POLSINELLI

Publications

October 28, 2024 • Updates

Cybersecurity for Critical Infrastructure Update – Incident Response Improves, Industry Standards Evolve

Critical infrastructure facilities are increasingly vulnerable to cybersecurity events, as demonstrated by the number of cyberattacks that have occurred this year against utilities including those in the energy sector (electricity, oil and natural gas, renewables), and water and wastewater systems sector (among some of the 16 sectors deemed 'critical').

For the latter sector, attacks have occurred in Texas, Kansas,[1] and Europe which included physical attacks on water towers and treatment facilities.[2] The Texas attacks involved industrial control system (ICS) interfaces (operational technology (OT)). Two weeks ago, a major utility in this sector successfully activated its incident response protocols and third-party cybersecurity experts.

That's a far cry from the Colonial Pipeline cybersecurity incidents in 2021 that halted one of the United States' largest pipeline systems due to a ransomware attack. Within days a state of emergency was declared in 17 states. The pipeline eventually resumed service, and Colonial acknowledged it paid $4.4 million to cyber criminals before restoring service.[3]

In April, we noted how government officials and cybersecurity firms were mandating improved readiness for critical infrastructure entities, and how new incident response recommendations issued by an important standard bearer (the National Institute of Standards and Technology) further elevated incident response within existing risk management frameworks.[4]

National Cybersecurity Strategy 2.0

In May, the White House released its 2024 Report on the Cybersecurity Posture of the United States, to update the public on the progress of the initiatives set by last year's National Cybersecurity Strategy Implementation Plan that vowed "to secure the full benefits of a safe and secure digital ecosystem."[5]

The Report outlines the current efforts taken by the administration, including top trends in critical infrastructure, emerging technologies, and artificial intelligence that cover 31 new initiatives and building on previous accomplishments to further efforts. The Report harkens

Related People

- Romaine C. Marshall
- Caitlin A. Smith
- Mary Ann H. Quinn

Related Capabilities

- Privacy & Cybersecurity
- Data Breach & Incident Response
- Energy

back to Pillar One of the Strategy's strategic objectives, emphasizing that the work is far from over.[6]

The newest addition to these efforts is the Critical Infrastructure Security Agency's AI roadmap addressing a plan to promote the beneficial uses of AI to enhance cybersecurity capabilities, ensure AI systems are protected from cyber-based threats, and deter the malicious use of AI capabilities to threaten systems relied on daily by Americans.[7]

The Department of Commerce has also been tasked with assessing the likelihood of AI being used to defend against threat actors. Yet, with these developments, the goal of concrete regulation and guidelines has not been realized. But with the passage of laws such as the Critical Infrastructure Reporting of Cybersecurity Incidents Act, new industry standards are expected.

Guidance for ICS and OT

For ICS and OT, there has been a sustained emphasis on recommended practices, including a prioritized set of security practices that are sector-specific and referred to as Cybersecurity Performance Goals. Indeed, CISA has made public numerous tools and resources for covered entities to enhance their programs.[8]

For example, in the water and wastewater systems sector, there is a new resource. Last month, the Environmental Protection Agency released *Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems*. The Guidance is 39 pages and includes numerous and specific resources to help with assessing gaps and reducing risk from cyberattacks.[9]

For ICS, the Guidance includes a desktop software tool that evaluates those security practices, provides links to industry handbooks, and a model with network segmentation guidance. For OT, the Guidance has a checklist of best practices that includes inventory, authentication, and training recommendations.

Relatedly, last month at the 15th Annual National Cybersecurity Summit in Huntsville, Alabama. Among the things discussed was how threats to ICS and OT systems can require separate incident response plans, especially since ICS and OT systems do not run on traditional operating systems and because they often have different control systems, sensors, and interfaces.

Conclusion

Cybersecurity and industry standards – i.e., the usual and customary practices in the delivery of products or services within a particular business sector – are rapidly evolving, especially for critical infrastructure. Experienced cybersecurity counsel can provide guidance on how to tailor compliance, especially for the main governance requirements.

To be most effective, partnerships between legal and technical professionals are ideal,[10] the latter being able to provide a greater understanding of how threat actor tactics, techniques and practices impact operations.[11] In rare instances, both sets of qualifications can be merged for certain sectors.[12] Under certain circumstances, confidentiality privileges can and should apply.

[1] https://www.bleepingcomputer.com/news/security/kansas-water-plant-cyberattack-forces-switch-to-manual-operations/

[2] https://foreignpolicy.com/2024/07/26/russia-sabotage-poison-finland-water-treatment/

[3] https://polsinelli.gjassets.com/content/uploads/2022/12/National-Security-Focus-on-Cybersecurity-for-Critical-Infrastructure-Sharpens-7.pdf

[4] https://www.polsinelli.com/publications/critical-infrastructure-cybersecurity-evolving-incident-response-obligations-integral-to-effective-risk-management

[5] https://www.jdsupra.com/legalnews/it-s-here-the-new-national-9071703/

[6] https://www.whitehouse.gov/oncd/briefing-room/2024/05/07/fact-sheet-cybersecurity-posture-report/

[7] https://www.cisa.gov/ai

[8] https://www.cisa.gov/news-events/news/cybersecurity-performance-goals-sector-specific-goals

[9] https://www.epa.gov/system/files/documents/2024-08/epa-guidance-on-improving-cybersecurity-at-drinking-water-and-wastewater-systems-1.pdf

[10] https://ampyxcyber.com/

[11] *See also* https://www.crai.com/services/information-security-and-privacy/

[12] https://www.cnksolutionscorp.com/