KPMG

May 7, 2020

Plugged in: Maintaining cybersecurity vigilance during business continuity challenges

Actions to mitigate the spread of COVID-19 are forcing power and utility organizations to increase their reliance on remote access and fewer on-site operational staff, raising cybersecurity concerns. We talked to Jason Haward-Grau of KPMG Cybersecurity Services about how the sector is taking steps to bolster cyber defenses and expand their business continuity plans.

Question 1:

How are the cyber operations of U.S. power generation and transmission organizations impacted by COVID-19?

The number one priority of utilities, like every other organization right now, is maintaining a healthy and effective workforce. At the same time, chief information security officers (CISOs) must still ensure cybersecurity coverage for information and operational technology (IT and OT) as traditional competencies are eroded by the need to operate under business continuity plans (BCPs). It's much more difficult to patch devices, keep operations current, and protect the overall organization from cyber intrusion all while a substantial portion of the workforce is operating remotely.

Meanwhile, like other industries that require a significant number of on-site employees, utilities have been structuring teams, shifts, and workspaces to support social distancing and protect employees who must work on site. In the power and utility sector in particular, most operations are managed in a single control room where staying six feet apart is a logistical challenge. Many of the most knowledgeable and critical utility employees are older, and therefore in a category of people most at-risk for complications from the virus.

As the number of people testing positive grows, thereby increasing the need for more employees to quarantine, staffing levels are bound to be affected.

Question 2:

What are the specific cybersecurity concerns for utilities?

Increased remote infrastructure usage by employees means more "holes", more often, in the firewalls in both corporate and OT networks that require monitoring by the cybersecurity team, and an increased risk that malware—if successfully deployed in an environment—could impact safety, power generation, and operational integrity.

Social distancing measures also are forcing third-party suppliers, who are often highly specialized OT personnel, to work from home. These added "hops" through remote access to the plant open up even more vulnerabilities. Cybersecurity now must monitor dozens of key connections, instead of a handful, while they also work remotely. It also means that in the event of a security breach, there are fewer people on site to chase it down and prevent damage.

A lot of maintenance for older, non digital technologies also must be done on site. With the need to reduce the number of personnel on location at any one time, utilities have to determine which regular maintenance can be delayed to focus on essential work. At many utilities, turnarounds are largely on hold.

Utilities with renewable energy operations may be facing particular challenges. Distributed generation is even more reliant on integrated networks to share information. The control processes tend to consolidate in one control room, creating a single point of intrusion, and are often at a distance from the wind, hydro or solar farm. This can invite attacks across those distributed channels and result in a network outage or potential ransomware.

As bad actors seek to take advantage of the situation during this period of reduced operational strength, phishing attacks targeting utility employees are on the rise. The U.S. Federal Bureau of Investigation is warning of an increase in cyberattacks related to COVID-19, including fake CDC and phishing emails.[1] Cyber adversaries are already taking advantage of the situation, and phishing emails related to COVID-19 are surging along with their malware payloads.[2]

Utilities didn't design their BCPs to operate under these circumstances for what could be an extended period of time, so they have to stop and think about how to address these issues. This is especially important as utilities are critical infrastructure, responsible to the government and citizens. The country can't afford outages and downtime now.

[1] Source: Federal Bureau of Investigation. Alert Number I-032020-PSA: FBI sees rise in fraud schemes related to the Coronavirus (COVID-19) pandemic.

[2] Source: Dark Reading. "FBI Warns of Fake CDC Emails in COVID-19 Phishing Alert." March 23, 2020.

The good news is that—having been targeted by advanced persistent threats for 10 years or more—utilities have a lot of experience identifying and fighting off attacks, and they have been working for years to bolster their defenses.

Question 3:

What considerations should utilities keep top of mind as they protect their operations and ensure their BCP plans are as robust as possible?

The need for remote working has weakened the separation between IT and OT, and the staff on hand who can act to protect operations under attack has been, by necessity, reduced. However, utility organizations still have a number of steps they can take to help mitigate the increased risk.

— To counter the reliance on a single control room, especially as the need for remote work continues, several utilities we work with have created or are in the process of duplicating back-up control rooms. One company turned its training room into a second control room to run concurrently, shifting back and forth for a "deep cleaning" in between to enable continued operations.

— Most BCPs assume one disaster at a time and continuity challenges lasting from two to 12 weeks. COVID-19 has highlighted the need to update planning scenarios that include extended work under BCPs and the potential for concurrent issues, such as a pandemic and power outages from a hurricane or other natural disaster. And now that many utilities have been operating under BCPs for several weeks, it's time to look at what's working and what needs to be improved based on experiential data such as resources available to respond, the number and pattern of phishing attacks, and critical maintenance activities undertaken. BCPs can then be adjusted to work smarter, rather than harder, given staffing limitations.

— With some of their most experienced engineers stuck at home, utilities can take advantage of the required remote work as an opportunity to capture all the knowledge in their heads. These employees can document what they've learned over the decades, including details on OT configurations and processes that are often lacking in many utility BCPs.

— Utilities should plan and conduct remote penetration testing activities to check and secure facilities, especially plant-side VPNs. For distributed renewable operations, they need to validate that the plants would still continue to generate and supply power if the control room went offline.

— Security operations may need to be fortified so that they can handle both the IT and OT layers. Where possible, organizations should increase their capabilities to "look for bad" on the networks.

— Planned security reviews should be accelerated, including a review of remote access arrangements and procedures for the OT organizations, and any OT hardening that can be done tactically. The OT risks around delayed patch deployments and the potential vulnerabilities those delays will cause also require review to ensure that compensating controls are in place (e.g., ensuring the Safety Instrumented System (SIS) is still islanded from the rest of the network).

— Termination processes may need expansion to cover security procedures should organizations be in the unfortunate position of laying off or furloughing staff outside of the office. As several high-profile accounts have shown, one disgruntled former employee can wreak havoc through remote access, wiping out control systems equipment or destroying vital backups and configuration documentation.

— Utilities may need to focus more on documenting and testing their recovery procedures, particularly for OT which has traditionally relied on complexity and air gapping for greater security. A cyber breach can be diagnosed quickly, but deleted onsite backups and configurations for recovery can take weeks to rebuild, and longer with current restrictions.

— With the additional stresses and demands on the security team at this time, organizations need to rally the entire employee base to protect the company with a reemphasis on security awareness. As one CISO we talked to said, his organization doesn't have a few hundred employees working on security, it has thousands.

— Given that power generation in the United States is so fragmented, utility CISOs don't often have an opportunity to speak and share ideas. Now is a good time to start connecting. A lot of good cybersecurity work is being done at different organizations that would benefit others and the sector as a whole.

With all the hard work that power and utility organizations have done for years to improve their cybersecurity and protect the infrastructure, the sector is in a better position than many to rise to the challenges presented by COVID-19. By keeping these new considerations in mind, utilities can help protect their operations while developing a number of new, effective ways of working that can be used again in the future.

KPMG Global Energy Institute

The KPMG Global Energy Institute (GEI) is a worldwide knowledge-sharing platform on current and emerging industry issues. Launched in 2007, the GEI interacts with over 30,000 members though multiple media channels, including audio and video webcasts, publications and white papers, podcasts, events, and quarterly newsletters. Subscribe today to begin receiving valuable insights covering critical business topics and industry issues by visiting read.kpmg.us/gei

Contact us

Jason Haward-Garu
Managing Director
Cybersecurity Services
T: 713-319-2000
E: jhawardgrau@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.