On the evening of July 13, a large swath of Midtown Manhattan and the West Side of New York City went dark. Subways shut down, the lights went out on Broadway shows, traffic lights stopped working, and hundreds of people were trapped in elevators. The energy company Con Edison reported a “significant electrical transmission disturbance” that originated at its West 49th Street substation and sent hundreds of thousands of people into darkness for five hours.

Exactly 42 years prior to the outage on Saturday, a much larger blackout hit New York and left the city without power for 25 hours. While the speaker of the city council described the aftermath of the more recent blackout as a “textbook response where things went well,” the 1977 blackout led to chaos in the streets – looting and vandalism caused millions of dollars in damage and there were almost 4,000 arrests. The 2019 blackout wasn’t as severe, but it was a stark reminder that many of the infrastructure systems we take for granted are far from invulnerable.

After the blackout in July, New York City Mayor Bill de Blasio pointed out that “This was not a cyber attack and this was not an act of physical terrorism.” If Abraham Beame, the mayor of New York in the summer of 1977, had reassured his citizens that the blackout wasn’t the result of a cyber attack, they wouldn’t have had any idea what he was talking about. But as we approach the third decade of the 21st century, major cyber attacks on critical infrastructure in the United States are more likely than they have ever been.
In December 2015, the control systems of three Ukrainian energy companies were infiltrated by Russian hackers – a cyberattack that affected 30 substations and caused a power outage for more than 225,000 people. A year later, another cyberattack struck a control center in Kiev. According to a 2016 report by the Electricity Sharing and Analysis Center, the 2015 hack was the “first publicly acknowledged” cyberattack to result in a power outage, and it was immediately clear that something similar could happen in the United States.

A 2017 report published by researchers at the University of Washington noted that the attacks in Ukraine “represent a growing category of hacks intended to sabotage critical infrastructure.” Many cybersecurity professionals are increasingly worried about these hacks – a 2018 survey of “1,100 senior information technology practitioners” conducted by the Ponemon Institute found that 64 percent of these practitioners consider “breaches that damage critical infrastructure” to be the cyber threats that pose the greatest risk in the future. Infrastructure hacks were second only to “breaches involving high-value information,” an umbrella category that includes a huge range of cyberattacks across all categories.

According to a 2018 threat assessment by the U.S. intelligence community, “The risk is growing that some adversaries will conduct cyber attacks – such as data deletion or localized and temporary disruptions of critical infrastructure – against the United States in a crisis short of war.” One of the reasons for the surging risk of cyberattacks against critical infrastructure is the rapidly increasing interconnectivity of systems and devices. A recent report from Gartner found that there were 8.4 billion “connected things” in 2017, a number that’s “up 31 percent from 2016, and will reach 20.4 billion by 2020.” The world of networked things includes everything from digital doorbells and home assistants to hydroelectric dams and nuclear power plants.
While the ever-expanding Internet of Things (IoT) creates a target-rich environment for hackers who want to infiltrate critical infrastructure systems, the number of potential attackers is increasing (along with their capabilities). The U.S. intelligence community’s threat assessment points out that just 10 countries were capable of carrying out cyberattacks in 2011 – a number that increased to more than 30 by 2017. Meanwhile, the report explains that there will be convergence between state-sponsored attacks and transnational cybercrime: “We expect the line between criminal and nation-state activity to become increasingly blurred as states view cyber criminal tools as a relatively inexpensive and deniable means to enable their operations.”

Companies in the infrastructure sector should be particularly concerned about cybersecurity, as they’re tempting targets for hostile foreign powers and cybercriminals alike. This is why the President’s National Infrastructure Advisory Council emphasizes the fact that “Cyber is the sole arena where private companies are the front line of defense in a nation-state attack on U.S. infrastructure.” For example, while attacks like the ones that hit Ukraine in 2015 and 2016 had a specific geopolitical motive, other attacks could be carried out for purely mercenary reasons (such as the collection of a ransom).

All of these factors come together to create a cybersecurity environment that’s more threatening than ever for companies and government agencies responsible for protecting critical infrastructure in the United States.
CONSEQUENCES OF CYBERATTACKS ON INFRASTRUCTURE

In the summer of 2017, Russian hackers attacked again. But this time, the consequences would be far worse than a few blackouts in Ukraine – they would reach around the entire world, costing some of the largest global companies hundreds of millions of dollars.

The attack was carried out with a form of malware called NotPetya, which combines two powerful infiltration tools (Mimikatz and Eternal Blue, which was developed by the NSA and leaked in 2017) to break into computers and run malicious code. NotPetya was launched in Ukraine, but it spread around the world at a furious pace, locking down ports, striking hospitals, airports, and power plants, and even preventing the production of pharmaceuticals (Merck lost $870 million in the attack).

One of the biggest victims of NotPetya was the Danish shipping giant Maersk – a case study that demonstrates how destructive a cyberattack on infrastructure can be in a heavily interconnected global economy. As an August 2018 article in Wired explains: “An attack aimed at Ukraine strikes Maersk, and an attack on Maersk strikes everywhere at once.”

When Maersk’s systems went dark, the consequences were vast and immediate: Convoys of trucks couldn’t unload their freight at the company’s shipping terminals, the company couldn’t take new orders, and global supply chains were severed. As Andy Greenberg put it in his article for Wired: “For days to come, one of the world’s most complex and interconnected distributed machines, underpinning the circulatory system of the global economy itself, would remain broken.” Maersk, Greenberg notes, accounts for almost a fifth of the world’s shipping capacity.
As cyberattacks on critical infrastructure have become more likely, their potential effects have become more devastating. And this isn’t just because so many companies and public services would cease to function without reliable electricity, roads, Internet connections, etc. It’s because the infrastructure sector itself is so interconnected – as a report on the cybersecurity of the U.S. power grid by the Council on Foreign Relations explains: “All sixteen sectors of the U.S. economy deemed to make up the nation’s critical infrastructure rely on electricity.” A successful attack on the power grid could affect transportation, water, communications, healthcare, and manufacturing systems all at once.

The NotPetya hack demonstrates that secondary and tertiary targets of cyberattacks can suffer consequences every bit as serious as primary targets. It also demonstrates how far-reaching a hack’s effects can be, even to the point of causing unintended consequences – the Russian hackers who unleashed NotPetya probably weren’t expecting the infection to spread all the way to Rosneft, the Russian state oil company.

Global interconnectedness doesn’t just increase the amount of damage infrastructure hacks can cause – it also gives hackers more attack vectors to exploit. For example, global supply chains are vulnerable to infiltration and harder to defend than domestic production lines. As a 2018 report from the Congressional Research Service explains: “OT and IT systems rely on hardware devices and software systems, procured from a variety of manufacturers and vendors, often from international sources. The security of the design, manufacture, and patch management practices of these devices and systems is a potential vulnerability due to their global nature.”

The destructive capacity of cyberattacks on critical infrastructure has never been greater than it is right now. Recent incidents like the WannaCry malware attack launched by North Korea and the NotPetya attack have cost billions of dollars – according to the White House, NotPetya alone caused more than $10 billion in losses. The evidence that the infrastructure sector faces unprecedented cyberthreats is overwhelming. We have all the warnings we could ever need, so let’s take a look at what can be done to heed them.
DEVELOPING AN INTEGRATED DEFENSE AGAINST CYBERATTACKS ON CRITICAL INFRASTRUCTURE

You may have noticed a theme in this report – perhaps we should have called it “Infrastructure cybersecurity in the 21st century: The perils of interconnectivity.” While globalized supply chains, distribution networks, and communication channels have ushered in an unprecedented era of productivity, wealth creation, and international cooperation, they have also drastically increased the international economy’s susceptibility to cyberattacks. This susceptibility is particularly consequential in the infrastructure sector.

This is why infrastructure companies have to develop a comprehensive and integrated cybersecurity platform that covers as many attack vectors as possible and cultivates a security-oriented mindset among all their employees. With so many more methods of infiltration available to hackers – particularly in the infrastructure sector – it’s vital for employees across departments and teams to be equipped to identify, prevent, and if necessary, contain cyberattacks.

A 2018 Kaspersky Labs survey of infrastructure-focused cybersecurity professionals found that “employee errors/unintentional actions” were the third-most-cited causes of OT/ICS cybersecurity incidents in the previous year (“OT” stands for “operational technology” and “ICS” stands for “industrial control systems”). Meanwhile, almost half of the respondents said employee errors and unintentional actions were a “major concern.” More respondents cited “Hiring ICS cybersecurity employees with the right skills” than any other major challenge.
However, almost half of the companies surveyed didn’t have any OT/ICS cybersecurity awareness or compliance programs in place and almost two-thirds didn’t have a dedicated budget for OT/ICS security. While 82 percent of companies provide “security awareness training for staff, contractors and vendors with access to control systems and networks,” these programs need to be expanded to include all employees. If there’s one thing companies in the infrastructure sector should recognize by now, it’s the fact that hackers will exploit gaps in their security architecture at every level: from sophisticated hacks of control systems and networks to the theft or infiltration of a company laptop.

Speaking of company laptops: Greenberg explains that “a finance executive for Maersk’s Ukraine operation had asked IT administrators to install the accounting software M.E.Doc on a single computer. That gave NotPetya the only foothold it needed.” It would be difficult to come up with a clearer example of the importance of security awareness than the decision of a single employee that ended up costing a company hundreds of millions of dollars, breaking supply chains all around the world, and having a significant impact on the global economy.

Just as a single computer caused the breach at Maersk, a single computer brought the company’s systems back online. Employees couldn’t find a backup domain controller, which would have prevented the company from recovering massive amounts of data. Fortunately, a computer in an office in Ghana wasn’t connected to the rest of the network when the attack took place, and its hard drive contained the data the company needed. This suggests that one fail-safe tactic companies may want to consider is the storage of backup files on an unconnected device in a secure location.

While companies responsible for critical infrastructure are increasingly investing in cybersecurity, there are still fundamental changes that need to be made in the industry. For example, a recent McKinsey report points to the “common consensus in the industry that the technology governing physical infrastructure is fundamentally different from the technology used in other industries.” This attitude can lead to security lapses, such as failing to update out-of-date operating systems or checking for weak links in networks.

Security awareness training should also be provided to all employees in the infrastructure sector – not just personnel who have direct access to control systems and networks. As the number of attack vectors continues to increase and systems become more and more interconnected, a single mistake (such as using the wrong software on a single company computer) can lead to a massive breach.
Just as it’s vital to develop a company-wide cybersecurity strategy that includes all departments and employees, infrastructure companies need to work with external actors as well – from government agencies to other companies. Recall the security liabilities presented by global supply chains: The Congressional Research Service report points out that devices manufactured abroad could be tampered with given the “general lack of consistent oversight of standards and practices to prevent impaired or compromised functionality.” This is why companies should thoroughly vet their partners and maintain open lines of communication with them. They should also work with government agencies responsible for trade, cyberdefense, and other relevant fields. For example, McKinsey notes that “utility owners and governments can work together in this area to create more – and more widely distributed – utility networks.”

Integration is the key to an effective cybersecurity platform – especially for companies that maintain and protect the arteries of the global economy: from roads, bridges, and powerlines to cargo ships and lines of fiber optic cable. The culture of security at these companies has to include every department and employee, as employees are often the first and last line of defense. In many cases, cyber awareness plays the most critical role in ensuring that organizations aren’t hacked. As cyberattacks on critical infrastructure become more common and destructive, these companies have to use all the resources at their disposal to thwart them if possible and contain them if necessary.