bcg.perspectives
by THE BOSTON CONSULTING GROUP

PLATINION
A COMPANY OF
THE BOSTON CONSULTING GROUP

OUR CRITICAL INFRASTRUCTURE IS MORE VULNERABLE THAN EVER

IT DOESN'T HAVE TO BE THAT WAY

By Nadya Bartol and Michael Coden

Subway cars stuck in a tunnel. Electricity blackouts. A breached dam. Jammed telecommunications. These and other potential consequences of critical infrastructure security breaches can at best cause inconvenience; at worst, they can lead to death or destruction on a shocking scale. Power outages in the Ukraine in 2015 and 2016 represent two such cases in point.

In today's hyperconnected world, such infrastructure is more vulnerable than ever to cybersecurity threats, whether from nation states with bad intentions, criminal organizations, or individuals. This new vulnerability stems from fundamental changes in the critical infrastructure of organizations' technology systems. Such organizations—health care providers, utilities, chemical producers, manufacturers, defense agencies, first responders, banks, transportation systems—have long owned and operated two types of technology systems. Their IT systems run basic office functions, such as e-mail, payroll, and human resources systems; while their operational technology (OT) systems control physical equipment and personnel essential for carrying out their mission, such as generating and transmitting power.

In the past, OT consisted of standalone systems that used little-known proprietary protocols—their very obscurity made them secure. But now, OT systems run on the same commonly known software and hardware platforms as IT systems. These systems are well understood by hackers and are therefore significantly less secure.

Unprecedented Exposure

What has led to this convergence of OT and IT? It's the growing demand for seamless access to information—access that hinges on the use of "smart" digital technologies, including sensors, cameras, and wearables. For instance, a utility gathers online data on power outages from smart meters so it can swiftly identify problem locations and restore power to customers. A homeowner remotely adjusts the thermostat at her residence to lower the tem-

perature while she's on vacation. A doctor views patients' insulin use on an office computer. Companies remotely monitor the status and location of trains, buses, and trucks; the flow of oil and gas through pipelines; or water or electricity consumption to manage these services effectively and efficiently.

While the technologies in these examples improve our lives and infuse efficiencies into our economy, they can also make us more vulnerable. When customers of three Ukrainian power utilities lost power because of a cyber incident, those utilities were able to fall back on manual operations to restore power. This would not be possible in a number of other countries, where manual operations no longer exist. When a hospital in Los Angeles experienced a ransomware attack, which locked up the hospital systems and made them unavailable, the hospital temporarily lost information about medications prescribed to patients. Fortunately, no one died from receiving the wrong medication or not receiving the right medication.

As the number of interconnected devices continues to increase, the number of potential access points for hackers to disrupt critical infrastructure grows as well. All of these devices need to be designed, implemented, and deployed in ways that make them less vulnerable to attacks.

In short, our dependence on technology is now critical and increasing exponentially. When attackers strike the systems that use those technologies, being inconvenienced or annoyed may constitute the very least of our worries.

Understanding the Challenges

Today's high levels of interconnectivity and exposure have also spawned serious challenges for critical infrastructure organizations, as we recently explained to the US presidential Commission on Enhancing National Cybersecurity in a report submitted to the National Institute of Standards and Technology (NIST). Let's take a closer look.

The Need to Secure Future Digital Infrastructure While It's Still Evolving

Smart cities, technology-enabled medicine, and driverless cars carry a wonderful promise of better, safer, and more productive lives for us all. But to build the digital infrastructure required to fulfill this promise, critical infrastructure organizations must anticipate future needs.

Some of the technologies that the infrastructure will have to support have not yet been invented. It's akin to building an airplane without knowing how far it will have to fly and how many people it will carry. To make matters even more difficult, critical infrastructure organizations' OT systems consist of older technologies that were designed and implemented before cybersecurity was on anyone's radar. Because these systems are critical, they frequently cannot be taken offline for redesign and repair. What's more, replacing that installed base is costly and time consuming. Can you imagine shutting down the electricity to your neighborhood for six months to do an upgrade?

Cybersecurity Talent Deficit

Ensuring that smart devices are designed, implemented, and maintained with security in mind is not easy. Furthermore, it requires specialized expertise that is in short supply globally. The global deficit of cybersecurity expertise is well documented. Finding those who know how to secure both IT and OT systems required by critical infrastructure is even more difficult.

Although the technology underlying the two types of systems is now the same, securing both types entails different priorities and different approaches. The difference in priorities is pronounced: OT systems must first and foremost be safe and available, while IT systems must first and foremost protect the confidentiality of the data that they process and store. People who spend their careers in IT or OT environments are driven by these very different priorities, usually have different educational backgrounds, and, as a result, have very different mindsets. Finding people who can

practice both OT and IT cybersecurity is no small feat, while cross-training is difficult, costly, and not always successful.

Resource Disparity Between Large and Small Organizations

Cybersecurity is a complex discipline comprising multiple knowledge areas. Doing it right requires a variety of specialized expertise that smaller organizations cannot afford. Large critical infrastructure organizations with hefty resources can hire their own experts and set up sophisticated cybersecurity programs. Smaller ones (like emergency response agencies and water utilities) have to manage the same risks with significantly fewer resources.

Reliance on Third Parties to Deliver Critical Capabilities Securely

The laws of economics drive businesses to focus on core competencies and outsource the rest. So it's not surprising that transportation companies, utilities, health care providers, financial services providers, and countless other industries rely on numerous partners to deliver anything from software and hardware to legal or consulting services. That includes the hardware and software components of critical infrastructure and the multitude of smart devices. Companies that merge are integrated much more tightly than in the past, including interconnecting each other's systems and exchanging highly sensitive information. To make matters more complicated, suppliers have their own suppliers, subsuppliers, and so forth.

The supply chain has thus become a supply network—long, extended, complex, multidimensional, and multinational. This provides an almost infinite number of additional points that can be compromised. While traditional IT manufacturers have been dealing with cyberthreats for 20 to 30 years, smart device and critical infrastructure systems manufacturers have only recently been introduced to the problem. The cybersecurity workforce shortage discussed earlier has a significant impact on suppliers' ability to secure their devices, including securing their own supply chains. Suppliers that used to make manually operated hardware devices and that now make software-driven smart devices have to learn about cybersecurity quickly.

Taking Action: Our Recommendations to the Presidential Commission

Internet time advances much more swiftly than people time. That is, threat actors move in internet time, while people think, analyze, and agonize over decisions. Organizations must act now to mitigate the cybersecurity challenges facing them today. We've developed several recommendations for contributing to effective, collective action.

IT/OT cybersecurity-practitioner development is a case in point. While federally funded cybersecurity workforce development programs are a step in the right direction, they focus on general cybersecurity training, not IT/OT environments. They therefore don't fully address the needs of critical infrastructure organizations in industries like manufacturing, transportation, and utilities—or their supplier ecosystems. To help close the gap, organizations can support the creation of a broader range of educational approaches, including college degrees, apprenticeship programs, and IT/OT security training for existing employees.

Cross-organizational mentoring and knowledge transfer is another recommendation. Organizations with less cybersecurity experience or smaller cybersecurity teams can learn from the experiences of their more seasoned peers. Larger organizations should also encourage their experts to participate in industry associations, public-private partnerships, and regional organizations, which all provide opportunities for formalizing cross-organizational mentoring and knowledge transfer. Smaller organizations should encourage similar participation. In the short term, such working groups take time away from people's day jobs. But in today's interconnected world, organizations will benefit in the long run, because the knowledge transfer will improve the security of the infrastructure that connects them.

Embedding Cybersecurity into Organizational Culture and Strategy

In addition to the recommendations described above, critical infrastructure organizations must weave cybersecurity into their very culture and strategy planning. As with safety and quality programs, these efforts will call for large-scale, transformative change. Organizations can't just rely on adopting cybersecurity technology solutions. Instead, they must set up the right incentives, performance management, training, processes, procedures, and other systems, to ingrain the mindset, behavior, and practices that cybersecurity requires. This includes using existing technologies effectively and enforcing new policies. On a more detailed, day-to-day level, executives need to lead by example, demonstrating the thinking, actions, and values that they want others throughout their organization to emulate.

In short, the most effective way to increase cybersecurity resilience is by changing the way people use technology—not by adding technology to compensate for technologies that are not being properly used. Most of the categories in NIST's Cybersecurity Framework are nontechnical, supporting this fact. Indeed, we recommend the following practices, inspired by our work with MIT, the World Economic Forum, and companies around the world, as crucial for weaving cybersecurity into an organization's culture and strategic planning:

- Empower your top cybersecurity leaders by giving them authority, budget, and regular access to your organization's board of directors.
- Acquire appropriate expert support—internally and externally.
- Define your cyber-risk tolerance consistently with your business strategy and risk appetite.
- Support cybersecurity investments that maximize business impact.
- Require reports containing achievable information that supports effective, prioritized decision making.
- Establish clear communications and accountability to encourage collaboration across the enterprise.
- Support cybersecurity collaboration and information sharing with third parties, including customers, suppliers, business partners, and competitors.

In the end, organizations that integrate cybersecurity into their culture and strategic planning will be the most resilient. Everyone in the organization will understand what cybersecurity means; why it matters to their organization, society at large, their jobs, and their families; and how they, in their everyday work and interactions, can make a difference in securing the entire nation's critical infrastructure. Hard work? Most certainly. But no critical infrastructure organization can afford to shy away from it.

About the Authors

Nadya Bartol is the associate head of the Cybersecurity practice at BCG Platinion. You may contact her by e-mail at bartol.nadya@bcgplatinion.com.

Michael Coden is the head of the Cybersecurity practice at BCG Platinion. You may contact him by e-mail at coden.michael@bcg.com.

This article was originally published by the World Economic Forum.

The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all

regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with 85 offices in 48 countries. For more information, please visit bcg.com.

3/17