Drilling down: Maintaining cyber security vigilance during business continuity challenges

Actions to mitigate the spread of COVID-19 are forcing oil and gas 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 Cyber Services about how the sector is looking to bolster cyber defenses despite the impact of depressed oil prices on capital.

How are the cyber operations of U.S. oil and gas companies impacted by COVID-19?

Like business and technology leaders worldwide, oil and gas chief information security officers (CISOs) are concerned about keeping their workforce healthy, while at the same time ensuring cyber operations are maintained to protect their information and operational technology (IT and OT). The mantra of "when, not if" attempts will be made to attack systems applies now more than ever.

On top of that, the oil and gas sector is dealing with a double whammy of COVID-19 and oil price declines driven by a price war between OPEC and non-OPEC producers, leading many organizations to rapidly review their capital spending for the year ahead. Despite the urgent need to maintain security, cyber projects are among those being delayed or canceled. The operations side of the house is looking to go leaner, with factory turnarounds being reduced or delayed as more social distancing protocols are put in place, resulting in a potential increase in risk to safety and the security of the OT landscape.

Finally, older populations are considered to be at a higher risk of complications from the virus. The potential impact of COVID-19 on oil and gas plant operations is heightened given the average decades-long experience of the plant workforce and the senior engineers with deep tribal knowledge.

What are the specific cyber concerns for oil and gas IT and OT?

As bad actors seek to take advantage of the situation during this period of reduced operational strength, we anticipate an increasing number of phishing attacks. In fact, 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] and cyber experts in the U.K. noted that online attacks are increasing and evolving.[2] Indeed, cyber adversaries are already taking advantage of the situation, and phishing emails related to COVID-19 are surging along with their malware payloads.[3] Typically, the attack vector is through corporate IT, then down into the industrial zone once the bad actor has identified the account of an employee involved in both IT and OT.

Meanwhile, refinery systems—including distributed control systems (DCS), supervisory control and data acquisition systems (SCADA), and programmable logic controllers (PLC)—rely on their proprietary vendors to provide support, traditionally on site or from suppliers' offices. Now stay-at-home orders and social distancing measures are forcing supplier personnel to work remotely, adding even more "hops." This has impacted a range of activities, from normal maintenance to dedicated projects and, importantly, system security and patching.

How is the industry dealing with increased cyber risk, while at the same time managing the dual COVID-19 and oil price challenges?

Every organization is at a different level in its maturity, operational response capabilities, and functional security organization. That said, most organizations have invoked their business continuity plans (BCPs) given COVID-19 travel and social distancing restrictions, and they are operating on a skeleton crew in the office. This works for most "corporate" employees who can function remotely with a laptop and VPN access.

However, the risk is potentially increasing at the plant operations level as staffing levels are reduced and remote working is ramped up, pressuring the IT and OT teams that manage those operations. And as mentioned, critical service partners such as DCS, SCADA, and PLC providers now also need to operate remotely. Where supply chain contracts already allowed remote access for these outside companies, access is now likely to be even more remote through the vendors' VPN networks—one further step removed. Security infrastructure at suppliers will also be under additional load as remote workers won't have traditional access to IT security tools and resources in the offices, elevating the risk of compromise.

[1] Source: Federal Bureau of Investigation. Alert Number I-032020-PSA: FBI sees rise in fraud schemes related to the coronavirus (COVID-19) pandemic. March 20, 2020.

[2] Source: National Cyber Security Centre. Weekly Threat Report 27th March 2020.

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

In order to accommodate the need for remote work, oil and gas organizations are having to increase remote infrastructure usage. However, that means more "holes" in the firewalls in both corporate and OT systems that require monitoring by the cybersecurity team, and an increased risk that malware, if successfully deployed in an environment, could impact safety, production, and operational integrity. Unfortunately, the economic realities of the current price war will no doubt continue to have effects on the operational delivery of cyber, as traditional security projects become subject to harsh budgetary reviews.

Meanwhile, from a health and safety perspective, plant operations will look to limit the exposure of workers, including by organizing shifts to keep the same smaller teams of engineers together to limit widespread COVID-19 exposure. However, this presents a potential headache should the virus impact one of the teams. Should the virus continue to spread among the workforce, current BCP operations will need to be further adjusted, though in the short term this shift-matching process should provide tactical relief. However, economic pressures (both supply and demand) will necessitate a rethink of operations in the medium term, along with increased pressure for factory turnarounds and maintenance windows (which traditionally have up to three times more staff on the factory floor) that allow for security patching as well.

Given concerns around the more at-risk older employee demographic, some organizations are kicking off accelerated, extensive documentation of plant operations and critical knowledge from engineers and other key employees. The documentation effort is often in conjunction with a review of the operational safety processes such as ISA-18.2, which focuses on capturing the alarm management logic for plant operations and the need for alarms to be in place.

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

- In the short term, consider the need to continue operating with reduced staffing under the BCP longer than anticipated. However, now also is the time to start updating the BCP in light of potential longer-term disruptions, and stress test the BCP for scenarios where multiple disruptions occur at the same time.
- Accelerate any planned security reviews, including a review of remote access arrangements and procedures for the OT organizations (looking for security quick wins for those who have remote access into the plant environment from the outside) and look at any OT hardening that can be done tactically.
- Consider whether security operations are robust and able to handle both the IT and OT layers, and where possible, increase the capability of the organization to "look for bad" on the networks.
- Review the OT risks around delayed patch deployments and the potential vulnerabilities those delays will cause, ensuring that you have compensating controls in place (e.g., ensuring the Safety Instrumented System [SIS] is still islanded from the rest of the network).
- Plan and conduct remote penetration testing activities to check and secure facilities, especially plant-side VPNs. (The concerns are now that this will need ongoing change and expansion, without resources to manage, police changes, and continually monitor.)
- Operational efficiency reviews: Conduct BCP/disaster recovery reviews with a focus on critical documentation to put "knowledge in heads" on paper and a look at a potential streamlining of plant procedures.
- Assess ways to help shore up defenses with quick wins, such as BCP or ops documentation reviews, process reviews, and toolsets risk remediation. Ensure best practice sharing across the organization and look to provide appropriate resources to help address the increasing confluence of risk.

By keeping these considerations in mind, along with ensuring regular cyber-readiness reviews, oil and gas organizations can help keep plants safe and secure while likely developing a number of new, effective ways of working that can be used again in the future.

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.

KPMG Global Energy Institute

The KPMG Global Energy Institute (GEI) is a worldwide knowledge-sharing form 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.

Jason Haward-Grau
Managing Director – Cyber Security Services
KPMG in the US
T: 713.319.2079
E: jhawardgrau@kpmg.com

April 9, 2020