Harvard Business Review
ANALYTIC SERVICES

Pulse Survey

CYBERSECURITY AND THE INDUSTRIAL INTERNET

Sponsored by

SIEMENS
Ingenuity for life

DR. ROLAND BUSCH

CHIEF OPERATING OFFICER AND CHIEF TECHNOLOGY OFFICER

SIEMENS AG

The digital world is changing everything. Billions of devices are connected through the Internet of Things. This holds great potential for everyone, but also great risk.

That's why we are convinced that cybersecurity is crucial to the success of and eventually the only limiting factor for a fast growing digital economy. People and organizations need to trust that their data and networked systems are safe and secure.

There is more to it than just technology; cybersecurity must become part of the DNA of every organization, like it is for quality in outperforming companies. Anyone that intends to supply secure products and systems to the market, and maintain cybersecurity along their entire life cycle, needs a holistic cybersecurity strategy that is clearly formulated and consistently implemented across the entire organization.

In our company, we made cybersecurity a top priority. We hold ourselves accountable to the highest standards. Therefore, we initiated the Charter of Trust with 10 guiding principles making the digital world a safer place. Siemens and its global partners launched the Charter at the Munich Security Conference 2018 and have actively promoted it ever since—with success, as an initial review clearly shows. In terms of content, politics and organization, the initiative made important progress in its first year and the partners have set themselves ambitious goals for the future.

The power of the Charter of Trust stems not only from the fact that it is driven from the very top of the organizations involved or that it is a cross-industry initiative, but also that it is based, first and foremost, on the principle "lead by example."

The goal of the Charter is to protect the data of individuals and companies; to prevent damage to people, companies, and infrastructures; and to create a reliable foundation for fostering trust in a networked, digital world.

For us, cybersecurity is not a new topic. The first IT Security team at Siemens was set up in 1986—about 30 years ago—at the central research department Corporate Technology.

And with our Chief Cybersecurity Officer Natalia Oropeza, we have anchored our responsibility for cybersecurity even more firmly in our company. Together with our new cybersecurity organization, she is driving this important topic forward. We have an ecosystem in place consisting of more than 1,200 cybersecurity experts who have technical expertise in cybersecurity as well as extremely deep domain knowledge. They secure our own IT and OT infrastructure, and make sure that the products, solutions and services we deliver to customers have the highest possible security. They also develop cybersecurity solutions for various industries.

This survey is part of our efforts to raise awareness for cybersecurity not only as a threat to the digital economy but also to highlight the opportunities the industrial internet holds for different sectors and how to leverage them. I invite you to look at the survey to learn about the challenges that decision makers in different industries face and how they deal with cybersecurity in their organization.

CYBERSECURITY AND THE INDUSTRIAL INTERNET

Industrial and non-industrial companies alike are racing toward digitalization. The benefits of automation, connected devices, and artificial intelligence are simply too enticing to ignore. CEOs and their boards anticipate greater efficiencies, new competitive opportunities, and the ability to better serve and delight customers. Even companies that don't have a clear view of the potential benefits often feel the hot breath of new digital competitors on their backs. It's hard to find a CEO today who doesn't believe their company's future—if not their present—is digital.

In a recent survey from Harvard Business Review Analytic Services, only 10% of respondents said their company was "not digital," with few if any of their products, operations, and business model/s dependent on their ability to exploit digital information and technologies[1]. FIGURE 1 Half (51%) described their business as "moderately digital," with less than half of their products, operations, and business model/s dependent on digital, and 39% described themselves as "very digital." This is an increase of 10 percentage points from a similar survey conducted a year ago.

This is a big change for industrial and infrastructure companies (manufacturers, utilities, hospitals, shippers, chemical plants), where information technology (IT) and operational technology (OT) have existed in separate silos. To gain the benefits of digitalization, the two must be fused.

"IT is going to win," said Ed Amoroso, CEO of TAG Cyber and former chief information security officer (CISO) of AT&T. "The force is too strong. The cost savings are too significant. The capabilities are too numerous. There are just too many reasons to not be running Windows on a factory floor. And that's already happened—that ship has sailed. The ship that hasn't sailed is to control factory floors in the cloud." Boards and CEOs looking to increase margins are eager to do more.

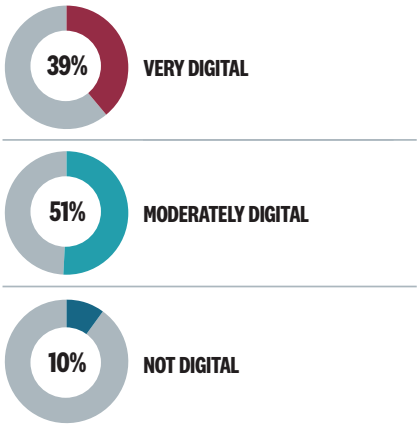
Predictive maintenance has been one of the transformative applications of digitalization for industrials. "It makes sense on every level," said Sven Schrecker, co-chair of the Industrial Internet Consortium's (IIC's) security working group and vice president and chief architect for cyber security at LHP Engineering Solutions. "It's cost savings. It ensures the uptime and the reliability of the equipment [and provides] better monitoring, better financial resource utilization and planning, etc. So really there's no downside to predictive maintenance."

51%
OF RESPONDENTS DESCRIBED THEIR BUSINESS AS "MODERATELY DIGITAL," WITH LESS THAN HALF OF THEIR PRODUCTS, OPERATIONS, AND BUSINESS MODEL/S DEPENDENT ON DIGITAL.

39%
DESCRIBED THEMSELVES AS "VERY DIGITAL." THIS IS AN INCREASE OF 10 PERCENTAGE POINTS FROM A SIMILAR SURVEY CONDUCTED A YEAR AGO.

FIGURE 1

HOW DIGITAL IS YOUR ORGANIZATION?



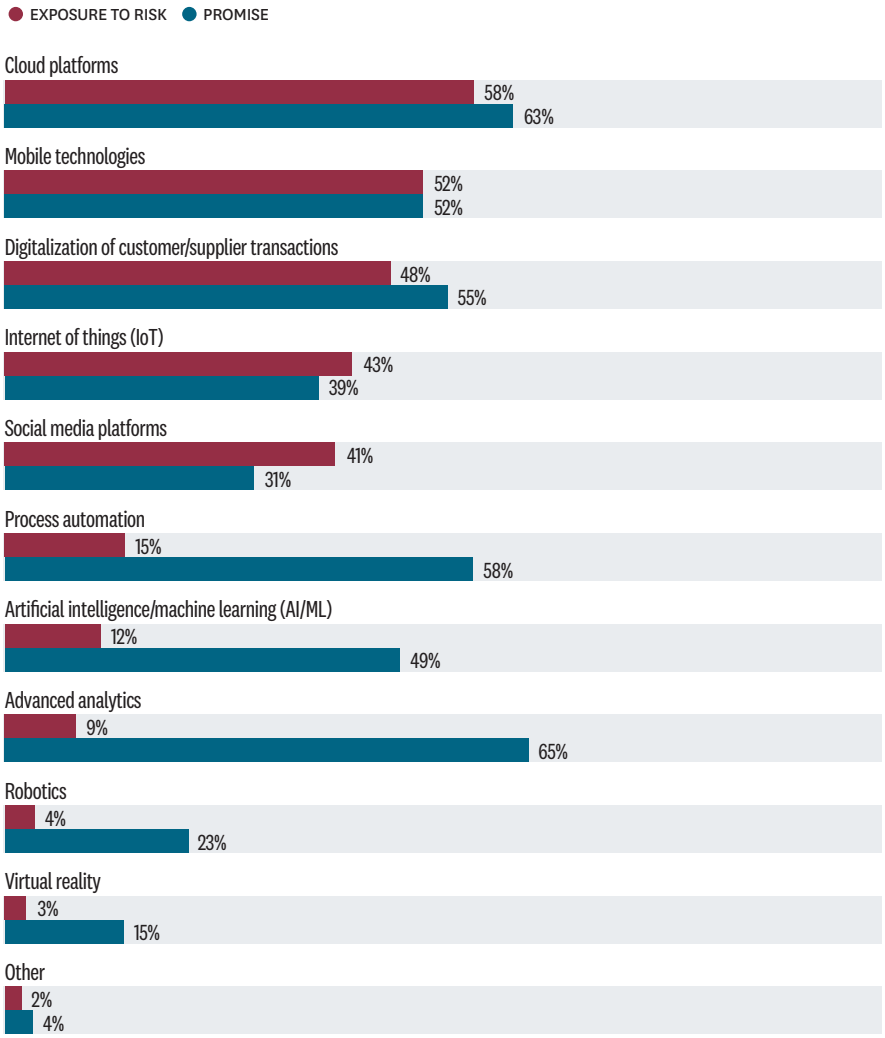
SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2018

1 Note that due to the low number of respondents in the "Not Digital" group (29 respondents, or 10%), these statistics should be considered directional, not definitive

FIGURE 2

TECHNOLOGY PROMISE VS. RISK

Which digital technologies hold the greatest promise for your organization? Which create the greatest exposure to cybersecurity threats?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2018

INDUSTRIALS ARE TWICE AS LIKELY TO SAY IoT HOLDS SIGNIFICANT PROMISE FOR THEIR BUSINESS (50% VERSUS 26%).

However, unlike with traditional OT systems, "in predictive maintenance these things, whatever they are—electric generators or hospital equipment—need to be monitored, and those monitoring results need to be aggregated in some kind of intelligence platform," Schrecker said. "That requires connectivity, and so now you need to move this data, which means it can't be on dedicated lines. There has to be a path into the open internet to pass this data out, which means the return path is also possible."

Exposing IT and OT systems to the internet increases the risk of cybersecurity threats. Nearly two-thirds of survey respondents (64%) say that digitalization has increased their organization's exposure to risk from cyber threats. Not surprisingly, those whose organizations have experienced a cyber breach in the past year are the most likely to take this position, with more than three-quarters (76%) saying digitalization creates higher risk.

For many companies, this is not just a matter of taking on somewhat higher risk in order to gain the advantages of digital. More than a quarter (26%) of all respondents say digitalization creates significantly higher risk for their organization. While some might speculate that this is simply unwarranted fear of the unknown, that's hardly the case. Those with experience—companies that are already very digital, and those that have experienced a breach in the past year—are nearly twice as likely to say digitalization creates significantly higher risk from cyber threats.

The challenges are not likely to get easier. There is near unanimous agreement (92%) that cyberattacks will increase over the next two years. Three-quarters of respondents (76%) strongly agree. To thrive as a digital industrial, companies must prepare.

"What really matters in industrial is that we have trustworthy systems," said Schrecker. "The value that the technology brings is just so great that it can't be ignored, and so the problems have to be addressed."

Interestingly, while respondents say that digitalization increases their exposure to risk, companies that are already very digital are the most confident that they are very well prepared for a cyber attack, with 62% saying so compared with 21% of not digitals and 42% of moderately digitals.

The Leadership Mandate

With potentially high benefits on the one hand and seemingly certain risk

on the other, strong oversight and leadership of cyber risk is crucial, experts agree. FIGURE 2 "One of the first things you need to do is balance the board with people who have deep cyber instinct," said Amoroso.

It appears that boards and executive committees (ExCos) are stepping up. Close to two-thirds (64%) of survey respondents say that cybersecurity is a board or executive-committee level issue at their company. That number jumps to 80% at companies that are already very digital, while it drops to 48% at not-digital companies. FIGURE 3

What that really means is open to interpretation, Amoroso believes. "In an energy company, for example, you're going to have a CEO and a bunch of executives who know the energy business, but when you start talking about cloud, virtualization, utilizing the power of mobility, software-defined infrastructure, they're going to go, software-defined what? They don't even know what that is." Business leaders need to accelerate their own learning and supplement their ranks with real expertise in digital capabilities and cybersecurity.

The most common way senior leaders increase their understanding is from their company's own cybersecurity experts (named by 63% of respondents), followed by industry peers (46%) and consultants/analysts (44%). This is just one reason to prioritize the hiring of a capable chief cybersecurity officer.

This has yet to happen. Despite having elevated cybersecurity to be a board and ExCo issue, only 37% of respondent companies have a chief cybersecurity officer reporting to the highest level of their organization. Very digital companies are more likely to do so, but even there, only half (49%) have a senior CSO. FIGURE 4 It will be extremely challenging for industrials to operate with confidence in the digital era without having this kind of talent on board.

Industrial companies are even less likely to have a very senior cybersecurity officer than non-industrials (34% versus 41%). However, those that do are fairly likely to have that person responsible for both IT and OT security, at 69%. This is important, as IT and OT converge.

"Security is security," said Richard Soley, executive director of the Industrial Internet Consortium. "You've got to have the same person involved in both. Traditionally, the chief security officer has been involved in physical security and cybersecurity but not operational security as such.... I think eventually you're going to see one person responsible for both, but it's going to take some time because the IT people don't want to talk to the OT people and vice versa."

Respondents had fairly strong faith in their boards' and executive committees' understanding of the costs of a potential cybersecurity incident, at 58% overall. Very digital companies were much more likely to have faith in this understanding, at 69%, compared with 52% of moderately digitals and 41% of not digitals.

Despite understanding the costs, investment in cybersecurity still lags. Fewer than half of respondents (47%) say their company places a high priority on cybersecurity as part of its digitalization efforts, investing adequate resources. Very digitals do better, at 62%, but that's still nearly 20 percentage points behind the number

FIGURE 3

BOARD LEVEL ISSUE

Is cybersecurity a board or executive-committee-level issue at your company?

ALL SAYING YES

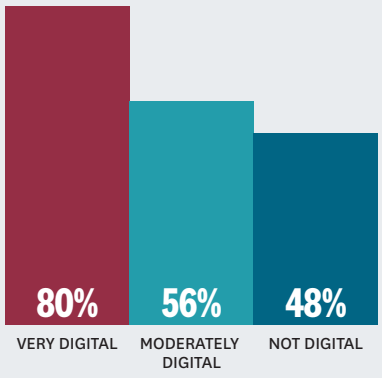


FIGURE 4

CHIEF CYBERSECURITY OFFICER

Does your company have a chief cybersecurity officer reporting to the highest level of the organization?

ALL SAYING YES

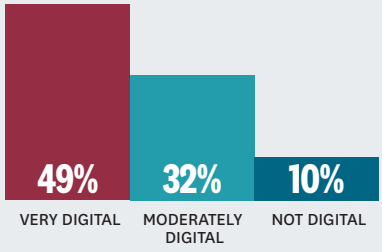
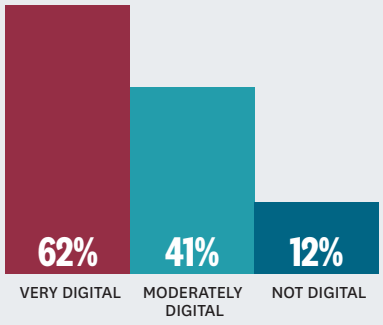


FIGURE 5

HIGH PRIORITY

To what extent does your company prioritize (i.e., invest adequate resources in) cybersecurity as part of its digitalization efforts?

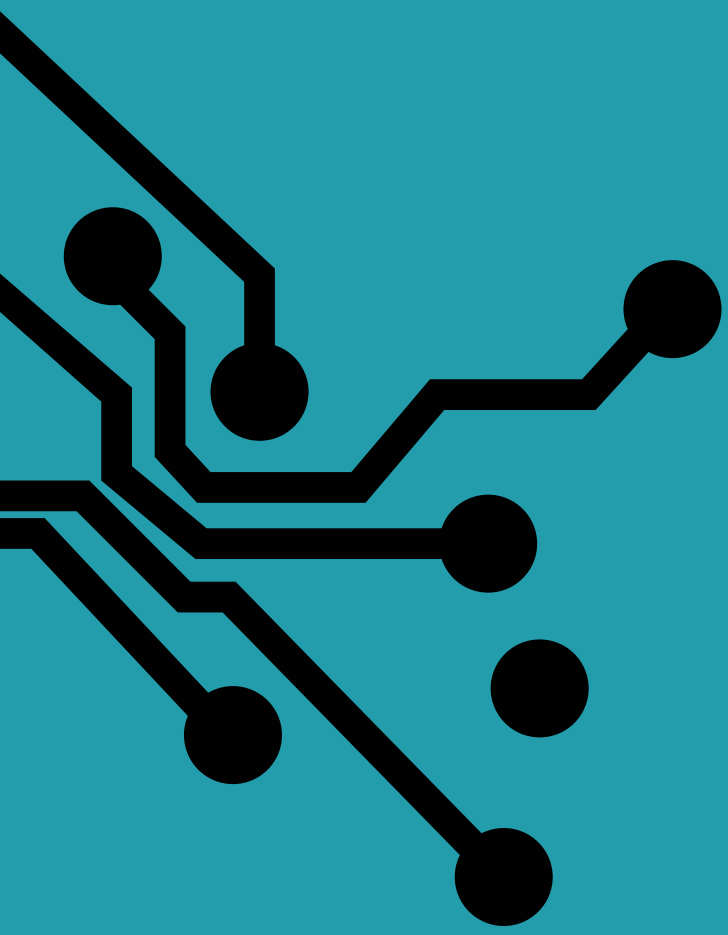
ALL RATING 8-10 ON 10-POINT SCALE



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2018

"IF YOU BECOME AN INCREASINGLY DIGITALLY ADVANCED—AND THEREFORE DIGITALLY DEPENDENT—BUSINESS, YOU HAVE TO TAKE ON THE CYBER RISK ASSOCIATED WITH THAT."

JOEL JACOBS, CIO AND CSO,
THE MITRE CORPORATION



who claim it to be a boardroom issue. The gap is even greater at not digitals, with 48% saying it's a boardroom issue, but only 12% saying it has been made a high priority with adequate investments. FIGURE 5

"If you become an increasingly digitally advanced—and therefore digitally dependent—business, you have to take on the cyber risk associated with that," said Joel Jacobs, who is both chief information officer (CIO) and chief security officer (CSO) for the MITRE Corporation, a not-for-profit company that operates federally funded research and development centers for a variety of government agencies. "If you don't, you're saying, I'm going to take on this business in this way and I'm not going to worry about the risk elements that come as an inherent part of that. CEOs need to recognize that if transactions and customer relationship arrangements are increasingly through digital means, then your business and your customer's trust in your business are dependent on your security assurance. Lose that assurance and you lose their trust—and your customer."

Leading infrastructure companies understand the importance of underpinning digital operations with strong cybersecurity, according to Michael Assante, director of critical infrastructure and industrial controls systems at the SANS Institute. The SANS Institute includes presentations on its website from members that showcase, "here's how we're digitizing and here's how we've structured a security program to tell you how to deal with all this new technology that we're bringing in," he said. "They're saying, look, our business really digitized and we made this big investment. And at the same time, we had to grow the security capability because we quickly realized that we exposed ourselves with these investments."

An important part of building that capability is investing in the knowledge of frontline professionals. "It's really important that the engineers for a facility understand their responsibilities and obligations, and that the corporate center provides resources to them," said Assante.

AN IMPORTANT PART OF BUILDING A SECURITY CAPABILITY IS INVESTING IN THE KNOWLEDGE OF FRONTLINE PROFESSIONALS.

"You can't just say, great, I want to take advantage [of digitalization] and become lean, or I want you to keep pushing the productivity limits, [without making] resources available to make our average engineer on the floor a little more cybersecurity aware. We need to budget for that."

Increasing Trust through Openness and Working Together

Around a third (35%) of respondents participate in industry-, government- or academia-sponsored groups or consortia to share cybersecurity information and best practices. A similar percentage say they do not, and 28% say they don't know. Very digitals are four times as likely as not digitals to participate in such groups (46% versus 10%).

Collaborating with partners to secure systems is becoming increasingly important—for the same reason that cybersecurity in general is. "Everything's interconnected; you can't just protect yourself," said Amoroso.

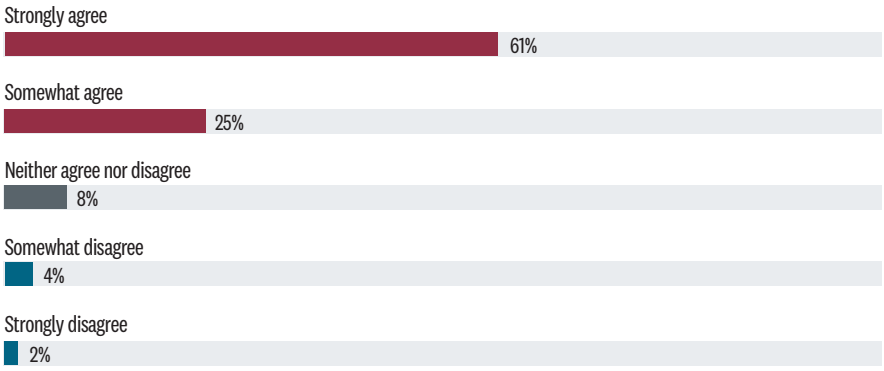
Assante used the example of a large U.S.-based industrial firm to illustrate that point. The company polled its industrial internet customers about how they were managing their cyber security because, being in a cloud model, "one customer is exposing all their other customers," he said. "And so, companies like this started thinking, gee, we've got to really think through the security that our customers provide themselves. That's important to our business model [because their security] is our security."

"The problem that we've got with IT is that the weakest link exposes the entire chain," said Bob Hayes, managing director of the Security Executive Council, a peer-based advisory organization for chief security

FIGURE 6

NEED FOR CROSS-INDUSTRY STANDARDS

The digitalization of industrial and infrastructure operations creates a need for cross-industry cybersecurity standards.

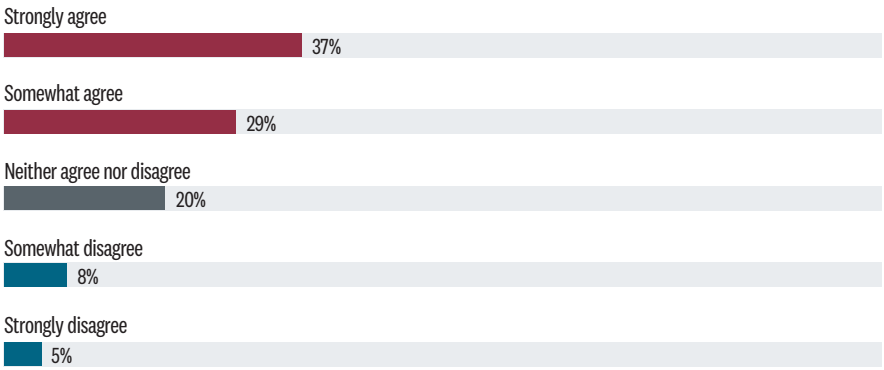


SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2018

FIGURE 7

NEED FOR MORE GOVERNMENT REGULATION

More government regulation is necessary to protect industrial operations and critical infrastructure in the digital age.



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, AUGUST 2018

officers. It becomes incumbent on more sophisticated partners to help others in their supply chain or ecosystem evolve.

"There's a pay-it-forward value proposition in these things," said Jacobs. "If you are the best in class, you get less back. But if the best stop participating, the value proposition erodes."

Given all the endpoints and connections in a digital infrastructure, old models of managing security simply won't work, experts agree. "The ecosystems that we're building for a digital factory or digital infrastructure have to be able to scale and change at speed," said Vernon Turner, principal and chief strategist at Causeway Connections, and executive analyst at Ecosystm. "We want to onboard a new sensor into this ecosystem. We can't wait for everybody to approve it.... We have to have enough trusted advisors inside the system to say, yes, it's okay to onboard this device or pass this data from the factory floor into the public cloud securely."

In the future, that "trusted advisor" will likely be automation based on approved standards, but to get there will require a lot of collaboration and agreement among connected parties. At the moment, "it's very hard to define what is needed because there are no comprehensive standards," said Schrecker.

A significant majority (86%) of respondents say that cross-industry cybersecurity standards are necessary as industrial and infrastructure operations become more digital; 61% strongly agree. FIGURE 6 Respondents were somewhat less certain about the need for more government regulation, with two-thirds (67%) saying they believe more government involvement is necessary, and a little over a third (37%) strongly agreeing. FIGURE 7

The Industrial Internet's Soley sees industry collaboration leading to standards, which can then be used for regulations. "We're going to find commonalities that eventually will turn into standards of practice that can be required by governments. But I don't think we're close to that. I think that we will get [regulations] before we have

the standards of practice," Soley said. Such premature regulation can make it hard for companies to do business—or are simply impossible to enforce. For example, Soley said, "a year and a half ago, the digitalization commissioner of the European Commission announced that they were no longer going to allow the sale of IoT devices in the EU unless they passed a security test, which sounds really good. The only thing that was missing was the security test. He's no longer the digitalization commissioner, and I already heard from several makers of IoT devices that what they were going to do in Europe was simply not call their devices IoT devices."

But there are other ways governments can help. "This is a constant arms race," said MITRE's Jacobs. "Conditions keep changing, and some of the information and understanding can only be seen by aggregating the challenge. The government is often in a position to do that more than others." The challenge is that not all the information or control systems are government systems. "To increase assurance and protection of the most important things" means collaborating and sharing information with industry groups.

"I think companies would like to see government solve some of the problems for them," said Soley. "They've been trying to get governments to solve the internet security problem for them for a long time." But that doesn't let them off the hook to manage their own security, he said. "That's like saying I don't have to lock my door because the government is going to come check." Industry still needs to do its part.

The likelihood that an organization will share information about cybersecurity not just in a confidential setting of an association or information-sharing group but with employees and the public is very evenly distributed across the spectrum from highly unlikely to highly likely. Twenty-eight percent say they are very likely to share (scoring it 8-10 on a 10-point scale); 28% say they are very unlikely to share (1-3), and 44% fall somewhere in the middle. Very digitals are more likely to share, at 40% very likely, while none of the not digitals said they were very likely to share.

THE PRIMARY MOTIVATION FOR SHARING CYBERSECURITY INFORMATION WITH EMPLOYEES AND THE PUBLIC IS TO BUILD AWARENESS SO THAT THEY WILL BE MORE LIKELY TO COMPLY WITH NECESSARY SECURITY MEASURES.

The primary motivation for sharing cybersecurity information with employees and the public is to build awareness so that they will be more likely to comply with necessary security measures, cited by 59%. That was followed by 22% saying their motivation is to build trust and enhance their reputation as a company that takes cybersecurity seriously.

The top three barriers to greater information sharing and collaboration for cybersecurity include the risk of defense measures becoming known to potential attackers, cited by 41%; a potential negative impact on the company's reputation, 40%; and the belief that cybersecurity is only as strong as the weakest member in the chain, 39%. This is one reason many companies would like to see stronger government regulation.

Conclusion

The potential benefits of digitalizing industrial operations are too compelling to ignore. But the risks of exposing industrial systems to the internet are serious. CEOs who want to seize new opportunities are educating themselves and their boards about new technologies like AI-powered automation and the internet of things, what these make possible, and how to protect their operations in this new environment. They are hiring security executives with deep expertise to lead these efforts and advise them. They are investing in cybersecurity not as an afterthought but as part of their digitalization efforts. And they are engaging with their industry peers, associations, and government entities to ensure the security of the entire business ecosystem. This is a radically different world. Companies that figure out how to capitalize on it in the context of a trustworthy environment will come out on top.

METHODOLOGY AND PARTICIPANT PROFILE

A total of 281 respondents drawn from the HBR audience of readers (magazine/ enewsletter readers, customers, HBR.org users) completed the survey.

SIZE OF ORGANIZATION

34% 10,000 OR MORE EMPLOYEES

29% 1,000- 9,999 E MPLOYEES

12% 500-999 EMPLOYEES

24% 499 AND FEWER EMPLOYEES

SENIORITY

22% EXECUTIVE MANAGEMENT/BOARD MEMBERS

31% SENIOR MANAGEMENT

28% MIDDLE MANAGERS

18% OTHER GRADES

KEY INDUSTRY SECTORS

14% MANUFACTURING

13% TECHNOLOGY

10% EDUCATION

10% FINANCIAL SERVICES

8% OR LESS OTHER SECTORS

JOB FUNCTION

17% GENERAL/EXECUTIVE MANAGEMENT

14% IT

8% OR LESS OTHER FUNCTIONS

REGIONS

44% NORTH AMERICA

25% EUROPE

16% ASIA/PACIFIC

8% MIDDLE EAST/ AFRICA

7% LATIN AMERICA

Figures may not add up to 100% due to rounding.

Harvard Business Review
ANALYTIC SERVICES

hbr.org/hbr-analytic-services

CONTACT US

hbranalyticservices@hbr.org