MICROGRID KNOWLEDGE

Whether Facing a Cyberattack or a Pandemic, Preparation Is Critical

September 28, 2020
By Guest Post

S&C Electric's Stephanie Pine explains why cybersecurity and threat preparation is critical for the utility industry during uncertain times — a fact underscored by the pandemic.

The COVID-19 pandemic has provided the ultimate lesson in the value of preparation and crisis management. As we've collectively experienced this pandemic, it has helped us to more clearly imagine a non-biological virus, such as a successful cyberattack on electric utilities, similarly traversing the globe and leaving destruction in its path.

The power industry has more than a century of experience in preparing for threats to electrical systems. Utilities regularly invest in protective equipment to prevent unnecessary outages. Large campuses install backup generation to ensure continuity when the grid is down. Storm-prone areas harden their electrical gear to jump-start recovery measures. Storms and other commonly caused outages are known and accepted threats for the power industry, and the industry knows poor preparation for these inevitable circumstances can cause severe, cascading problems.

Challenges associated with the COVID-19 pandemic have brought to mind an unfortunate comparison to the varying levels of preparation (or lack thereof) for a cyberattack. Similar to the threat of a pandemic, a cyberattack is something expected to happen eventually, but it doesn't spark a sense of urgency before the threat is upon us. Preparations can be made to combat pandemics and

Stephanie Pine, Director—strategic accounts, S&C Electric Company

cyberattacks in advance, and in the long run thorough preparation is more cost-effective than only relying on reactive measures.

Having a basic response plan in place is critical because, regardless of the amount of preparation that goes into cyberattack and pandemic response plans, numerous unpredictable secondary and tertiary effects will occur.

For example, supply-chain disruption could degrade a utility's ability to have critical spare parts in stock during times of need. This potential shortcoming previously may not have been a concern. This is similar to what might be expected in a cyber intrusion with a novel entry point, such as an unprotected USB port. Once the entry point is identified, responders then can start adapting to this challenge. These less predictable "known unknowns" make base-level planning even more critical.

Cybersecurity in the utility industry

Cybersecurity isn't a *new* topic to the power industry, and many utilities and commercial and industrial (C&I) companies are taking proactive steps to start preparing for a cyberattack. But, few of these organizations are investing the proper focus and resources into being truly prepared for a full-blown cyber incident.

Some utilities are testing innovative approaches by making adjustments to their protective networks, or they are integrating microgrids throughout their grid to provide an additional level of energy security. These actions are steps in the right direction, but one-off preventive measures will not provide the comprehensive cybersecurity, or analysis capabilities, the electrical grid requires to successfully navigate and overcome a cyberattack. When an attack does occur, utilities and C&I organizations that don't have a plan in place will need to rely on reactive solutions, which will inevitably be more expensive, take longer to implement, and result in more severe systemic damage.

Utilities are responsible for providing cyber protection at the grid level, but C&I companies should be investing in cyber protection as well. One of the largest impacts of a cyberattack is economic losses. Cyberattacks lead to outages and system failures, which in turn lead to operations downtime and financial blows. A recent study found nearly 20% of C&I customers that experienced an outage in the last year incurred a cost of $100,000 or more.

continued on next page

Originally published on Microgrid Knowledge | www.microgridknowledge.com

The US pandemic response continues to highlight parallels with the need for cyber protection. In the midst of the pandemic, one of the major concerns has been the impact educational changes will have on children. If they fall behind now, it's expected it will take longer for them to catch up. The utility industry sees the same challenges with cyber protection. By not implementing comprehensive cyber monitoring and not investing in cyber strategies now, utilities can expect potential problems to accumulate. By failing to develop strong protection plans now, the industry is unintentionally creating more intrusion points for a cyberattack.

Following the lead of federal facilities

Utilities and C&I companies can look to the Department of Defense (DoD) for examples of strong cyber preparation. Federal cybersecurity is state of the art thanks to implementation of various guidelines and associated accreditation processes, such as the Risk Management Framework. These security measures focus on critical infrastructure facilities, where a successful attack could be catastrophic.

When finding parallels with the global pandemic, federal cyber protection for critical facilities is similar to hospitals having greater stockpiles of medical equipment such as gloves, hand sanitizer, and antibacterial cleaning supplies than department stores. The risk of not having these protective measures in place is clearly greater at some locations than others, and the DoD has taken many actions to limit risk, including the use of hardened, secure equipment, multi-level protection, and microgrid solutions.

Establishing cyber protection in resiliency solutions

It's unrealistic to believe a single solution can fix every problem associated with cyber concerns, but there are steps the industry can take to help mitigate the risks associated with an attack. Just as the world has turned to face coverings to help limit the spread of COVID-19, utilities can add resiliency elements to help limit the harm of a large-scale cyberattack. These protection strategies are often less costly and more effective than trying to repel a cyberattack after the fact.

One tactic utilities can explore is the use of non-wires alternatives, including microgrids. The ability to create electrical islands separated from the utility grid can help limit the reach of a cyberattack and keep the lights on for homes and businesses.

Nested microgrids can provide additional security layers. Future cyber-protection strategies and resiliency solutions will need to focus on distributed systems to protect the wide range of infrastructure a utility manages. Experts in both cybersecurity and electrical distribution can help utilities deploy these distributed systems.

Regardless of whether a utility is pursuing a microgrid, systems that include an intelligent control system are proven to be more cyber-secure. Microgrid controllers, with built in layers of cybersecurity, can aid utilities in crafting an intentional defense embedded in the system as opposed to conventional overlaid protection methods.

It's unrealistic to believe a single solution can fix every problem associated with cyber concerns, but there are steps the industry can take to help mitigate the risks associated with an attack (Photo By Gorodenkof/Shutterstock.com)

Nested microgrids and advanced, cyber-secure control systems at a few locations have proven to be effective countermeasures to the risk of cybersecurity, but for these strategies to work at utility scale, they must be adopted more broadly.

Just as the risk of a pandemic is known and generally rising, so too is the risk of a catastrophic electrical system cyberattack, and it is in the industry's best interest to have protection strategies in place now. Society has witnessed the deep global disruption and heroic efforts to keep the lights on during the pandemic, and the utility industry must translate some of the preparation and risk-management lessons learned to protect our country's electrical infrastructure from a devastating cyberattack.

Originally published on Microgrid Knowledge | www.microgridknowledge.com