Strengthening Cybersecurity in Smart Manufacturing

How food and beverage companies can connect facilities and protect data

Umair Masud, portfolio manager for Consulting Services, and Sherman Joshua, global marketing director for IIoT Services, Rockwell Automation

Introduction

Food and beverage producers are tapping into the power of smart manufacturing at a rapidly accelerating pace. They recognize the value of connectivity and the opportunities it provides to gain better insights into production processes; improve food-safety visibility and practices; and resolve or help prevent food-safety issues. However, with this important trend comes another, more concerning issue: vulnerabilities from insufficient cybersecurity.

Security threats now come in more forms than ever before: physical and digital, internal and external, malicious or unintentional. The truth is that no organization is immune to a security incident. And, more connected operations create more security risks – particularly cyber.

There are a wide variety of potential adversaries in the world, all with different goals and methods. Food and beverage companies could be targeted specifically with threats tied directly to food safety and the integrity of the nation’s food supply. They also could be targeted as a means of testing attack methods ultimately intended for other organizations or industries. All potential threats pose significant risks to food and beverage operations, brands, and the consumers they serve.

More stringently regulated industries were forced to connect and grapple with increased security needs much earlier than other industries. For a time, the focus among many food and beverage producers remained on more traditional, physical security considerations associated with food safety and quality. Now, many companies are taking a fresh look at their security approach to make it comprehensive and cohesive in a connected environment.

Risk-based approach

Cybersecurity is a journey – there’s no silver bullet or catch-all to create a permanently secure environment. Producers need to introduce a variety of capabilities and controls that allow them to respond and adapt to emerging and evolving threats.

A risk-based approach identifies the unique people, process and technology-related risks an organization faces and implements policies and procedures to address them. This allows producers the flexibility to right-size their efforts and allocate the right resources to mitigate risk down to the acceptable level for their organization.

Done right, this approach offers value beyond the most obvious security implications – it also fuels improved productivity and helps prevent unnecessary losses. With cybersecurity programs in place, producers have better visibility into their full range of assets, as well as the ability to identify and correct issues more effectively. As an example, when engineers have remote access to a PLC in a production environment, it’s a benefit that helps sustain productivity levels. However, without the right controls in place, an engineer could access the wrong PLC, causing unnecessary disruption and inhibiting productivity.

So, how can producers evaluate their existing security program and find ways to take a more comprehensive, risk-based approach? There are three key areas to consider: the organization’s cyber hygiene, a defense-in-depth strategy, and planning across the attack continuum.

Cyber hygiene

For food and beverage producers that have more recently introduced smart manufacturing or are in the early stages of updating their cybersecurity practices, cyber hygiene offers a natural starting point. Addressing four key programmatic areas can help an organization establish a base level of cyber hygiene.

- It begins with conducting a thorough inventory of the assets connected on the plant floor – as well as their known vulnerabilities. This asset inventory must be maintained and updated regularly.
- Second, the organization needs to create programs to address the assets' known vulnerabilities, patch regularly and confirm that mature processes are in place to make and track configuration changes.
- Third, it's important to employ backup and recovery mechanisms for all critical assets. This helps make sure a known good backup is on standby and can be accessed quickly.
- Finally, completing regular risk assessments allows an organization to measure and manage risk on an ongoing basis. These assessments provide the most up-to-date view of the level of risk the organization is exposed to and the resources required to mitigate it.

These are fundamental steps that build a cybersecurity foundation from which an organization can continue to build. While maintaining proper cyber hygiene is essential, a connected organization will want to go further to develop a more robust cybersecurity program implemented across all operations.

Defense-in-depth

A security-through-obscurity approach no longer offers sufficient protection against today's wide array of threats and threat actors. An organization should build its security around the idea that any one point of protection probably can and will be defeated. A defense-in-depth strategy creates multiple layers of protection through physical, electronic and procedural safeguards. In the event of a threat, the organization has more than one line of defense in place.

There are six primary components in a defense-in-depth strategy: policies and procedures, physical, network, computer, application and device. While every organization will have a unique security strategy, each of these components will have a role to play in the effectiveness of the overall approach.

Policies and procedures address the human side of security, helping to shape employee behaviors – and to confirm that security practices are followed, and technologies are used appropriately. Physical security limits facility access among both external and internal audiences. For personnel, access should be tightly controlled, limited not only in terms of areas within a facility, but also to entry points on the physical network infrastructure, such as control panels, cabling and devices.

The network security framework should be developed through close collaboration between IT and OT, working together to identify and implement the right technologies and policies. These technologies likely will include an industrial demilitarized zone (IDMZ), which separates the enterprise and industrial zones and helps to manage access and monitor traffic.

The computer component is vital, as software vulnerabilities represent the top means of intruder entry into automation systems. Patch management, antivirus software, application whitelisting, and host intrusion-detection systems are specific measures that help harden an organization's computer assets. At the production application level, security devices are needed to restrict both physical and digital access. Authentication, authorization and accounting (AAA) software helps to restrict and monitor application access and changes.

Finally, devices represent the last area of defense-in-depth security. Organizations should consider deploying device authentication and unauthorized device identification as well as modifying default configurations for embedded devices.

Much of this defense-in-depth approach is focused on proactive, defense measures that prevent threats from fully manifesting. However, it also is important for an organization to investigate and prepare for the entire lifecycle of potential threats, including those that may escalate into a security incident.

Attack continuum

The most robust and effective cybersecurity program addresses each phase of the attack continuum – before, during and after an attack occurs. The steps and activities detailed above relate directly to the before phase, when an organization needs to focus on the identification and protection of its assets, both IT and OT. A thorough, frequently updated risk management plan and a robust cybersecurity program put an organization in the best position to minimize the occurrence of attacks.

Of course, constant vigilance is necessary in the face of the increasingly complex and evolving threat landscape. Organizations must have systems in place to monitor for and detect any network behavior that does not conform to the expected patterns or baseline, equipping them to react, adjust the system and impede potential threats during an attack.

After an attack, the top priority is helping to ensure safe production and minimizing downtime as a result of the cyber-attack. An organization's risk management plan should include processes for containing an attack, eradicating the effects and recovering rapidly. The plan also should outline steps for a post-incident investigation with the goal of identifying root causes and means of strengthening resilience.

Taking action

For years, food and beverage producers have focused on the physical security measures that promote food quality and safety, protecting consumers and stewarding the nation's food supply. In today's connected environment, however, physical security and cybersecurity are inextricably linked. Now is the right time for organizations across the industry to confirm that they have a robust cybersecurity program to mitigate the broader spectrum of potential risk and threats. Applying the same rigor across physical and cybersecurity programs best positions food and beverage producers not only to protect people, but to protect their brand, reputation and financial interests.

Learn more at rok.auto/security

Umair Masud

Sherman Joshua

Masud manages the security services portfolio at Rockwell Automation. He has over 10 years of experience working to help customers manage cyber risk within their industrial control system environments. Reach him at utmasud@ra.rockwell.com.

Joshua leads global marketing for IIoT services at Rockwell Automation. These services include remote support services, network and cybersecurity consulting, remote monitoring, and data analytics. Reach him at sljoshua@ra.rockwell.com.

"How to Strengthen Cybersecurity in Smart Manufacturing"
Umair Masud and Sherman Joshua, Food Quality and Safety
March, Copyright © 2019

Rockwell
Automation

Connect with us.

rockwellautomation.com — expanding **human possibility**™

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication FOOD-SP028A-EN-P - August 2019