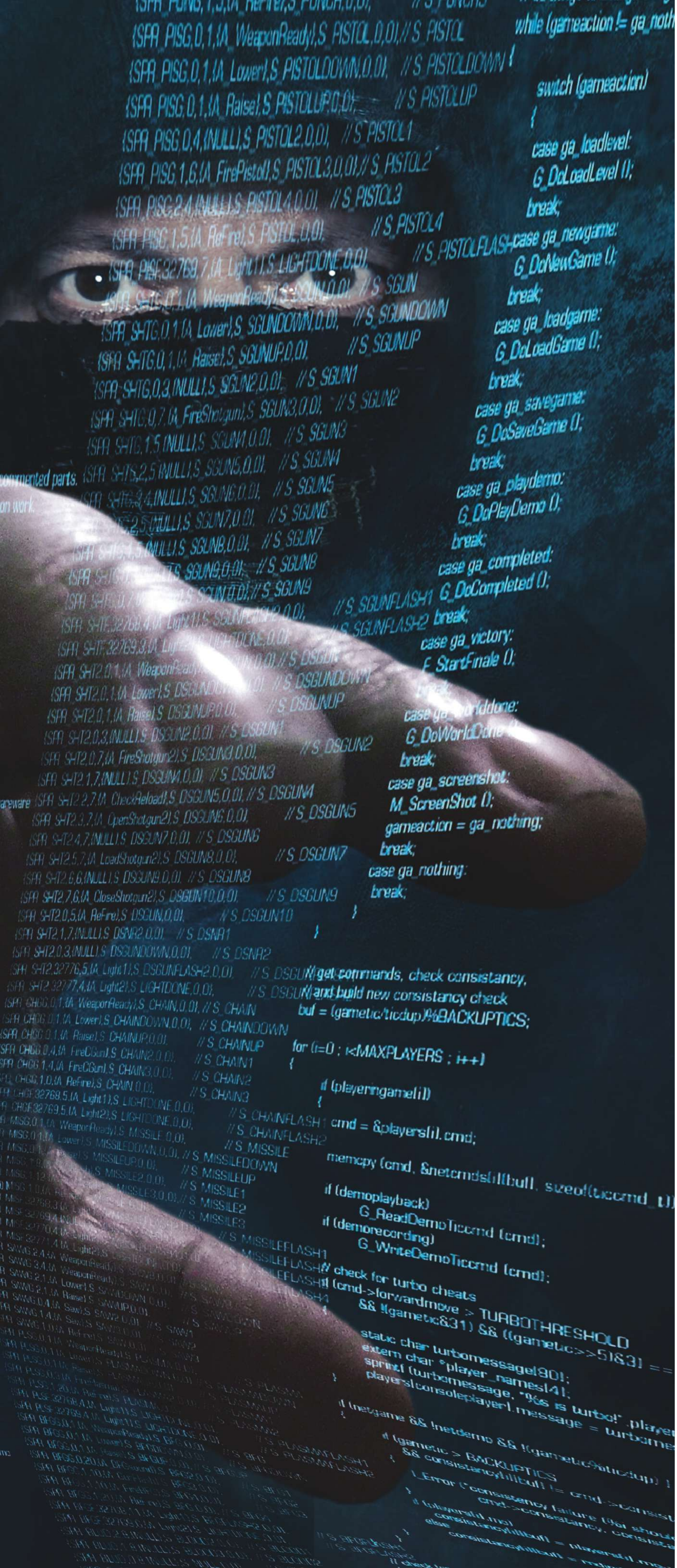
# CYBERSECURITY – the No. 1 threat facing manufacturers

BY ANDERS ERICKSON AND TODD NEILSON

## EXECUTIVE SUMMARY

Manufacturers are the No. 1 target for business cyberattacks. Cybersecurity is a two-headed beast that every business must tame. The invasive damage cyberattacks and hackers torment companies with is juxtaposed against how companies remain ignorant and resistant to effectively doing what must be done to achieve cybersecurity. Cybersecurity is a problem that manufacturers, or for that matter any company, can't ignore if they expect to survive.



Cyber risk is business risk. The cyber threat condition that now escalates concern over business data and asset security is somewhat driven by a self-fulfilling prophecy. Due to the integration of more technology built into the very fabric of an organization's day-to-day operations, those technology touch points have become the breeding ground for cyber insecurities. For manufacturing environments, this is more true right now than in other types of business environments.

Becoming more efficient, increasing quality, reducing expenses and driving productivity are the strongest pressures as to why more and more technology continues to be implemented. While this has enabled manufacturers to operate at performance and revenue levels never achieved before, it has also brought the loss of critical assets, data and relationships that cyberattacks create.

Hackers largely target the manufacturing industry to steal trade secrets, business plans and valuable intellectual property.

Manufacturing organizations must take on the responsibility and investment of implementing the right cybersecurity measures to avoid these losses. Without significant cybersecurity-driven change, U.S. manufacturers may erode strategic partnerships and customer confidence, which will generate a hard hit to the bottom line.

## Areas most affected

Hackers largely target the manufacturing industry to steal trade secrets, business plans and valuable intellectual property. But there are at least three broad categories under which most cyberattacks and threats occur:

**Espionage and intellectual property theft:** When things are made well, they become a target for other companies, organizations and even nation-states. If they can just steal what they need rather than investing the time, money, expertise, research and the other thousand layers of processes and resources needed to get from A to B, many will not hesitate to resort to theft in order to gain a competitive advantage. Hackers see manufacturer business plans, trade secrets and intellectual property as an extremely lucrative venture.

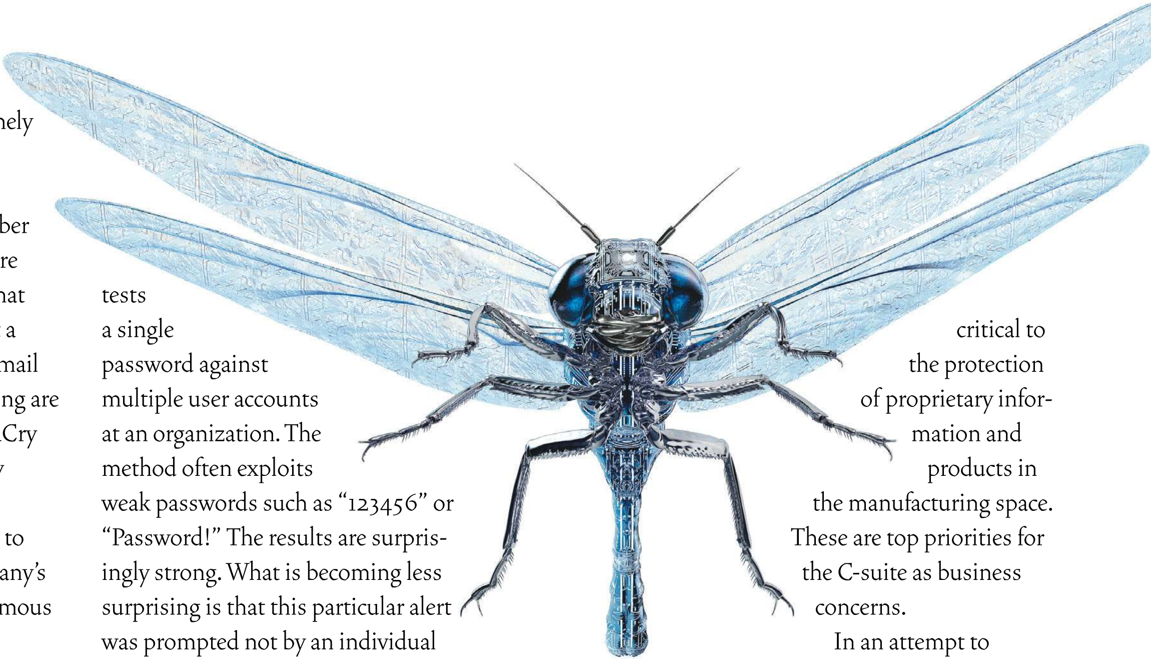
**Ransomware for revenue:** Ransomware is an example of cyber extortion. Ransomware attacks are usually undertaken by a Trojan that is designed to look like a file that a user downloads or opens in an email attachment. Even more devastating are worms such as the recent WannaCry attack that traveled automatically between computers and users. Ransomware is usually designed to encrypt data and prevent a company's access to the data until an anonymous payment is made to the hacker. Many times, even after payment, the encryption keys are not provided, and access to the data is not granted. Those who engage in ransomware are almost always out for money. In other words, it is a business; the intent of ransomware is to gain a return on investment.

**Pure destruction and harm:** For some, the purpose of hacking is not for financial gain but rather to cause damage for political or emotional purposes. According to *Wired* magazine, one of the first confirmed cases of a cyberattack against manufacturing that caused physical damage occurred in 2015 when hackers struck an unnamed steel mill in Germany. They were able to gain access to the network and disrupt control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive" damage.

## Evolving attacks

Hackers are getting more creative. In March, the FBI and U.S. Department of Homeland Security issued a warning to American businesses that hackers are using a new attack called password spraying.

"According to information derived from FBI investigations, malicious cyber actors are increasingly using a style of brute force attack known as password spraying against organizations in the United States and abroad," the agencies said in a US-CERT technical alert.



In a password-spray attack, a hacker tests a single password against multiple user accounts at an organization. The method often exploits weak passwords such as "123456" or "Password!" The results are surprisingly strong. What is becoming less surprising is that this particular alert was prompted not by an individual acting alone, but by a federal indictment against nine Iranian nationals associated with the Mabna Institute, which is a private Iranian-based company accused of hacking on behalf of the Iranian state. The indictment was focused on a four-year spear-phishing campaign to steal credentials from thousands of university professors whose publications could allegedly advance Iranian research interests.

Manufacturers need to understand that when they find themselves in the crosshairs, beyond the loss of money, damages can easily add up to a litany of loss, including (but not limited to) the following:

- Harm to reputation
- Destruction of data
- Loss in productivity
- Theft of intellectual property
- Theft of personal employee data
- Disruption to business continuity
- Damage to physical facilities
- Liability or fines for noncompliance with data-privacy regulations
- Possible legal action by customers and employees whose personal information has been breached or employees suing for lost wages if the company can't pay due to the breach
- Costs of remediating the damage itself

At their core, having secure production environments, functional networks and trusted supply chains are critical to the protection of proprietary information and products in the manufacturing space. These are top priorities for the C-suite as business concerns.

In an attempt to protect them, traditionally, business leaders would turn to their information technology departments to determine strategies for mitigating cybersecurity risks. After all, it's a threat involving technology, and therefore technologists would be the ones who would be equipped best to handle it.

The challenge of this approach is that not only does the IT team speak a different language than the C-suite, that team also has different priorities than the CEO, chief financial officer or even the chief information officer. The IT department has approached solving the issue by installing more software and more tools. There is a better way.

Manufacturers need to understand that when they find themselves in the crosshairs ... damages can easily add up to a litany of loss.

## C-level strategy

Cybersecurity should be a top-down issue. Instead of just throwing it over the fence to the IT team and hoping team members understand the business's priorities, it has become clear that both sides of the company need each other. The C-suite needs to embrace and own cybersecurity as it would other business risks. This will also empower the IT department to take a more strategic approach.

The key is how the organization looks at risk. Businesses face risks of all types: competitive risk, where the competition does something to gain competitive advantage; economic risk, where commodity prices increase suddenly; operational risks, where processes such as customer support collapse; legal risks, where the company gets sued; credit risks, where accounts receivable stops receiving checks; compliance risks, where the company violates regulations (even with the best intentions); and many, many more.

The common thread among all of these is that they are business risks. Cybersecurity is also a business risk. It should be treated in the same way as all of these.

As such, the proper approach should be for the business leadership to think of cybersecurity simply as any other risk. If it does, the process is as follows:

1. Executives identify business risk.
2. Business impact assessed: How does the risk impact the business?
3. The company makes a control recommendation designed to address risk.
4. The company finds the best product, process or procedure for control to address the risk.
5. The company mitigates, ignores, accepts or assigns the risk based on the control.
6. The company addresses business risk and technical risk.

Working together is the key. To mitigate and manage cyberthreats, the C-suite cannot and should not do it alone. A team effort helps create a safer and more cybersecure business when involvement and cooperation is had from all areas of the business.

When working to shore up cybersecurity risks, the following three questions should be asked:

1. What is the business impact if data is not available? Take one company, for instance. This commercial builder got hit with a ransomware attack. The attacker encrypted files on both the company's file server and backup server, which made the data inaccessible unless the company paid the ransom. The builder had a bid that was due in the next couple of days that was worth more than $1.5 million for a large commercial project, and the plans for that project were part of the encrypted files. The company did not get its bid in on time due to the breach and lost this business opportunity because that data was unavailable.
2. What is the business impact if the integrity of data is altered or changed? Data integrity is vital to companies that use key information for credit cards, invoice numbers, patient records and similar type information. A healthcare company offered its customers a portal that allowed clients to enter their customer identification and pay their bill. However, the web application did not check to ensure the integrity of the ID number and assumed that the client would enter it correctly. Hackers simply accessed the portal, entered random ID numbers into the application until they found a correct one, and then proceeded to take information associated with that account. If the integrity of the account number was protected and checked, this could have been prevented.
3. What is the business impact if the data is lost or stolen? Data that is lost or stolen has value to those who know how to monetize it, but the real impact to a business can be measured in a number of areas, including brand and reputation with clients and prospects, legal liability, cost of remediation to victims for their loss of data and fines for noncompliance with state and federal laws. There are countless examples of lost or stolen data that impacted companies in this way, including TJ Maxx, Target stores, Sony and Yahoo just to name a few.

These are foundational questions that should be asked to improve cybersecurity. There is no mention of what tools should be used or what technology threats they are facing. These are business questions that the C-level team owns and lives with. They are of central importance to a manufacturer's operational strategy.

Furthermore, many honest IT people will admit that they are not cybersecurity experts. Companies hire lawyers who are expert at law. They hire accountants who are expert at taxes and accounting. Depending upon the size and ability of your IT department, you can hire staff to handle your cybersecurity concerns or you can go the outsourcing route for experts. Either way, all your stakeholders must work together to establish strategy and strengthen the business against an attack and mitigate interruption to business operations when (not if) a breach or attack occurs.

To mitigate and manage cyberthreats, the C-suite cannot and should not do it alone.

Managing the risks inherent to running a business today requires dedicated expertise to develop the infrastructure necessary for small and large companies to provide strategic, tactical and day-to-day incident response.

When executives, the IT department and experts come together in cooperation, addressing cybersecurity can provide substantial business benefits. One of the intangible elements that comes from taking a different, top-down approach to cybersecurity is the opportunity to increase brand and corporate reputation with better security messaging. Manufacturers can discuss with prospects and employees the proactive approach they are employing to keep their systems and production environments safe.

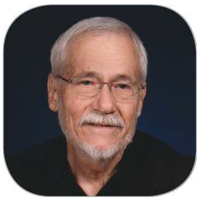
## Cyber risk is business risk

Because of the cyberthreat condition that now permeates the global business ecosystem, companies have to take a different approach to cybersecurity. Company leaders need to take an active role in identifying business priorities and company risks. This type of leadership is not only needed, it is the only way that a healthy, holistic and effective strategy can be created for each individual manufacturing business environment. ❖

# contributors
## in this issue

Christopher Bailey

Terence T. Burton


Donald L. Caruth

Gail D. Caruth

Anders Erickson

**Christopher Bailey** is an innovation catalyst with ExxonMobil, where he has spent the last 12 years working to create the innovative and inclusive environment he and others love to work in. Bailey seeks out diverse sets of creative partners to create innovation services, education and consulting at ExxonMobil. He has a master's of information systems management from Brigham Young University.

**Terence T. Burton** is founder and president of The Center for Excellence in Operations Inc. (CEO), a professional management consulting firm specializing in strategic and operational transformation. Burton has more than 40 years of executive operations and supply chain experience as an industry executive and has consulted on major strategic improvement initiatives with more than 400 clients in 23 countries around the globe. His latest book is *Global KATA: Success Through the Lean Business System Reference Model.*

The late **Donald L. Caruth**, Ph.D., taught management at a number of universities for more than 40 years and was an independent management consultant for more than 100 companies. He earned the designation of Senior Professional in Human Resources. His articles appeared in more than 100 professional and academic journals.

**Gail D. Caruth**, Ed.D., is a former human resource manager as well as an organizational consultant. She holds the professional designation of Senior Professional in Human Resources. Her articles on human resource management, adult learning and higher education have appeared in more than 80 academic and trade journals. She serves as an editor, member of the editorial board or reviewer for a number of academic journals.

**Anders Erickson** is the director of cybersecurity services at Eide Bailly, a business management firm that has been around for more than a century. He is a certified information system security professional, a certified information systems auditor and is certified in risk and information systems control. He has a master of information systems management from Brigham Young University.

Kyle T. Jones

Todd Neilson

Andrea Belk Olson

Jeffrey Rosenbaugh

**Kyle T. Jones** is a data science and analytics advisor for ExxonMobil. He specializes in big data analytics and research and development management. He is a certified project manager (PMI-PMP) and holds a doctorate in systems engineering from George Washington University and a master's in public administration from Harvard. His work has been published in *IEEE Engineering Management Review* and the *International Journal of Business and Management*.

**Todd Neilson** is the chief technological officer of Secuvant. He has spent more than 30 years delivering solutions in the areas of technology services, security management and threat detection infrastructure, including implementing multimillion-dollar IT security solutions for Fortune 500 companies.

**Andrea Belk Olson** is CEO of Pragmadik, an operational strategy consultancy, and also director of the Midwest Manufacturing Business Coalition, a nonprofit organization dedicated to the advancement of midmarket manufacturing in the United States. The author of *No Disruptions: The New Future for Mid-Market Manufacturing*, Olson is inspiring and educating industrial business leaders on how to transform their outlook and approach to marketing, technology and communications for more efficient operations and increased profitability. She has more than 20 years of experience in creating leaner, more effective, technology-driven, customer-facing operations. The four-time ADDY award winner began her career at a tech startup.

**Jeffrey Rosenbaugh** is evolve program manager at ExxonMobil. He has spent his career coaching on innovation, searching out bleeding edge technology and evangelizing agile/DevOps organizational transformation. He went to Brigham Young University.