Grayway

A JOURNAL FOR BUSINESS & INDUSTRY

JANUARY/FEBRUARY 2019

STRENGTHENING MANUFACTURING

CYBERSECURITY IN A CONNECTED WORLD

SMART DEFENSES FOR SMARTER PRODUCTION

WELCOME

Stephen Gray
President &
Chief Executive Officer

Gray's No. 1 core value is to put safety and quality of life first – a growing part of safety in the industrial sector is cybersecurity. As digitization has grown in a myriad of industries, they have adapted to meet this new challenge. No company is exempt from cyber threats, even Gray.

We often think of financial and healthcare as the center of this new cybersecurity focus, but we should not overlook manufacturing. In this issue of the GrayWay, we focus on why manufacturers, specifically food processors, are targeted and how IIoT actually adds another layer of complexity to assessing security readiness. Cybersecurity professionals offer strategic advice for ensuring secure and robust operations throughout the supply chain.

Gray practices methods which protect our environment.

MIX
Paper from responsible sources
FSC® C016583
www.fsc.org

INSIDE THIS ISSUE

CYBERSECURITY: SECURING THE FRONT LINE

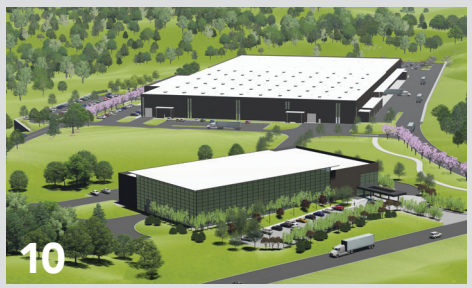
Protecting your manufacturing network involves the entire organization

PROTECTING OUR FOOD INFRASTRUCTURE

Making food and beverage manufacturers tough to target

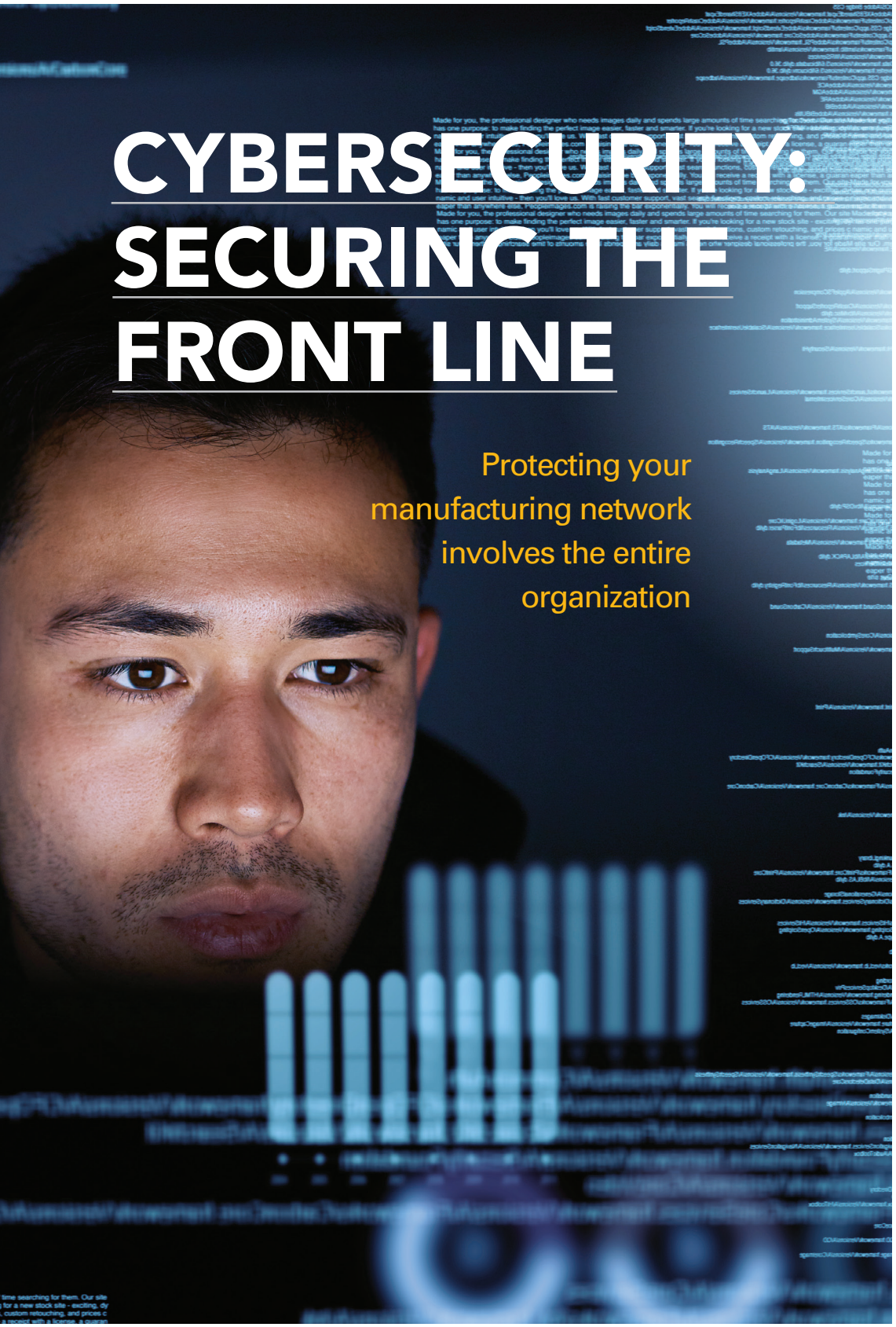
THE NEW FACE OF MANUFACTURING

Thomasnet.com provides cutting-edge information on cybersecurity and other critical categories for industry



GRAY... WE'RE BUILDING

Amada America Inc.
High Point, N.C.



CYBERSECURITY: SECURING THE FRONT LINE

Protecting your manufacturing network involves the entire organization

In recent years, the Department of Homeland Security and United States Secret Service arrested a foreign agent alleged to have facilitated over $4 billion worth of transactions worldwide for cyber criminals engaging in computer hacking, identity theft and ransomware. Major manufacturers are often targets. Last year, hackers infiltrated Tesla's cloud environment and stole computer resources to mine cryptocurrency (dubbed "cryptojacking"), while proprietary data related to mapping, telemetry and vehicle servicing also was exposed.

While the breach was swiftly rectified, it illustrates manufacturing's need for improving cybersecurity. Manufacturing supply chains are connected, integrated and interdependent to improve production efficiencies. Securing the entire multiple company supply chain is not a top-down mission. Rather, it depends on security decision-making at each local plant level.

"Industrial cybersecurity is now central to business strategy, not an afterthought," says Rebecca Taylor, vice president of the National Center for Manufacturing Sciences (NCMS). "Security at every level should be a prerequisite for deploying new technologies."

Rebecca Taylor
Vice President
National Center for Manufacturing Sciences

At the 2018 Automation Conference, Taylor cited a recent Symantec study showing there has been a 92 percent increase in malware, and a 46 percent increase in ransomware. Ransomware in particular has evolved, with hackers no longer asking for exorbitant amounts of money. They now make it a "nuisance" amount like $30,000, Taylor says, and they usually get it.

Is manufacturing particularly at risk? "All critical infrastructure sectors present unique challenges and are at risk due to vulnerabilities that can be exploited by criminals and nation-state cyber actors," replied the U.S. Department of Homeland Security in a statement. "The last five years have brought an increase in concern regarding the potential for cyber-based attacks on critical infrastructures, and the number of cyber-based incidents across critical infrastructure sectors that asset owners reported to DHS's National Cybersecurity and Communications Integration Center (NCCIC) has risen."

When adversaries inevitably strike, will defenders be prepared, and how quickly can they recover? Findings from the Cisco 2018 Security Capabilities Benchmark Study—which offers insights on security practices from more than 3,600 respondents across 26 countries—show that defenders have a lot of challenges to overcome. Even so, defenders will find that making strategic security improvements and adhering to common best practices can reduce exposure to emerging risks, slow attackers' progress and provide more visibility into the threat landscape.

Standards organizations are one place to look for direction on how to establish risks and set up responses. The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce, is a collaborative hub where industry organizations, government agencies and academic institutions address the most pressing cybersecurity challenges for businesses. This public-private partnership enables practical cybersecurity solutions for specific industries or broad, cross-sector technology challenges. Working with technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE and NIST are developing modular, easily adaptable examples of cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

The five "functions" of NIST's Cybersecurity Framework Core are:

Identify
Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.

Protect
Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.

Detect
Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Respond
Develop and implement the appropriate response actions regarding a detected cybersecurity event.

Recover
Develop and implement the appropriate activities to maintain plans for resilience and to restore any impaired capabilities or services due to a cybersecurity event.

"All critical infrastructure sectors present unique challenges and are at risk due to vulnerabilities that can be exploited by criminals and nation-state cyber actors."

– U.S. Department of Homeland Security

On or Off the Internet?

Joe LaRussa
Director of Industrial Engineering
Brose Group

"The issue every manufacturer needs to take a hard look at is how militant do they need to be about network security," said Joe LaRussa, director of industrial engineering – seats at Brose Group, the world's fourth-largest family-owned automotive supplier. Addressing the Michigan Manufacturers Association, he said building a point-to-point off-internet hardware network among all company locations minimizes entry points and makes manufacturing a harder target. The downside is such a setup is extremely costly.

LaRussa adds, "Perhaps sharing costs with local municipalities would not only make cybersecurity more affordable but make the U.S. more competitive compared to other countries relying on strong incumbent internet service providers. Managing internet infrastructure as a utility could provide a high security alternative to traditional internet service."

Solving emerging security challenges is a vital part of ongoing continuous improvement in manufacturing. As threats appear seemingly daily, so are solutions from a number of automation, network, industry associations and cybersecurity specialists. The value of production efficiency means sharing it wisely and protecting it securely.

With connected systems in plants and throughout supply chains, cybersecurity for manufacturers must be a strategic process, not a response.

PROTECTING OUR FOOD INFRASTRUCTURE

Making food and beverage manufacturers tough to target

The manufacturing industry, while leading the way with connected production systems and supply chains, is still seen as emerging in effectively applying cybersecurity to protect its systems. The same can be said of food and beverage manufacturers.

"Food safety is something we all care about," says Umair Masud, product manager, cybersecurity services at Rockwell Automation. And like conventional manufacturing, food and beverage producers are implementing connected systems with complex supply chains while facing increasing threats to intellectual property, formulas, recipes and operational efficiencies.

Dawn Cappelli
Vice President of Global Security and Chief Information Security Officer
Rockwell Automation

"We've seen a lot of focus on the "before," or what can be done to prevent cyberattacks, but not so much on the "during" and "after" – what capabilities do you have for effective detection, response and recovery?" adds Dawn Cappelli, Rockwell Automation's vice president of global security and chief information security officer. "You need a holistic strategy that looks at the entire enterprise ecosystem to make sure products and systems are secure. This involves organizing and getting the input of security teams across IT, operations and engineering and having strategic and tactical discussions to establish a common language and framework when it comes to cybersecurity."

The U.S. Department of Homeland Security (DHS) works closely with the thousands of registered food manufacturing, processing and storage facilities to assess and implement risk management for cyber and physical threats. With input from the Department of Agriculture and the Department of Health and Human Services, DHS also pursues a model of "collective defense" in cybersecurity, meaning government and industry take collaborative, tangible actions together to mitigate threats and reduce the most serious, enduring and collective strategic cyber risks. "Collective defense is central to our long-term DHS Cyber Strategy of managing national cyber risks, especially in the area of vulnerability and threat reduction," the department replied in a statement.

Is there "best advice" for food and beverage processors to improve cybersecurity? The DHS's National Cybersecurity and Communications Integration Center (NCCIC) continues to observe that lapses in basic cybersecurity practices are the most prevalent type of vulnerability "stumble."

From critical infrastructure control system assessments conducted, NCCIC found the most frequently identified vulnerabilities to be: (1) boundary protection—this was the single most prevalent area of concern; (2) continuing a four-year trend, identification and authentication of legitimate system users; and (3) allocation of resources.

In response, NCCIC offers free tools that can help companies and industries address many of their cybersecurity challenges. The Cyber Security Evaluation Tool (CSET) is a no-cost, voluntary technical assessment that provides a snapshot of

an organization's cybersecurity posture. It helps asset owners and operators assess cybersecurity strengths and weaknesses within their control system environments and can also be used to assess traditional IT infrastructure. In addition, DHS offers Cyber Resilience Reviews, a no-cost, voluntary, non-technical assessments to evaluate operational resilience and cybersecurity capabilities of an organization, and industrial control system (ICS) cybersecurity training either online or instructor-led classes at their Idaho Falls facility.

Rockwell Automation's Dawn Cappelli also advises not letting down your guard when it comes to mitigating insider threats. There are common sense tips for everyone to implement on the plant level:

- Identify and classify key information and technology. Know who has access to critical information.
- Conduct training for managers on behaviors that could indicate increased risk of either workplace violence or cyber insider threats, such as deliberate sabotage of plant operations. Managers need to recognize increased risk following a negative workplace event, like a reduction in force, new management, lower raises than anticipated or an employee that does not get the promotion they think they deserve.

"You need a holistic strategy that looks at the entire enterprise ecosystem to make sure products and systems are secure."

– Dawn Cappelli
Vice President of Global Security and
Chief Information Security Officer
Rockwell Automation

A negative event followed by concerning behaviors that get worse and worse over time instead of better could indicate increased insider risk.

- Ensure coordination and collaboration between HR, security, IT and all employees, not only for updating passwords and security patches, but for creating a culture of accountability and security where data protection is seen as everyone's responsibility.

Cyber or not, the best security asset in any organization are employees with the training, awareness and dedication to spot an issue and raise it to management.

THE NEW FACE OF MANUFACTURING

Thomasnet.com

Thomasnet.com provides cutting-edge information on cybersecurity and other critical categories for industry

Rita L. Lieberman
Director,
Marketing
Communications
Thomasnet.com

Online search engines, traditional reference catalogs and the advice of friends and colleagues come to mind as initial methods of finding out more about manufacturing suppliers. One of the leading resources that engineers, purchasing managers and other industrial experts rely on is Thomasnet.com.

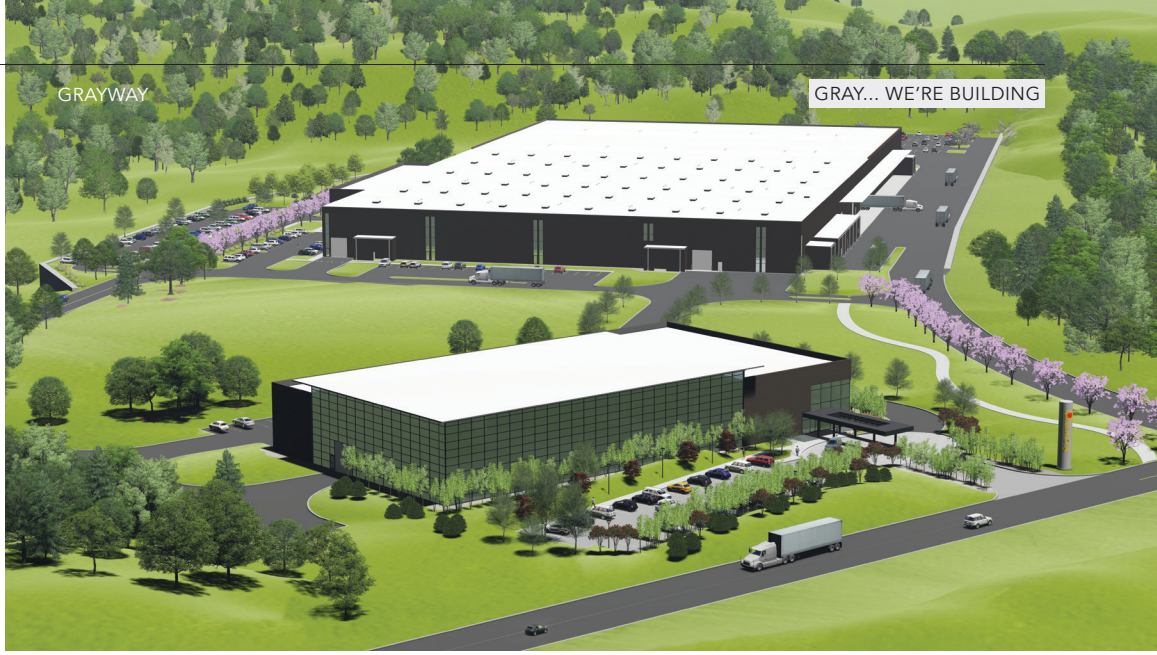
Thomasnet.com is the leading platform for product sourcing, supplier selection and actionable information for industry. Thomas, the company behind Thomasnet.com, regularly analyzes the petabytes of buyer behavior data generated on the platform to help buyers make better purchasing decisions.

"Our data-driven analytics allow in-market buyers to find the right products and services when they need them," said Rita Lieberman, Director, Marketing Communications.

Through Thomas Insights, the company also provides both manufacturers and industrial buyers with insight into the trends, changes and challenges facing the industrial sector. To that end, Thomas recently highlighted findings from the Hackett Group in the report The Six Biggest Risks Facing Your Manufacturing Business Today. Unsurprisingly, cybersecurity was high on the list.

According to Thomasnet.com., in addition to using both traditional and advanced security software, companies can regularly perform insider threat prevention and detection audits, prohibit the use of personal devices within the facility, continually educate employees and communicate meaningfully with vendors and suppliers.

THOMAS™
For Industry.



GRAY... WE'RE BUILDING

AMADA AMERICA INC.

HIGH POINT, N.C.

Amada America Inc. is a global manufacturing leader of precision sheet metal fabrication equipment such as punch presses, lasers, press brakes and flexible manufacturing systems, software and tooling.
The company selected Gray Construction to design and build its more than 250,000 s.f. manufacturing operation in High Point, N.C. which includes a manufacturing facility, technical center and offices.

The new facility will manufacture and assemble a line of high-precision press brake bending equipment for the U.S. market and will create some 200 jobs for the region.

10 Quality Street
Lexington, KY 40507-1450, USA
T 859.281.5000

Alabama | California | Georgia | Illinois
Kentucky | North Carolina | South Carolina
Edmonton, Canada | Tokyo, Japan

www.gray.com