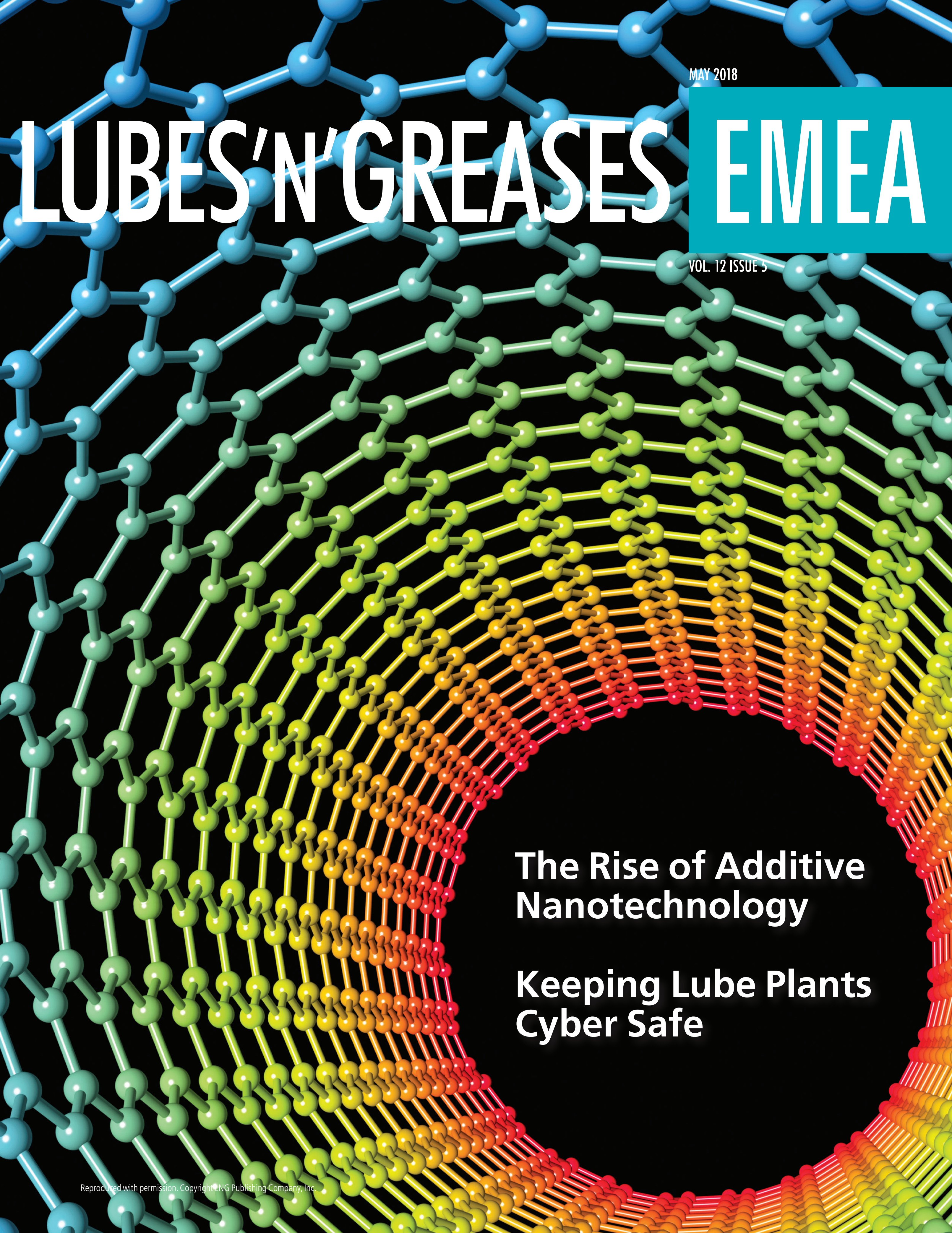
MAY 2018

LUBES'N'GREASES EMEA

VOL. 12 ISSUE 5



The Rise of Additive Nanotechnology

Keeping Lube Plants Cyber Safe

Reproduced with permission. Copyright LNG Publishing Company, Inc.

CYBERSECURITY IN THE LUBRICANTS WORLD

Cybersecurity threats represent one of the biggest challenges for lubricant and grease manufacturers, or any organization in the petrochemicals industry. From the theft of formulas and other intellectual property to plant shutdowns, product manipulation, physical damage and demands for payment from ransomware, the threats are growing. Cybersecurity expert **Gareth Leggett** explains the pitfalls of lax security in the lubricants business.

Reproduced with permission. Copyright LNG Publishing Company, Inc.

The 13th edition of the Global Risks Report presented this year at the World Economic Forum in Davos, Switzerland, ranked cyber attacks as the third most-likely global risk after extreme weather events and natural disasters. And yet despite such assessments, cybersecurity has been viewed as a hindrance, with the misconception that it places obstacles in the way of growth.

Cybersecurity should not be viewed at best as protection against external threats to existing systems. To view it as such is to ignore its benefits and the opportunities it brings. On the contrary, effective cybersecurity is a business enabler that allows organizations to address their business challenges and deliver their strategic plans.

The objectives for companies in the lubricants sector – reducing downtime, improving safety, meeting regulatory demands, protecting intellectual property, improving efficiency, reducing costs and protecting brand reputation and product quality – can only be achieved by reducing security risks.

> Industrial control security should do no harm to industrial systems, require no downtime, detect and enable early warning of malicious and accidental threats, and enable rapid response and reduce time to resolution.

Effective cybersecurity reduces these risks by lowering the probability of an unwanted event and its effects, allowing lubricant companies to meet their business objectives. Digitization and automation initiatives are made possible when organizations adopt a unified enterprise-wide approach to cybersecurity.

One Enterprise, Two Systems

Petrochemical companies are not the same as organizations in other business verticals, and yet the majority of cybersecurity companies treat them as if they were. Outside this sector, companies operate the kind of information technology systems found in every office, which are made up of components such as laptops, printers and file servers. For companies in the lubricants industry, this is only half the story.

While IT systems power the corporate network, the production network is run on operational technology systems that drive the automated, real-time production environment. They operate nonstop and include the programmable logic controllers and remote terminal units that control the switches, pumps, valves and heaters that power the industry. In the OT environment, safety and availability are paramount since these essential components have minimal service windows.

OT systems are not IT systems and should not be treated as such, but protecting them requires a recognition that corporate and production systems are now connected for management and business purposes, and it is these connections that attackers take advantage of. Malicious attacks to OT systems often originate in the IT system. Therefore, a holistic approach must be adopted in order to achieve unified enterprise-wide defense.

Cybersecurity providers can use site surveys and discovery programs to identify the connections between the industrial network and the corporate network, the internet and to third parties. Once discovered, solutions can be deployed to provide protection across technology areas.

This cross-domain protection is especially relevant for lubricant and grease manufacturers. They are a primary target of cyberattacks as the product formulas are highly valuable. A unified cross-functional approach across corporate and production networks is essential to secure the internet protocol chain on both IT and OT systems.

Product quality is another area of concern, as the rise of attacks aimed at product manipulation is a worrying trend in the petrochemicals business. A unified, enterprise-wide

Reproduced with permission. Copyright LNG Publishing Company, Inc.

Industrial Systems Cyber Security Programs

SECURE	DEFEND	PROTECT	MONITOR	MANAGE
• Physical Security • Security Practices • Access Control • Asset Inventory • Device Hardening • Vulnerability Management	• DMZs • Firewalls • Unidirectional Gateways • Anti-Malware • Endpoint Protection	• Application Whitelisting • Zone Firewalls • Device Firewalls	• SIEM • Configuration Change Management • Continuous ICS Security Monitoring	• Threat Intelligence • Incident Management

Source: Kemsec

approach to cybersecurity involving all functional and technology areas is the best defense for product protection.

Evolving Threats

The methods and motivations behind cyberattacks develop as fast as the technology used by the attackers and defenders of industrial systems. One would not assume that the global explosion in cryptocurrency poses a threat to operators of industrial systems, yet already in 2018 they have been increasingly targeted by so-called "cryptocurrency mining" attacks.

Industrial infrastructure is an appealing target for such attacks, which hijack compromised systems to run the processor-heavy algorithms that are part of the process of acquiring, or mining, currency. An attack reduces the host's program and system performance and the extra CPU load increases response times, which are critical for real-time industrial systems designed for process control, jeopardizing their safety and availability.

While the aim of cryptocurrency mining attacks is financial and not sabotage, the same cannot be said of the recently discovered Triton malware attack framework, which infiltrates specific industrial safety systems for purposes that are not yet understood but are likely to be malicious. Variants of these attacks have caused plant and facility shutdowns across the globe.

These industrial systems are the critical last line of defense for plant and process safety. But the lack of security and authentication for devices at the lowest levels of the industrial controls architecture within many petrochemicals plants leaves them open to attack. (Industrial networks are made up of levels, with level 0 being hardware such as switches, valves and pumps, and level 1 being the devices that control them, etc.)

Building a Wall

In the past, industrial systems were standalone and contained within the walls of the facility, but this is no longer the case. As mentioned, there are now connections to corporate systems, as well as to vendors.

2018 has also seen a rise in the number of internet-accessible industrial control system components. Whether these components are intentionally connected or connected due to poor design, configuration or security, the effect is the same – an increased attack surface. Industrial operators must discover and secure all connections to the industrial environment and not believe in the misconception that their systems are "air-gapped".

Effective cybersecurity is not achieved by simply installing technology, however. Protection is achieved by a combination of people, processes and technology. This approach must extend to the entire organization. Cybersecurity should be a board-level priority issue. It is a job for senior executives and not just security practitioners. The executive level is also key to the successful convergence of IT and OT functions.

Traditional structures place IT functions under the chief technical officer and OT functions under the chief operating officer. This approach creates a "silo mentality", whereby one department withholds information from others, which in turn prevents effective enterprise-wide cybersecurity.

Many organizations are now creating a new executive level role of chief digital officer to bridge the gap. With boardroom support, organizations can adopt a security-centric approach. By aligning security with quality, safety, research, produc-

Reproduced with permission. Copyright LNG Publishing Company, Inc.

National Institute of Standards and Technology Cyber Security Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVERY
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Awareness Control • Awareness & Training • Data Security • Information Protection & Procedures • Protective Technology	• Anomalies & Events • Continuous Security Monitoring • Detection Processes	• Response Planning • Communication • Analysis • Mitigation • Improvements	• Recovery Planning Improvements • Communications

Source: Kemsec

tion and all other functional areas, lubricants businesses can effectively and efficiently utilize cybersecurity as a business enabler.

The security-centric approach must also extend beyond the organization. Automation and digitization are driving the creation of process-wide systems with more suppliers and facilities connected to what were once standalone systems contained within the walls of the plant. Cybersecurity across the supply chain reduces the risks and enables the creation of these extended systems. Enabling future digitization and automation for plants and facilities are priority projects across the sector, as organizations seek to become more efficient without affecting the safety and availability of their facilities.

> First steps to a security solution are to understand the design, protocols and systems of the industrial network; be acquainted with industrial control topographies; determine and monitor high-value targets; protect and keep an inventory of industrial end points; determine critical production services and appliances prone to crashing; and identify connections between industrial and corporate networks, the internet and third parties.

As petrochemicals organizations move toward Industry 4.0 – broadly defined as manufacturing technology automation and data exchange – the need for effective cybersecurity to both protect and enable has never been greater. Driven by strategic business initiatives, digitization and automation projects that utilize the industrial Internet of Things to enable cyber-physical systems that communicate and cooperate with each other and humans in real time require cybersecurity to enable them to operate without risking safety and availability.

Surveys show that while many businesses in the sector have invested in defense technologies such as firewalls, they have no visibility or protection for systems inside this perimeter. Effective cybersecurity is achieved by a "defense-in-depth" approach that protects all components across the system by placing multiple layers of security. Perimeter defense alone leaves systems unprotected once this border is breached. It also leaves businesses unprotected in the event of an insider attack or in the event of an accidental threat.

Accidental threats are caused by non-malicious actors, typically employees or contractors, undertaking actions that have the unintended consequence of increasing risk. Effective cybersecurity enables the detection and prevention of these threats.

> Project focus areas include asset discovery and management; incident detection and response; continuous network activity monitoring; configuration change management; vulnerability assessment and risk management; and architecture and enterprise readiness.

Cybersecurity is more than protection from external threats. It is a business enabler that allows petrochemical businesses to meet the challenges of today and supports the projects of tomorrow. □

Gareth Leggett is director of industrial control systems cybersecurity for Kemsec. He has 20 years of experience in the sector, working throughout the petrochemicals and manufacturing industries around the world helping clients secure their assets, improve availability and protect intellectual property. Contact him at gareth.leggett@kemsec.com

Reproduced with permission. Copyright LNG Publishing Company, Inc.