test patches for compatibility with production applications and systems, to help prevent surprises when the patches are rolled out to the customer's equipment. If we find a problem, we can exclude patches that are incompatible with control systems, or that may fix a critical security flaw but cause other issues as they may not have been adequately tested by the vendor on all system types. These findings can then be reported and evaluated with the client to ensure both compliance and continued system uptime.

Security Maintenance: Backups

Another component of a robust security program is maintaining current, complete backups. Companies often install backup software tools and then fail to ensure the backups are taking place at appropriate intervals and producing valid backup files. After a failure, they then discover the backups they were relying on for recovery are not current or even usable -the data is lost. Consider the number

of PCs in a facility, and recovery becomes very costly. Grantek helps companies develop and maintain a backup program that is effective and appropriate, minimizing disaster recovery time if a failure or cyberattack takes assets out of production.

How Grantek can help

Grantek's Industrial IT team members undergo continual training, participate in and attend key industry events and constantly monitor numerous sources of information to keep abreast of emerging threats and industry leading mitigation tactics.

Cybersecurity assessment and improvement should be a part of any facility project, whether Greenfield or enhancements to an existing facility. Grantek recommends security strategies for all projects because smart manufacturing initiatives require a reliable network, confidentiality, systems integrity, and high availability. A properly secured interconnected production system provides the means to minimize risk and downtime.

Production line and individual machine upgrades now require network connection and offer an opportunity to minimize risk. Connection of equipment from different OEMs poses a risk if attempted without adequate assessment or planning. Grantek offers assessment and strategic implementation to meet the latest security standards throughout the operation.

Grantek can also assist manufacturers with security assessment and improvements during network refresh or expansion on the plant floor, or when legacy assets such as PLCs, HMIs or control systems are being migrated from closed networks to business-wide. If a facility requires implementation of MES/MOM Overall Equipment Effectiveness (OEE) initiatives requiring automated data collection, Grantek can help ensure secure design.

Connecting the ERP to the shop floor for initiatives such as automated batching, serialization, and track and trace also has the potential to introduce unintended security risks, and Grantek's

cybersecurity team can analyze the system design changes to prevent data compromise between factory and business systems.

Of course, if a data breach or network outage/production downtime caused by intrusion has already occurred, Grantek's experts can help minimize the impact and facilitate recovery from the event, whether due to an external or internal malicious actor or an unintentional action.

If there are challenges in implementing corporate IT security policies in the production environment, Grantek offers valuable experience in this area – we excel at facilitating these interdepartmental conversations to attain alignment of goals and understanding between Engineering and Corporate IT groups. We can also help locate and document unknown assets or network configuration for the facility's ICS network.

We work with Operations, IT, Engineering, Safety, and even companies' legal departments—cyberattack in any area affects the bottom line of the entire enterprise. Our team of cybersecurity engineers can assist your company in building security into infrastructure at all levels, beginning with your production systems.

For over 30 years, top manufacturers in Food & Beverage, CPG, Pharmaceuticals and Energy have called upon Grantek to solve their most complex business and manufacturing challenges. Grantek's team of professionals located in 17 offices across the globe deliver solutions to complex problems in Smart Manufacturing, Industrial Networking, Automation and Industrial Safety. Call 1.866.936.9509 or email info@grantek.com to learn more.