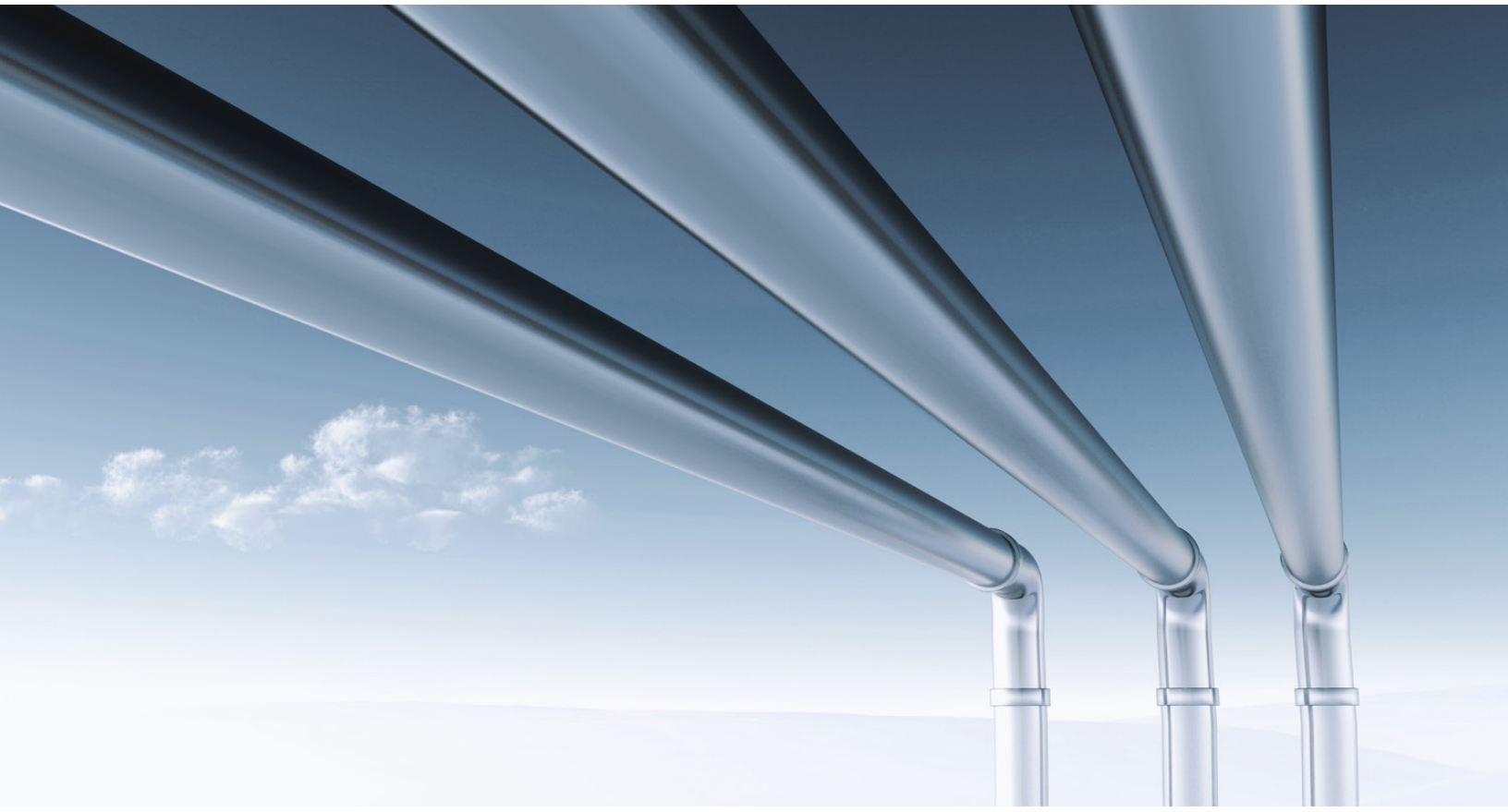
McKinsey & Company

Cyber Practice

Building cyber resilience in national critical infrastructure

Recent cyberattacks focus attention on the vulnerabilities of operations technology to web-based threats.

by Rich Isenberg, Ida Kristensen, Mihir Mysore, and David Weinstein



July 2021

The rising danger posed by cyberattacks on critical national infrastructure was evident again in May 2021, when a small group of hackers launched a ransomware attack on Colonial Pipeline, the United States' largest pipeline network for delivery of refined petroleum products. Colonial shut down its main lines for five days, disrupting nearly half the fuel supply for the eastern part of the country. Worried drivers drained supplies in gas stations in the Southeast, airlines rerouted flights to airports with available fuel, traders were rocked by unexpected price volatility, and logistics companies scrambled to locate new sources of fuel.[1]

The attackers seem to have initiated the havoc through "spear phishing"—the sending of emails apparently from familiar and trusted sources. Expected user response opened the way for the attackers to launch executable ransomware. This, in turn, enabled lateral movement deeper into the system and the compromising of credentials as the attack progressed. Colonial shut down affected systems, which protected them from broader damage. The company also paid a ransom to the attackers, to enable a reopening of operations.[2]

One unusual aspect of the attack is that the attackers attempted to apologize for it. On its site on the dark web, the group issued a statement that its sole motive was financial and it would choose its targets more carefully in the future. Future investigations may tell us more, but whatever the details, the attack is unsettling. A small group of hackers may have temporarily, and inadvertently, cut off energy flows to an important economic center, triggering real-world impact.

The Colonial Pipeline hack reveals that societies and economies are vulnerable to serious disruption, and physical harm, from *accidental overreach* by criminals. Ransomware exists to make money, usually through extortion from the private sector (or, sometimes, government agencies). When, as now, criminals launch unusually ambitious attacks on targets whose managers do not know exactly how their own systems work, then things can go wrong in dangerous ways.

The threat to critical infrastructure posed by ransomware attacks has only lately risen to an existential level—past attacks of this type did not implicate the security of operations technology (OT). OT security rather developed in response to threats by nation-state actors. The Colonial Pipeline attack, however, demonstrates that the picture has changed. Assurances about the separation of IT and OT systems are no longer tenable. If a relatively unsophisticated ransomware attack can take out infrastructure by disrupting the enterprise network, then more organized attackers will be emboldened.

The threats we face

Not long ago, cyberthreats on critical infrastructure were known only as acts carried out by nation-states. Specialists assumed that only states possessed the diverse skills and resources required to develop such threats. The targeted assets usually relied on analog operational technology and were relatively isolated from the internet. Gaining and maintaining access to such assets requires specialized tools, similar operational technology, reconnaissance capabilities, and even physical access to the site itself.

In recent years, however, business demands for remote visibility into industrial operations led to the convergence of IT and OT systems. The digital transformations that enabled sought-after business advantages, including remote access and predictive maintenance, created new vulnerabilities to cyberattacks. Now, less sophisticated attackers could prey on infrastructure assets.

In a recent attack on a water-treatment facility in Florida, for example, sodium hydroxide added to the water supply was raised to poisonous levels (an operator noticed the anomaly and took

[1] Niraj Chokshi, Clifford Krauss, and David E. Sanger, "Gas pipeline hack leads to panic buying in the Southeast," *New York Times*, May 11, 2021, nyt.com.

[2] Collin Eaton and Dustin Volz, "Colonial Pipeline CEO tells why he paid hackers a $4.4 million ransom," *Wall Street Journal*, May 19, 2021, wsj.com; Jason Fuller, Mary Louise Kelly, and Justine Kenin, "The Colonial Pipeline CEO explains the decision to pay hackers a $4.4 million ransom," *All Things Considered*, NPR, June 3, 2021, npr.org.

countervailing action in time). The attacker exploited a dormant, password-controlled remote-access software platform, compromising user credentials, gaining entry into the internet-facing system, and then moving laterally across the operational network. While the source of this attack has not been discovered, experts agree that the level of sophistication needed to carry it out is not particularly high.[3]

The attack on Colonial Pipeline was narrowly aimed to interrupt operations until the ransom was paid. For the target company, however, the attack led to uncertainty about the security of its OT systems, given the absence of proper network segmentation and security controls. In process-control environments, this kind of collateral damage disrupts availability but can also compromise the safety of personnel and citizens.

Web-based tactics, techniques, and procedures used against IT systems now put OT systems at risk. Barriers to entry are being breached with increasing frequency, making crystal clear that a new organization-wide approach to cyber resilience is needed—one that integrates IT and OT security.

How should organizations prepare?

Recent high-profile attacks and breaches have elevated awareness levels, and companies in the United States and in many other countries can expect regulations on resilience and cybersecurity to tighten over time. In particular, the Colonial Pipeline attack has moved ransomware from being the focus of experts into a mainstream concern. In the United States, pressure is mounting against a response in which ransom is quietly paid. In a direct response to the Colonial attack, for example, the Transportation Security Administration, which oversees the cybersecurity of pipelines, made it a requirement that companies report cyberattacks to the federal government within 12 hours of becoming aware of them.[4]

Companies will have to improve their knowledge of their own systems. Knowledge of operations, vulnerabilities, and remedies will be the starting point for building resilience. It will also enable companies to communicate effectively—to governments, regulators, customers, and the media—to build trust in the event of an incident.

The new threat to critical infrastructure is now out in the open, and it shows that a *step change* in both cyber defenses and our capabilities to absorb and navigate operational attacks is urgently needed. The following principles can guide critical-infrastructure companies in their operational and technical actions to build organization-wide cyber resilience.

Visibility, zero-trust architecture, resilience

Organizations need to establish visibility into their business-technology assets and their OT systems. Here the watchword might be, "You can't protect what you can't see"—words that are highly relevant to critical-infrastructure networks ranging from manufacturing plants to natural-gas pipelines.

The journey begins with gaining and maintaining real-time visibility into the assets on these industrial networks—but that isn't where it ends. Effective visibility demands that organizations take a posture that affords them greater detail. Owners and operators of these critical systems can establish high-fidelity baselines for the devices on the network and be able to detect subtle anomalies in behavior. Such slight changes can indicate threats and lead to unsafe conditions.

The recent ransomware attack against Colonial Pipeline was likely not targeted against the pipeline itself. Rather, the company's IT systems were attacked. The lack of visibility into the interconnection between the IT and OT systems contributed to the decision to stop operations. The operator could not be confident that the malware had been isolated. The necessity of such a decision might have been confirmed or disproved had operations visibility been established.

Second, owners and operators must move to a zero-trust mindset and architecture. Most of the OT

[3] Andy Greenberg, "A hacker tried to poison a Florida city's water supply, officials say," *Wired*, February 8, 2021, wired.com.
[4] Brian Naylor, "In wake of Colonial attack, pipelines now must report cybersecurity breaches," NPR, May 27, 2021, npr.org.

systems controlling America's critical infrastructure were designed at a time when industrial networks were far less connected than they are today. In the digital age, however, IT and OT systems are converging at a rapid pace. To address the changing picture, organizations can move from a "trust but verify" mindset to a "verify first" approach. Sophisticated actors are increasingly capable of exploiting trust-based approaches. They manipulate the native functionality of control systems while maintaining the appearance of a normal state. Proactive threat hunting and defense-in-depth controls can help ensure not only swift detection of threats but also containment to prevent lateral movement and therefore mitigate the impact of a compromising attack.

Finally, the Colonial Pipeline attack can be viewed as a case study in the importance of building resilience. Events like this one are extremely difficult, if not impossible, to predict, but a lot can be done to prepare for them. Organizations need to improve their systems' ability to respond, establish control, and spring back quickly. Scenario planning and threat mapping can help organizations define primary and second-order effects. These capabilities can identify in advance the actions to take in response to a large disruptive event. Thinking in advance about targeted ways to build in redundancy at critical points or capabilities to expand capacity at critical moments can make all the difference. Time is of the essence in a crisis. Organizations have to know what to do, develop the capabilities to do it, and then rehearse their crisis-response actions—all in advance of the incident.

Actions for critical-infrastructure organizations

To best prepare for ransomware and similar disruptive cyberattacks, critical-infrastructure companies can take preemptive action, by developing a comprehensive plan with steps to be taken within one, three, and 30 days. In its response to the attack on Colonial Pipeline and a subsequent high-profile cyberattack on JBS, the world's largest meat-processing company, the US government took specific note of the shift in ransomware targeting: from data theft to the disruption of operations. In no uncertain terms, the government told companies that they must ensure the separation of business functions and production operations so that attacks on corporate activities do not disrupt production and supply.

These preparations require advanced levels of cybersecurity capabilities. Depending on the status of their security environment, organizations will have to accelerate their journeys from maturity-based cybersecurity to an advanced, proactive cybersecurity posture. Foundational capabilities are only the starting point. The journey then moves to a risk-based approach, focusing on the risks that matter to reduce enterprise risk, and then to holistic resilience, embedding security by design into next-generation processes, services, and technologies, and incorporating customers, partners, third parties, and regulators into enterprise resilience management.

Preemptive activities include the following:

— *Mapping IT–OT interdependencies.* Organizations need to obtain a true understanding of the interdependencies of the network environment, including core systems and applications, and to discover the intentional and unintentional connections and overlap of the IT and OT environments. This mapping will enable organizations to grasp quickly the full resulting implications of a ransomware attack against any one part of the organization.

— *Conducting simulations.* Organizations can continue to rehearse and improve cyber crisis-response scenarios, including for ransomware attacks. Simulations are usually most effective when they include third parties such as law enforcement, public-sector industry groups, and critical customers and suppliers. The simulations should include further core decisions, especially when to isolate or shut down parts of the network and whether to engage with the attackers.

— *Making the changes needed to achieve cyber resilience.* The mapping and simulations can help organizations improve their operating model and governance structure. Both activities will aid in identifying and implementing the

necessary refinements to attain cyber maturity across the integrated IT and OT architecture. In addition to cyber maturity, the organization can gain greater clarity on the roles, responsibilities, and decision making that will form the core of its response in the event of an actual ransomware event or other cyberattack.

Evidence suggests that the ransomware attack on Colonial Pipeline was not a particularly sophisticated cyberattack—and yet it managed to paralyze a significant part of the fuel supply of the world's largest economy. Good could come of this disturbing event if it acts as a call to action for nations and organizations. Critical infrastructure is vital to a nation's economy and security. The investments needed to truly protect it can no longer be delayed.

Rich Isenberg is a partner in McKinsey's Atlanta office, **Ida Kristensen** is a senior partner in the New York office, **Mihir Mysore** is a partner in the Houston office, and **David Weinstein** is an associate partner in the New Jersey–Summit office.

The authors wish to thank Venky Anant, Tucker Bailey, Dumitru Dediu, Aman Dhingra, Ciaran Martin, and Daniel Wallance.

Designed by McKinsey Global Publishing