Critical resilience: Adapting infrastructure to repel cyber threats

As the digital world becomes increasingly connected, it is no longer possible for infrastructure owners and operators to remain agnostic in the face of evolving cyber threats. Here's what they can do to build an integrated cyber defense.

James Kaplan

Partner, New York
McKinsey & Company

Christopher Toomey

Vice president, Boston
CP&I Major Projects
McKinsey & Company

Adam Tyra

Expert, Dallas
McKinsey & Company

The BBC recently reported that researchers have discovered major security flaws—which affect flood defenses, radiation detection, and traffic monitoring—in the infrastructure for major cities in the United States and Europe.[1] Of those flaws, nearly ten are deemed "critical," meaning that a cyberattack on these systems would have a debilitating impact on essential infrastructure, including power grids, water treatment facilities, and other large-scale systems. It seems like the stuff of disaster films: A major city loses power. Huge amounts of the population panic. The roads clog. Planes are grounded. Coordinating a rescue effort—even communicating with the public—would be a colossal task.

While such scenarios may seem far-fetched, they are indeed reality. In 2015, Ukraine's power grid was the target of such an attack—in the hours that followed, nearly a quarter-million people were left without electricity—yet this and similar stories rarely reach the public consciousness.[2] As a result, there is little pressure from constituents and cyber threat operators are not top of mind.

The number and severity of cyber threats continue to grow exponentially as the world becomes increasingly connected. According to recent estimates from the research firm Gartner, by 2020 there will be 20.4 billion internet-connected devices, and approximately 37 percent of these will be used outside consumer settings—including large numbers dedicated to infrastructure monitoring and control.[3] While the proliferation of connected devices has created unprecedented productivity and efficiency gains, it has also exposed previously unreachable infrastructure systems to attack from a range of malicious groups with varying motivations.

Owners, planners, builders, and financiers routinely channel ample resources into mitigating any number of risks to an infrastructure asset. Yet they rarely if ever place as much care into anticipating potential cybersecurity incidents. There are many reasons for the lack of attention to cybersecurity. One is a common consensus in the industry that the technology governing physical infrastructure is fundamentally different from the technology used in other industries. In reality, it is not. While new technology solutions are emerging to deliver and operate infrastructure, these solutions still rely on the operating systems common to nearly all sectors.

Similarly, infrastructure leaders tend to think that they need industry-specific expertise when it comes to hiring cybersecurity specialists. But while having industry-specific expertise is helpful, it should not be viewed as essential; the tool kits across industries are largely the same. Owners and operators might not have the resources they need to make significant strides in their cybersecurity programs if they focus only on recruiting highly specialized talent, especially as it relates to people who can design and execute responses to cyber threats.

As it stands, infrastructure has a long way to go to catch up to other industries in terms of future-proofing for a cyber threat. To accomplish this, cities and organizations will need to integrate their defenses. They will need to recruit and retain new talent and develop a cybersecurity program. Furthermore, ensuring that infrastructure achieves and sustains resilience to cyberattacks in the midst of rapid digitization requires that designers and operators make a proactive mindset shift about cybersecurity—before hackers impose one.

Vulnerabilities do not expire or become obsolete

When considering digitized infrastructure, owners typically focus their energies on envisioning the improvements in efficiency and customer experience that can be realized by new technologies. Cyber

attackers, on the other hand, focus on uncovering the ways that new technology use cases rehash the same weaknesses and vulnerabilities of the old. Indeed, the problems faced by cybersecurity professionals—for example, authenticating users or protecting sensitive data from unauthorized access—largely stay the same over time, regardless of the technology in question. In a 2018 report, vulnerability scanning firm EdgeScan noted that approximately 54 percent of the vulnerabilities that it identified in customer networks that year originally became publicly known in the past ten or more years.[4] This is the cybersecurity equivalent of allowing yourself to remain susceptible to an infectious illness a decade after a vaccine becomes available. As a result, attack patterns that worked during the previous year will likely still work (in a modified form) against newly digitized infrastructure connecting to the internet today.

The takeaway is that infrastructure owners, engineers, and operators, many of whom are acutely aware of cybersecurity vulnerabilities in their information technology environments, must consider the operational technology that powers their digitized infrastructure to be vulnerable to the same issues.

Hackers have long exploited this insight. In February 2017, a cybersecurity researcher developed a ransomware variant that could successfully target and manipulate the control systems of a water treatment plant.[5] In theory, his malware could be used by an attacker threatening to poison a municipal water supply unless the ransom was paid. This may sound like a familiar scenario, because ransomware has been an increasingly common and disruptive cyber threat faced by business for the past three years. Even so, it is not possible for leaders to test for every possible risk or outcome. They will need to limit their attention to the most pressing threats. And the best way to determine those threats is to look at the issues affecting other, similar deployments of technology. By identifying similarities between new and old use cases for technology, infrastructure designers can ensure that cyber risks that were resolved in previous years don't recur in the infrastructure space.

Building cyber defenses for infrastructure

To build adequate defenses, infrastructure owners and operators should start by assuming that a cyber attack is imminent. Then they must build a unified, integrated cyber defense that best protects all relevant infrastructure assets. Going through the process of identifying what is relevant will often require the asset owner to understand what supporting infrastructure is also vulnerable—critical utilities, for instance—and ensure that it is reasonably protected as well. For example, a hotel that relies entirely on a local utility for its power supply may decide that it makes sense to find a redundant power source. In turn, the asset owner will be able to look beyond what would strictly be considered their responsibility, and consider the broader network in which they are included. By going beyond their "battery limit," so to speak, the hotel can gather more information about relevant vulnerabilities and threats.

Moreover, both utility owners and governments can work together in this area to create more—and more widely distributed—utility networks. If they can better isolate network vulnerabilities, they can help ensure service to any undamaged portions.

Start with the assumption that a cyber incident will occur

Since the March 2011 earthquake and tsunami that caused widespread damage to the northeast coast of Japan, including the Fukushima Daiichi nuclear plant, the country has constructed an estimated 245 miles of sea walls at a cost of approximately

$12.7 billion.[6] The same prudence is needed to protect infrastructure from cyber attacks. As a point of comparison, one cybersecurity research organization estimates that the cost of ransomware damages alone in 2019 could exceed $11 billion.[7] But in spite of an increasing torrent of cyber attacks afflicting internet-connected businesses and individuals globally, infrastructure owners largely continue to think of a cyber-attack as a mere possibility rather than a certainty.

By starting with an assumption that a future cyber attack *will* degrade, disable, or destroy key infrastructure functionality, owners and contractors can take action early to build resilience into their systems. For example, backups can be implemented for critical connected components, computers can be designed to fail safely and securely when compromised, and preparedness exercises can train operators to act decisively to ensure that cyber attacks aren't able to compromise connected infrastructure to threaten lives or property.

When planning incident response, leaders should look beyond the infrastructure sector for lessons learned from cyber incidents that caused outages in other sectors of the economy. The steps required for shipping firm Maersk to respond to a June 2017 ransomware outbreak are particularly informative. In order to purge itself of malware, the company executed a ten-day effort to overhaul its entire information technology (IT) infrastructure—a software reinstallation "blitz" that should have taken approximately six months under normal conditions.[8] While infrastructure owners are unlikely to have the same technology footprint as a global shipping company, understanding the steps required to respond to a major cyber incident can provide perspective on the level of effort and courses of action that may be required to respond to an attack in the infrastructure space.

An integrated defense is the only defense

Every infrastructure network has an associated IT network within which its owners and operators conduct their day-to-day business, such as sending and receiving emails and writing reports. Likewise, most organizations operating an IT environment—and some organizations operating a connected infrastructure environment—have cybersecurity programs in place to protect their data and technology assets. However, two discrete cybersecurity programs can't match the effectiveness of one unified program to protect both environments.

While the technology components deployed in the IT and infrastructure environments may differ significantly in their purpose and complexity, they're vulnerable to the same risks when connected to the internet. In the best known instance of this from recent years, hackers that breached the network of retailer Target Stores in 2013 made their initial entry through an internet-connected control system for the stores' air conditioning systems.[9] By connecting the infrastructure management network to the network through which Target executed its corporate functions and processed credit card payments, IT staff unwittingly elevated a minor risk into one with the potential to create catastrophic losses. While the Target breach was a case of attackers traversing an infrastructure environment to target the IT environment, attackers could just as feasibly have made the opposite leap, compromising an office network before leveraging connections to attack infrastructure.

Why wasn't Target's HVAC system cordoned off from its payment system network? The efficiencies gained from connecting networks are clear and undeniable, so preventing these types of technology interactions isn't a practical option. Instead, infrastructure owners must craft a cybersecurity program that takes a comprehensive view of all technologies in

the environment by working to understand how they're connected to each other and to the outside world. Then they must deploy security controls and defensive countermeasures to mitigate risks attributable to IT and connected infrastructure in a prioritized fashion.

Just as designers must take into account the physical resilience of infrastructure assets, owners should integrate cyber resilience. One way of ensuring this happens is to make cyber resilience an integral part of the design process. In addition to better incorporating protections, the Internet of Things has created a digital, keyboard-based operating culture that is often devoid of manual alternatives. Asset owners, notably those responsible for critical infrastructure, such as power plants and hospitals, should consider establishing core functionality that is either resistant to cyber attacks or that allows for an asset to more readily withstand the impact of a cyber attack. Some hospitals in urban areas, for example, might have digitally controlled HVAC systems, including all vents and windows. Having windows that can be opened manually—with the option to override digital controls and use mechanical switches or toggles to open them—could help create ventilation and allow operations to continue in the event of a cyber attack.

How to get started

We've identified three key steps for infrastructure owners starting the process of building their integrated cyber defense.

Recruit new talent. The cybersecurity industry is already severely constrained for talent, and infrastructure owners and operators often compete against other industries that offer higher-paying positions. Therefore, infrastructure groups need to get creative with where they look for cybersecurity talent. Infrastructure players might look to "cyber utilities," for instance, which are industry-aligned working groups that pool information and resources to improve cybersecurity effectiveness for their membership. These member-driven organizations—such as the Intelligence Sharing and Analysis Centers (ISAC) sponsored by the US Department of Homeland Security—were originally intended to serve as industry-sector-aligned cyber threat intelligence fusion centers for member companies. So, for instance, banks could join the financial services ISAC. However, the concept could be employed on a smaller scale to allow infrastructure owners in a particular region to share cybersecurity talent and resources for cybersecurity functions besides intelligence. For example, a cyber utility consortium in any given metropolitan area—hypothetically comprising a city government, a municipal utility district, and a publicly traded electricity company—could share a single cybersecurity team, rather than each entity competing to recruit their own.

Form a cyber response team. The first hours after the discovery of a cyber attack are the most critical in effectively mitigating losses, and their importance is magnified in the case of attacks against infrastructure where loss of life may be a possible second- or third-order effect. For this reason, selection and training of an incident response team *before* an incident occurs is key. Teams should include cybersecurity professionals skilled in cyber investigation and analysis, but they must also include experts familiar with the broader functioning of the infrastructure asset itself along with leaders who can make timely decisions about issues such as whether to shut down infrastructure or notify the public about an incident.

Cyber response teams should be subjected to regular incident exercises to build the muscle memory necessary to respond effectively and to uncover

potential weaknesses in response processes. The cyber utility concept described above might be specifically helpful in forming a response team, since skill sets such as cyber forensics are in particularly short supply.

Cultivate a mindset shift across the organization. Cybersecurity for infrastructure is often seen as a trendy topic—every other year something happens that makes headlines and then, weeks later, the industry has returned to the status quo. Owners and operators take a hard look at the situation and then lose interest when no clear path forward presents itself. This needs to change.

Two specific actions are key in beginning and subsequently sustaining the mindset shift required. To begin the mindset shift, organizations need to develop a perspective on what a cyber attack would actually look like *for them*. Cyber war gaming and table top exercises have long been a staple for developing this perspective in corporate environments, and they can be similarly effective for infrastructure. Effective exercise scenarios emulate the actions of timely real-world attackers to impose a series of difficult decisions on the team, creating numerous (and sometimes painful) learning opportunities. Through cyber war gaming, participants often learn that their organization lacks key response elements such as clear delineation of responsibilities in crisis situations, plans for how and when they should communicate with stakeholders or the public, and even procedures for shutting down compromised systems. The best programs deepen learning by establishing a regular cadence of exercises (e.g. quarterly or semi-annually) to accustom participants to the stress and confusion of a crisis situation and to continuously identify opportunities for improvement.

Once organizations begin to understand how bad an attack could be for them, they must remain focused on steady improvement. To sustain the mindset shift begun with cyber war games, infrastructure owners must integrate cyber resilience metrics into their regular performance measurement programs. As the cliché goes, "What gets measured gets done." By requiring their teams to continuously evaluate the organization's cyber resilience, leaders can ensure that the topic remains front of mind. Leading organizations take this a step further by integrating cyber metrics into the performance metrics for *specific individuals*, creating a culture of personal responsibility where bad cybersecurity can actually affect managers' compensation and prospects for promotion.

In a world steadily digitizing and becoming more interconnected, cyber attacks should be thought of as a certainty akin to the forces of nature. Just as engineers must consider the heaviest rains that a dam may need to contain in the next century or the most powerful earthquake that a skyscraper must endure, those digitizing infrastructure must plan for the worst in considering how an attacker might abuse or exploit systems that enable infrastructure monitoring and control. This shift in thinking will begin to lay the path to connected infrastructure that is resilient by design.

Cyber threats don't become obsolete or irrelevant in the same way that the technology underlying them does. So, in the context of cybersecurity, future-proofing infrastructure is primarily about ensuring that the steps taken to inject resilience into a system remain connected with the relevant threats of today and yesterday, rather than threats that may manifest tomorrow.

By starting with the assumption that not only will cyber attacks against infrastructure occur but also that they will likely be successful, infrastructure designers and operators can learn to trap many risks before they have the chance to develop into catastrophes. To do this, infrastructure owners and operators must first understand how old vulnerabilities will affect new technology and then develop integrated cybersecurity plans to apply the appropriate level of protection to their entire technology environment. The result will be safer and more resilient connected infrastructure delivering reliable services to customers for years to come.

---

[1] "Dave Lee, "Warning over 'panic' hacks on cities," BBC, August 9, 2018, bbc.com.

[2] "Ukraine power cut 'was cyber-attack'," BBC, January 11, 2017, bbc.com.

[3] *Gartner says 8.4 billion connected "things" will be use in 2017, up 31 percent from 2016*, Gartner, 2017.

[4] *2018 vulnerability statistics report*, edgescan, 2018.

[5] Michael Kan, "Researcher develops ransomware attack that targets water supply," CSO, February 14, 2017, csoonline.com.

[6] Megumi Lim, "Seven years after tsunami, Japanese live uneasily with seawalls," Reuters, March 8, 2018, reuters.com.

[7] Steven Morgan, "Global ransomware damage costs predicted to hit $11.5 billion by 2019," Cybersecurity Ventures, November 14, 2017, cybersecurityventures.com.

[8] Charlie Osborne, "NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs," ZDNet, January 26, 2018, zdnet.com.

[9] Brian Krebs, "Target hackers broke in via HVAC company," Krebs on Security, February 5, 2014, krebsonsecurity.com.