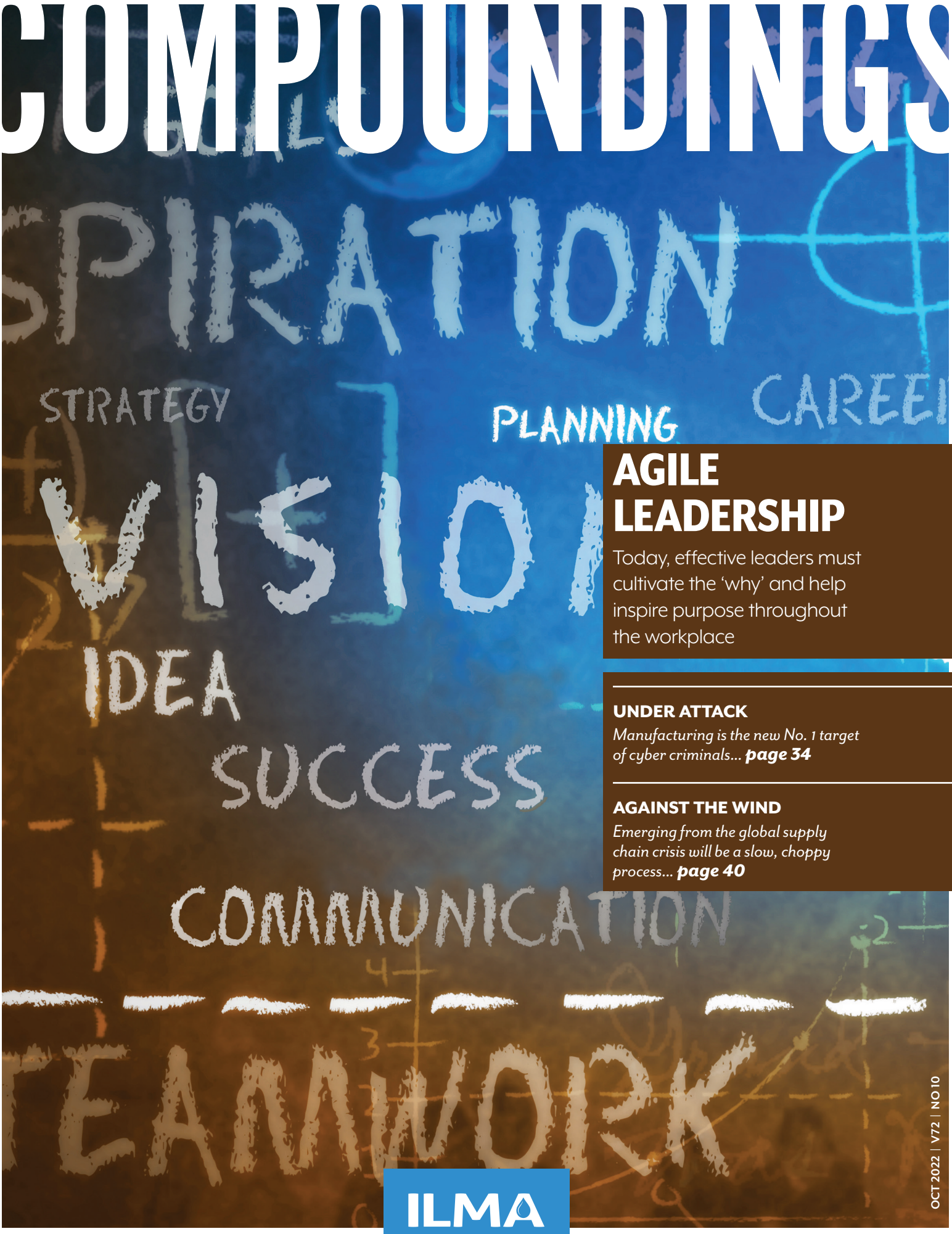
THE MAGAZINE OF THE INDEPENDENT LUBRICANT MANUFACTURERS ASSOCIATION

COMPOUNDINGS



AGILE LEADERSHIP

Today, effective leaders must cultivate the 'why' and help inspire purpose throughout the workplace

UNDER ATTACK

Manufacturing is the new No. 1 target of cyber criminals... ***page 34***

AGAINST THE WIND

Emerging from the global supply chain crisis will be a slow, choppy process... ***page 40***

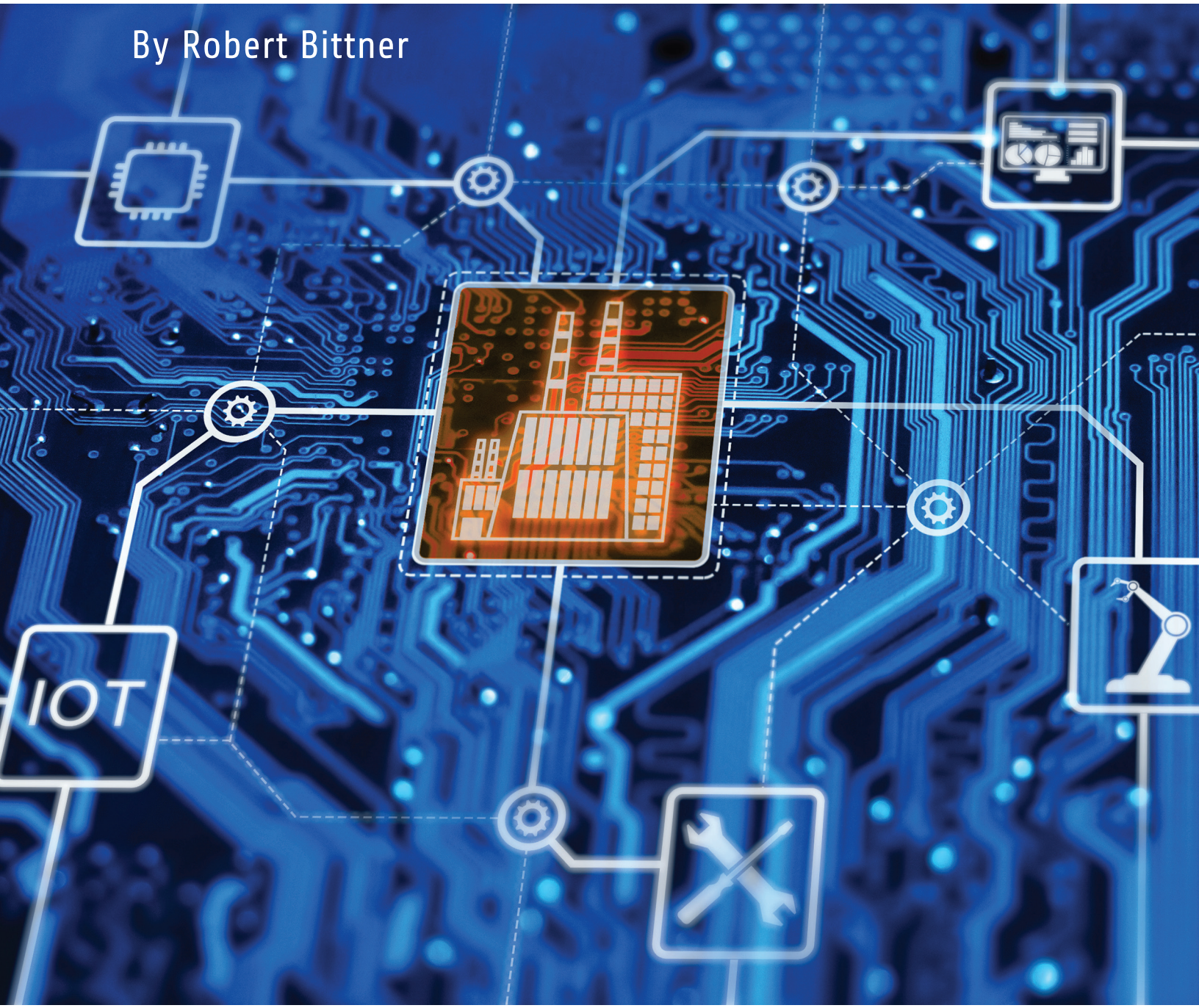
ILMA

OCT 2022 | V72 | NO 10

Under Attack

Manufacturing is the new No. 1 target of cyber criminals

By Robert Bittner



Every quarter, it seems, news breaks of a cybersecurity breach that exposes valuable data, disrupts business and results in financial losses. Last year, the big story was the Colonial Pipeline breach, which led to a six-day shutdown and $4 million ransom payment.

Previously, attackers focused their attention on financial institutions. Now, manufacturers are in the crosshairs. According to IBM's 2022 *Threat Intelligence Index*, "For the first time in five years, manufacturing outpaced finance and insurance in the number of cyberattacks levied against these industries, extending global supply chain woes. Manufacturers have a low tolerance for downtime, and ransomware actors are capitalizing on operational stressors exacerbated by the pandemic."

As attacks increase in frequency and sophistication, manufacturers are taking more comprehensive approaches to strengthening cyber defenses.

Surveying Manufacturing Cybersecurity

In July, the Manufacturing Leadership Council (MLC), the digital transformation arm of the National Association of Manufacturers (NAM), completed a survey on cybersecurity, its first since 2018. Over 160 manufacturers responded.

According to MLC Vice President and Executive Director David Brousell, cybersecurity is a top member priority. "We've seen a big jump in the percentage of manufacturers that have adopted formal plans and plant-floor strategies to combat cyberattacks," he said. "Nearly 62% of the survey respondents said they had put a formal plan in place. That compares to only 36% that reported having done so in 2018, which is a sign that manufacturers are taking cybersecurity very seriously."

Notably, companies are formalizing these strategies because they now see cybersecurity as an integral business issue, not an optional add-on. "This year, 83% said it was of high importance, compared with 66% in 2018," Brousell said.

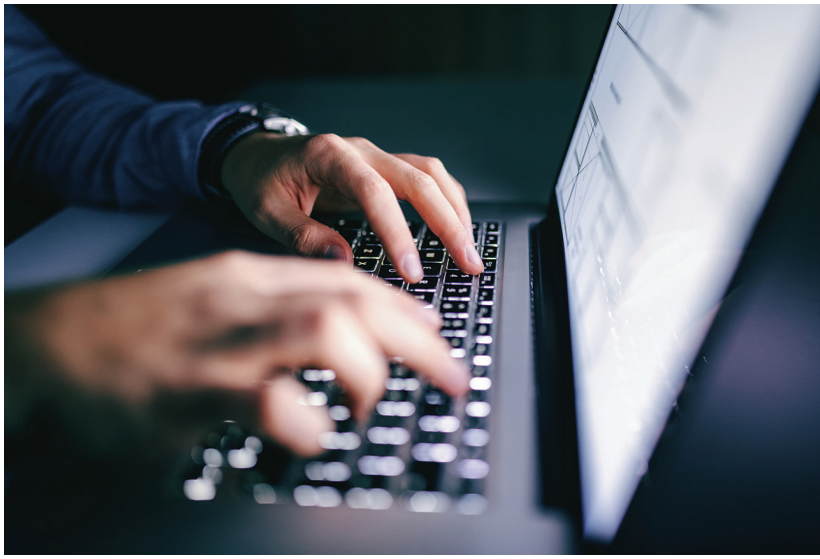
He pointed out that the No. 1 perceived risk for these companies is business disruption due to ransomware and other related attacks, not data theft. "Only 18% identified theft of information as a major risk, which is down from 2018, when it was 25%," Brousell noted. "The real risk is business disruption and the associated interruptions in operations that would impact them financially."

That anxiety reflects today's realities. "When a well-known, brand-name company gets hit with a cyberattack — like the Colonial Pipeline situation — it makes the news and gets a lot of exposure," Brousell said. "There also are more cyberattacks than ever before, with even small manufacturing companies getting hit. They don't get a lot of exposure — in fact, a lot of companies don't even want to talk about it, because they fear damage to their reputation or whatever — but 46% of this year's respondents said they have been attacked in the past, and 48% say that attacks on their companies, plant systems and networks have increased over the past year."

On the positive side, manufacturers reported increased confidence in their ability to manage cybersecurity issues. "This year, almost 40% of respondents were highly confident in their cybersecurity strategies, compared to 25% in 2018," explained Brousell. "So, they're getting better at raising this up as an issue in their companies, developing formal strategies and doing more frequent employee training and awareness training around cyber issues. A majority — 52% — now say they have dedicated budgets for cybersecurity, plant-floor cybersecurity, software training and education. That was well below 50% in 2018. That is significant, because the cyber landscape is changing, both in terms of

"The people within your business will ultimately determine how secure or how vulnerable your systems are. It is important to invest in educating them how to collectively protect the business from these risks."

***Aries Aquitania**, Vice President of Sales, Olyslager*



For Your Information

- To learn more about the Manufacturing Leadership Council's 2022 cybersecurity survey: manufacturingleadershipcouncil.com
- For information on the NIST cybersecurity framework: csrc.nist.gov
- For general information on a wide variety of cybersecurity frameworks: securityscorecard.com/blog/top-cybersecurity-frameworks-to-consider
- To see the IBM X-Force Threat Intelligence Index 2022: ibm.com/security/data-breach/threat-intelligence
- To read the Verizon 2022 Data Breach Investigations Report: verizon.com/business/resources/reports/dbir

attack frequency and attack sophistication. In fact, 78.7% expect more attacks in the year ahead than in the past year, which I think is a very dramatic finding."

The Weakest Links

Perhaps the most notable — and representative — example of the cybersecurity threat was the Colonial Pipeline breach in May 2021. The pipeline is one of the largest in the U.S., delivering refined oil for gasoline, jet fuel and home heating uses over a 5,500-mile span, from the Gulf of Mexico to the East Coast.

On May 6, hackers accessed Colonial Pipeline's systems, stealing 100 gigabytes of data in two hours. But they weren't finished. They then infected the pipeline's network with ransomware, which crippled a number of computer systems. To prevent the further spread of the ransomware, Colonial Pipeline shut down, affecting consumers and airlines all along the East Coast. Labeling the hack a national security threat, President Joe Biden declared a state of emergency.

While a team of federal law enforcement organizations worked behind the scenes, Colonial Pipeline paid the hackers $4.4 million in bitcoin to restore its data and regain the use of its systems. Six days after the initial attack, Colonial Pipeline restarted normal operations. Within a month, the U.S. Department of Justice recovered approximately half of the ransom.

That was the good news. The bad news: The Colonial Pipeline breach appears to have been completely preventable.

Attackers were able to gain access to the Colonial Pipeline network through an exposed password for a virtual private network (VPN) account. Typically, companies rely on VPNs to provide secure, encrypted remote access into a corporate network. However, a Colonial Pipeline employee was found to have used their Colonial VPN password for another site as well. The password was exposed when that second site was breached and its data compromised, and it became available to other hackers via the dark web, a part of the internet that requires specialized software for access and where all communication can be conducted anonymously. Had that password not been reused, this breach would not have been possible.

Aries Aquitania, vice president of sales for Olyslager, noted, "The people within your business will ultimately determine how secure or how vulnerable your systems are. It is important to invest in educating them how to collectively protect the business from these risks."

Security is everyone's responsibility, added Tom Rensink, Olyslager's chief operating officer and chief technology officer. "You are only as strong as the weakest link. That is why we not only have IT security measures in place, but all our employees are trained throughout the year, and we do various security awareness tests," he said. "In addition, we also involve our partners, and we look at this together."

Steps Toward Stronger Security

"Once you decide that something is valuable enough to be kept secure, then you have to do everything within your capabilities and restrictions to give it your best shot," said Aquitania. "As a data and solutions company, data protection is of utmost importance to our business. Not only do we gather data ourselves, but we also keep sensitive data for the hundreds of oil brands we work with globally. Keeping all of these secure is critical to our existence."

Security starts with employee education. "When I think about key factors in data security, I first think of our end users," said Chad Hudson, head of information security for Datacor Inc. "My job is to ensure that Datacor customer data is protected and that customers can trust our procedures and processes in terms of their information security. In a lot of companies, the users are where we see the most significant area of impact, both in terms of protection and also vulnerabilities. To develop that area, look at security-awareness training, enforcing multifactor authentication, ensuring good password hygiene and strength — that kind of thing."

Hudson noted that Verizon, in its *2022 Data Breach Investigations Report*, found that 80% to 85% of breaches are the result of employee actions, with around 60% involving some form of credential misuse — such as username, password or log-in identification. "If we can do a lot of education around those areas to strengthen the posture for users, that dramatically increases the overall organizational security posture," he said.

"Beyond that," Hudson continued, "there are a lot of things that can be done for fundamental information security: doing proper access reviews to ensure that we off-board employees when they leave the company, removing their access to information; reviewing your levels of permissions and authorization for different parts of your infrastructure or assets."

The cost for cybersecurity will, of course, vary from company to company. "A security budget of about 10% of your overall IT budget is an industry guideline," Hudson said — a good starting point.

"Where there's limited capability for spend, there are a lot of low-cost or no-cost improvements we can make to improve security hygiene," he continued. "There are a lot of

"Where there's limited capability for spend, there are a lot of low-cost or no-cost improvements we can make to improve security hygiene. There are a lot of things that can be done simply with software solutions, like password managers and multifactor authentication."

***Chad Hudson**, Head of Information Security, Datacor Inc.*

David Brousell

Vice President and Executive Director, Manufacturing Leadership Council

Tom Rensink

Chief Operating Officer and Chief Technology Officer, Olyslager

things that can be done simply with software solutions, like password managers and multifactor authentication."

While some larger companies can build out their security infrastructure and capabilities proprietarily, some might need to rely on vendors to provide those services. "Of course," added Hudson, "storing that information with a third-party partner carries some risk of its own. Before engaging a third-party vendor for any kind of cybersecurity product or service, conduct a risk assessment on that vendor to ensure that the risk is appropriate to the business."

Finally, companies are turning to cybersecurity frameworks for help in establishing, assessing, and monitoring cybersecurity best practices. "Cybersecurity frameworks essentially provide guidelines or benchmarks for evaluating your security structure in light of potential risks," Hudson explained.

NIST, developed by the U.S. Department of Commerce's National Institute of Standards and Technology, is perhaps the leading compliance framework for North American companies, with nearly 60% of the MLC's survey respondents stating that they used NIST for mitigating cyber risks. Other popular frameworks include ISAC, FISMA, GDPR, HIPAA, ISO 27001/27002, NERC-CIP and SOC2. (See sidebar, p. 36, for links to additional information.)

A Never-Ending Race

Regardless of the specific cybersecurity strategy, companies should regularly review their approach, Hudson advised. "Most compliance frameworks recommend an annual assessment. That can be challenging," he said. "Those frameworks cover a lot of areas, so trying to assess everything at one time, once a year, is pretty difficult. I think companies need to be performing at least a minimal review constantly."

"Try to think like a hacker," Rensink said. "It is an endless race."

Bittner *is a Michigan-based freelance journalist and a frequent* Compoundings *contributor.*