VOLUME 35, NUMBER 3, MAY/JUNE 2014

CYBERSECURITY

Grayway

ON THE DEFENSE

SECURING COMPANY DATA IN AN EVER-THREATENING CYBERWORLD

Gray

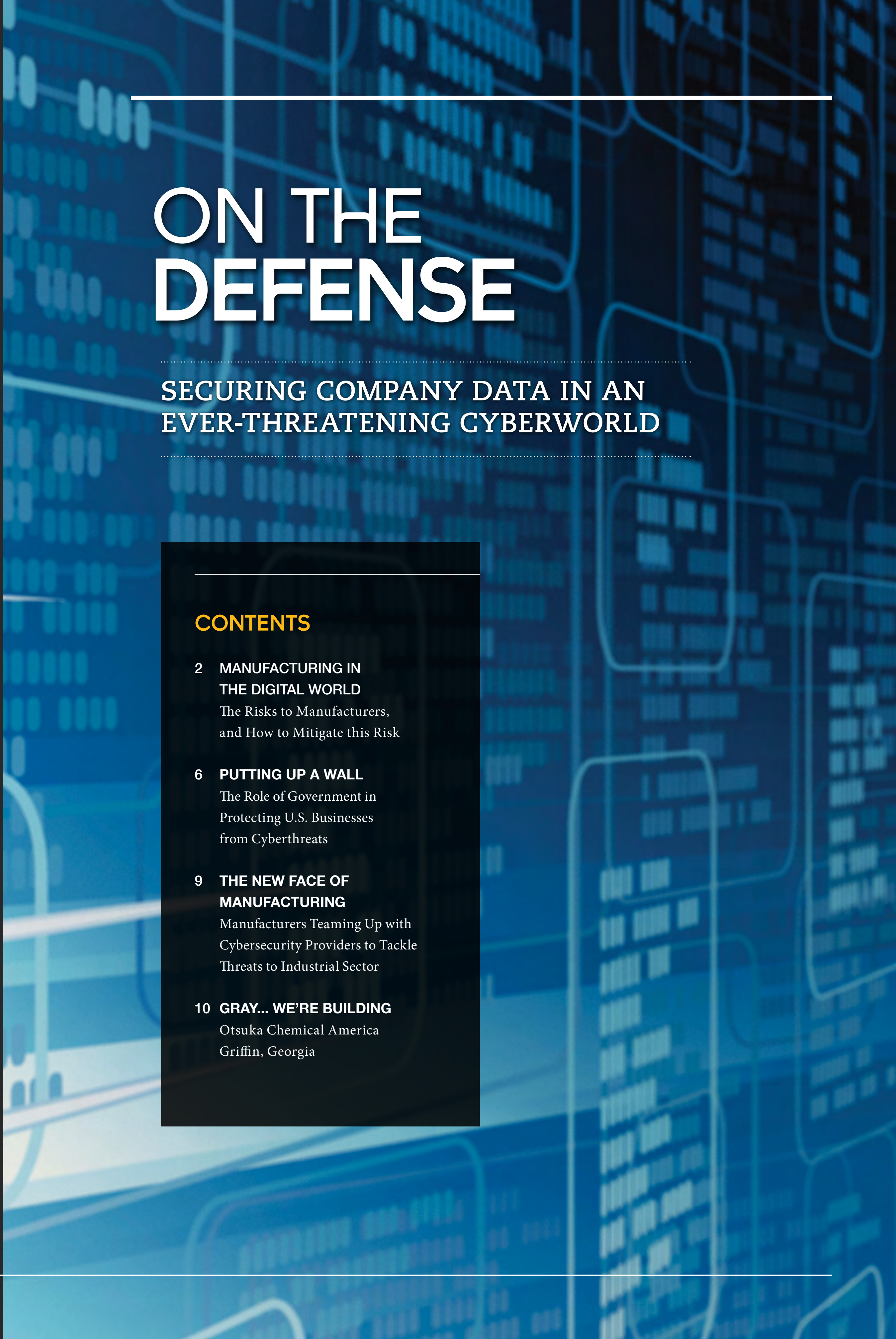
THIS ISSUE / On the Defense

Stephen Gray
Chief Executive Officer

Advances in global connectivity have had a tremendous impact on the way we do business. With just the touch of a button, company ideas, strategies, plans and decisions are being shared, improving efficiency and productivity for companies worldwide. But these conveniences have come at a great price. As our world becomes more and more connected, confidential and critical company information is being put at risk, and more sophisticated hackers are at the ready, waiting for just the right opportunity to strike. No industry is immune to these threats, including manufacturing.

In this issue of the GrayWay, we explore how manufacturers' company data may be at risk, the most serious threats they face, and strategies for reducing these dangers. We also cover the role government is playing in mitigating cyberattacks on U.S. businesses, at both the state and federal level.

Gray practices methods which protect our environment.



ON THE DEFENSE

SECURING COMPANY DATA IN AN EVER-THREATENING CYBERWORLD

CONTENTS

MANUFACTURING IN THE DIGITAL WORLD

The Risks to Manufacturers, and How to Mitigate this Risk

More than four-hundred billion dollars: this is the staggering cost of cybercrime to the global economy, according to a new study released by McAfee and the Center for Strategic and International Studies. In fact, the United States, Germany and China together lost more than $200 billion dollars to cybercrime in 2013, according to the report. And when the global economy suffers, so do jobs and manufacturers.

“In the United States alone, studies of how employment varies with export growth suggest that the losses from cybercrime could cost as many as 200,000 American jobs, roughly a third of 1% decrease in employment for the U.S.,” the study says.

Countries with robust economies, like the U.S., are more likely to be impacted because the value of its exports is dependent upon innovation, the report said. Stolen intellectual property reduces exports, as well as overall GDP, and even small changes to GDP impacts employment. For example, if lost jobs are in manufacturing or other high-paying sectors, the effect of cybercrime is to shift workers from high-paying to low-paying jobs, or unemployment.

While job loss is a concern as cybercrime rates increase, the study concluded the most significant damage comes from its effect on trade, competitiveness, innovation, and global economic growth.

Larry Clinton

According to Larry Clinton, president and CEO of Internet Security Alliance—a multi-sector trade association that focuses on cybersecurity economics and policy—even the most locked-down company can be subject to attacks due to vulnerabilities within the company’s supply chain. No longer is it enough to ensure your own computer networks are secure; it’s essential to understand the security level of your suppliers and vendors. Companies with deep supply chains, like manufacturers, can be among the most vulnerable.

“For economic reasons, many companies manufacture through the use of these long international supply chains,” said Clinton. “The problem with that is the longer your supply chain is, the harder it is to secure it.”

Clinton says there are a number of ways a manufacturer’s supply chain can be compromised, but the most common attack comes through interconnected software systems.

“We did a project a number of years ago specifically looking at the threats to the supply chain that was focused on hardware, but we found that in the commercial sectors, hardware supply chain attacks were of comparatively low risk,” he said. “Attacks on the software side were of a higher likelihood because they were cheaper.”

Another challenging area for manufacturers is protecting old and outdated software systems from data breaches, says Chester Wisniewski, senior security advisor with IT security product company Sophos, Inc. For example, if a robotics system on a manufacturing floor runs on an old version of Windows, it inherently will have fewer built-in security features to thwart modern-day attacks.

Chester Wisniewski

“This is a challenge in manufacturing because the timeframe for which you purchased your capital equipment is usually quite long,” said Wisniewski. “Whereas, most of the computers being built today are expected to have a lifetime of two or three years. So there’s a big conflict as manufacturing has moved to more mechanized processes and more computerized operations.”

But what these experts cite as the most significant security risk to manufacturers has nothing really to do with manufacturing at all, but rather is inherit to all sizable businesses: a vast network of people interacting on company-wide systems that are often interconnected with personal devices, like cell phones, laptops and tablets.

According to an article published in an April issue of the *New York Times*, a large oil company (whose identity has been kept confidential) was breached when hackers infected the online menu of a Chinese restaurant with malware that was popular with employees.

“When the workers browsed the menu, they inadvertently downloaded code that gave the attackers a foothold in the oil company’s vast computer network,” the article stated.

“People tend to think this is an IT problem—it’s not,” said Clinton. “It’s an enterprise-wide risk management problem. In fact, the number one vulnerability for companies isn’t the technology, it’s the people. And human resource management within the organization is just as important as IT management. Most people really haven’t thought through this in that sense. They still think as long as I update my software and do some best practices, I’ll be okay. That’s not the case.”

Clinton says companies that allow employees to use their own devices in order to cut costs and create efficiencies are putting their systems at risk.

"Thousands of employees walking around with your corporate data on their iPhones, that are probably not protected, really undermines your security," he said.

The transition to cloud-based technology that many companies are making adds another layer of complexity to cybersecurity. A recent study by computer scientists at Johns Hopkins University suggests that even the most cutting-edge cloud storage providers may be putting company data at risk. The study asserts that cloud providers who claim to employ a "zero-knowledge" approach—one that is thought to be virtually impenetrable—remain vulnerable to attack when data is shared with vendors.

> "In fact, the number one vulnerability for companies isn't the technology, it's the people."
>
> – Larry Clinton

Experts recently gathered at the RSA Conference to discuss global information security. John Pescatore, director of research at the SANS Institute, indicated that cloud adoption is inevitable even with potential concerns. In fact, the panel of experts concluded that cloud security concerns are overblown. According to Pescatore, "A vast majority of enterprise breaches involving cloud providers stemmed from enterprise failures and not cloud provider faults."

Whether or not there are risks associated with the use of cloud technology, Clinton says companies will largely continue this practice due to the enormous cost savings. In large part, Clinton says companies are not thoughtfully weighing the benefits of making additional investments in cybersecurity, nor are they assessing the risk to their businesses if they fail to do so.

"Those are the types of sophisticated decisions that are not being raised to the board or senior-management level in most industries, including manufacturing. But that's what needs to happen to solve this."

Wisniewski concurs, adding that cybersecurity investments are an important part of any risk management plan.

"What businesses should do when they're making any kind of security investment, whether it's physical or technological, is assess the risk to the business if these computers are down, or if this information is compromised, and what it's going to cost to protect our data and lower that risk," he said. "Because you're really buying insurance, aren't you? If you're manufacturing hardware for defense contractors, it would seem obvious that your business would come to an end if those blueprints were stolen from you. Nobody's going to ask you to make something again if you can't keep those plans secret."

Wisniewski believes these security investments may not be prioritized because, unlike retailers who handle massive amounts of consumer data every day, manufacturers may not assign a similar value to the data they possess.

"Anything that's of value, the attack community will attack," he said. "Intellectual property? Absolutely! But not just your intellectual property—your business processes as well. If you've been running an auto plant for 100 years, and during those 100 years, you've really learned how to build cars in a way that nobody else knows, and you've got proprietary processes that you use to create efficiencies, that's valuable stuff. People are liable to come in and attack it. If you are thinking of merging with an organization, people are interested in that information. Your merger/acquisition plans, your financial plans. All these things have great value in the wrong hands, and all of it is subject to attack."

ESSENTIAL SAFEGUARDS FOR EFFECTIVE SECURITY

Each year, the multinational professional services network—PricewaterhouseCoopers (PwC)—releases its Global State of Information Security® Survey, a worldwide study by PwC, CIO magazine, and CSO magazine. Below are "the fundamental safeguards you'll need for an effective security program," as recommended by PwC:

- A written security policy
- Back-up and recovery/business continuity plans
- Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
- Strong technology safeguards for prevention, detection, and encryption
- Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
- Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
- Ongoing monitoring of the data-privacy program
- Personnel background checks
- An employee security awareness training program
- Require employees and third parties to comply with privacy policies

PUTTING UP A WALL

The Role of Government in Protecting U.S. Businesses from Cyberthreats

Succeeding in today's intensely competitive global marketplace is challenging, to say the least, but with an ever-growing pool of cyberattackers specially trained to access and cripple large computer networks, international competition is no longer just tough, but can be downright vicious.

With manufacturing coming back to the U.S. due to a variety of reasons, some believe countries that have enjoyed a thriving manufacturing industry over the last decade or so view maintaining a competitive edge as a matter of national security. Rumors of state-sponsored cyberattacks have been circulating for years, but, for the first time ever, foreign officials have been indicted on charges of economic espionage, computer hacking and other offenses against U.S. businesses. This has some international companies pressing the panic button, scrambling for ways to protect their most valuable information and networks.

In light of the growing threat to U.S. commerce from overseas, in 2013, the U.S. government commissioned the National Institute of Standards and Technology (NIST) to develop a "Cybersecurity Framework"—a "best practices" for U.S. business and industry that consists of standards, guidelines and practices to promote the protection of critical infrastructure. The first version, released in 2014, is entirely voluntary and the NIST says it will "help align critical infrastructure of owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyberrisks."

But not everyone is convinced the U.S. government should be handing out such advice. Researchers with George Mason University's Technology Policy Program conducted a study on federally sponsored cybersecurity practices and concluded that, because cyberthreats are ever-evolving and changing, cybersecurity cannot be tackled by a one-size-fits-all solution. The study also suggested such an approach could thwart creativity from business and industry where some of the best solutions are innovated. And because the federal government does a relatively poor job of protecting itself from cyberattacks, U.S. businesses should have little faith that by following these standards, they will be protected.

The study suggested a better solution is to "promote private cybersecurity insurance that would provide competitive coverage for cybersecurity breaches that is tailored directly to the unique needs of each industry and organization." This would, in turn:

- Promote proactive risk reduction efforts to decrease insurance company costs. Insurance companies would use audits and rate pressure to encourage clients with substandard security practices to improve.
- Teach insurance companies best practices from experiences with their clients and continually improve the net level of cybersecurity by developing better recommendations and standards.
- More accurately price and distribute risks and liabilities.

Some members of Congress are attempting to address the issue of cybercrime by introducing legislation aimed at lessening the blow of attacks on U.S. companies. U.S. Senators Chris Coons (D-Del.) and Orrin Hatch (R-Utah)—members of the Senate Judiciary Committee—introduced what's being called the Defend Trade Secrets Act to help combat the loss of an estimated $160 billion to $480 billion each year in the United States to the theft of corporate trade secrets. The act would empower companies to protect their trade secrets in federal court by creating a federal private right-of-action. The bill has been endorsed by the National Association of Manufacturers, the U.S. Chamber of Commerce and companies including 3M, Abbott, AdvaMed, Boston Scientific, Caterpillar, Corning, DuPont, GE, Eli Lilly, Medtronic, Micron, Microsoft, Monsanto, Philips, P&G, and United Technologies.

State governments have also responded to growing cyberthreats, enacting laws to help protect their own interests and those of local businesses. All but three states—Alabama, New Mexico and South Dakota—have enacted data breach notification laws in order to track and address attacks on state governments and the companies operating within their states.

Joel Beres

Joel Beres—an intellectual property attorney for Stites & Harbison in Lexington, Ky. and a founding member of the firm's Intellectual Property and Technology Service Group—says many inconsistencies in cybersecurity law exist across state governments and, because of this, it can be difficult for businesses that compete on a national and global scale to stay in compliance with so many different regulations.

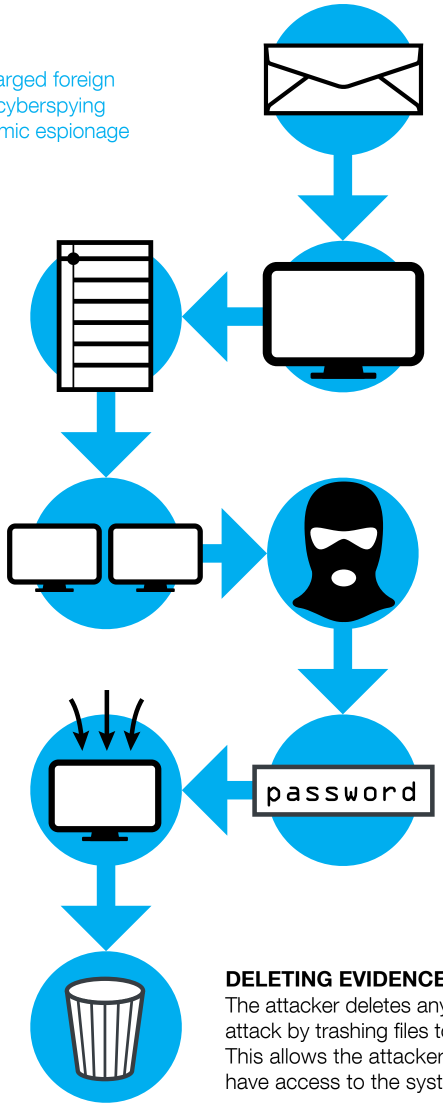
"The laws are not the same across the 50 states, so if you're a manufacturing company doing business nationally, you may have different obligations to provide notice in Kentucky than you would in California," said Beres. "And there are different time periods to provide the notice, different means of providing the notice, and a variety of ways to do it. And that's just if you're doing business in the United States. If you also are doing business in Europe, you're subject to the European Union's and individual nation states' laws, as well."

Cybersecurity in the industrial sector is a complex issue. It is becoming even more complicated as new, more sophisticated threats are introduced, and as new laws are passed to help curb cybercrime. While it remains to be seen how impactful governments can be in deterring attacks on U.S. manufacturers, the ultimate responsibility lies within the manufacturing community itself.

Today's manufacturers must make a company-wide commitment to remain educated on the latest threats to their internal networks. They must implore strategies to prevent and manage attacks, from the C-suite to the shop floor.

Cyberspying: How Cyberattackers Operate

For the first time, the U.S. has charged foreign government officials in a criminal cyberspying case. Here is how a typical economic espionage hacking attack works.



ATTACKER E-MAIL
The cyberattacker sends a phishing e-mail to gain access to the target's computer.

ATTACHMENT OPENED
If the victim opens the e-mail attachment, it installs the malware onto the computer.

MALWARE MULTIPLIES
The malware becomes a beacon on the victim's server and downloads additional malware onto their computer.

MULTIPLE CONNECTIONS
The attacker launches multiple backdoors to make sure access is continued – in case malware is found on other systems.

SYSTEM ACCESS
The attacker now has access to sensitive information and steals account names and passwords from the domain controller.

CRACKS PASSWORDS
Using the stolen information, the attacker gains access to legitimate user accounts and continues to attack other computers.

GATHERS DATA
The attacker explores the system further to identify and to gather sensitive information. Information is collected onto a staging server and then removed.

DELETING EVIDENCE
The attacker deletes any evidence of the attack by trashing files to avoid detection. This allows the attacker to continue to have access to the system.

Source:
The DesMoines Register

THE NEW FACE OF MANUFACTURING

Manufacturers Teaming Up with Cybersecurity Providers to Tackle Threats to Industrial Sector

The recent announcement of a partnership between one of the world's leading industrial automation products manufacturers and a global leader in network security to develop new manufacturing security solutions should come as no surprise. Manufacturers boast some of the world's most creative and innovative problem-solvers, and when a threat to the industry exists, manufacturers will inherently respond.

Earlier this year, the Siemens Industry Sector announced a partnership with McAfee, a division of Intel Security, to enhance the security offerings for industrial customers to protect against rapidly evolving global cyberthreats. This partnership will take advantage of the depth of both companies' security portfolios and further enhances the joint effort started in 2011.

"Siemens provides deep experience in automation across numerous industries," said Michael Fey, worldwide chief technology officer at McAfee. "By combining forces, McAfee, Intel and Siemens can drive the adoption of connected, managed and secured solutions at the plant level in order to help industrial customers to manage their security while bringing the uptime and reliability of the plant operations to a higher level. This collaboration should allow us to address the unique requirements of Industrial Control System customers for the operations technology market thus providing a complete security view across the entire company."

The companies also announced they are developing a line of security products designed to enhance security offerings for the process and factory automation industry.

GRAY... WE'RE BUILDING

OTSUKA CHEMICAL AMERICA, INC.

Griffin, Georgia

Gray has been selected by Otsuka Chemical America, Inc. to design and build its first U.S. plant—a 50,000 s.f. Terracess manufacturing facility on a 35-acre site at Georgia's first eco-friendly park. The Terracess facility will create over 30 jobs and will manufacture titanate friction materials for automotive brake pads. Otsuka is building the facility in response to a growing demand for the material due to what they call the United States' "robust market for new automobiles and the presence of numerous brake pad development facilities." This will be Otsuka's third such manufacturing facility; the others are located in Japan and China.

Construction is scheduled to begin in the summer of 2014. Gray will also be offloading and installing most of the process equipment that will be utilized by the facility when it becomes operational. The facility will have an annual production capacity of about 2,000 metric tons and is expected to commence commercial production in November 2015.

Founded in 1950, Otsuka Chemical Co., Ltd. is based in Osaka, Japan with production facilities and offices in nine countries throughout the world. The company engages in the research, development, manufacture, and sale of organic, inorganic, fine, and specialty chemicals.