Deloitte.

Five in 5: Cybersecurity in the energy sector

Energy cybersecurity risks and mitigation strategies

As cyberattacks on energy infrastructure become more common, how can energy, resources, and industrials companies (ER&I) shore up their cybersecurity footprint and confidently confront emerging risks? Our latest Five in 5 article features input from Deloitte leaders on five key questions about cyber risk and cybersecurity in the energy sector.

1 What new, emerging risks do energy organizations face today, and how are they different from past cybersecurity risks in the energy sector?

Mike Kosonog: We're seeing two important cyber-related developments playing out in world events. First, the quantity of cyberattacks on energy infrastructure has increased substantially, magnifying organizations' need to protect against cyberthreats. Second, the world has shifted in the race to the Future of Energy in all its forms. Today's ER&I companies are moving the needle quickly on decarbonization, electrification, and growing their renewables portfolio—all against the backdrop of a rapidly changing technology and geopolitical landscape with more sophisticated threat actors. Some of these companies are creating joint ventures or new organizations to advance green initiatives. They'll need to make sure that energy cybersecurity is high on the agenda.

Sharon Chand: Over the last several years, the cyberthreat story was ransomware disrupting businesses, cities, and governments for financial gain. That's still happening, and it's not slowing down. Late last year, killware—malware focused on causing physical harm, or even death—emerged. The pace and volume of killware threats is increasing. Operations, especially from an energy resources or industrials perspective, is also a primary target. Bad actors continue to innovate how they attack their target and are hacking third parties more frequently as an avenue to their ultimate target. If I want to attack a big power company or multinational oil and gas conglomerate, I'm probably not going to go after them directly. Instead, I'll go after the 200-person startup IoT company that makes sensors that measure some critical part of the client's infrastructure. Why? That IoT vendor probably doesn't have the same level of cybersecurity funding and talent that the big company has. The ER&I industry is working on ways to prevent third-party attacks, but it's a very complex problem in an environment where every company depends on hundreds of different ecosystem partners to operate. Whether you're a supplier, consultant, or cloud and technology providers, no one is an island, so third-party attack vectors are an easier way for the bad guys to do harm.

2 How are these and other cyber risks likely to evolve in the near and long term?

Mike Kosonog: There are well-resourced threat actors at work all over the world and, as Sharon mentioned, tactics are evolving to move toward killware types of attacks. If some of these attacks take down critical infrastructure, there are health and safety concerns that go well beyond operational or financial losses. As we think about the Future of Energy and our clients' decarbonization goals, the speed to green is going to increase pressure to build new forms of energy generation, along with the systems and processes that support it. We're seeing energy cyberthreats at an all-time high in terms of volume. ER&I organizations will need to stay ahead of these threats, make sure they've budgeted for cybersecurity for the long term, and build in security by design.

Sharon Chand: What concerns me going forward are vulnerable, underfunded ER&I sectors like water. Water is distributed across the country, and there's little cyber regulation in place to require investments in protective measures. The nature of water as a utility makes it highly vulnerable to physical attack, but vulnerable control systems and IT environments also make water a high value target for cyberattacks. As cybersecurity in the energy industry ramps up protection for generating plants, alternative energy sites, and oil and gas pipelines, attackers are going to look for squishy, underprotected targets like water.

3 Who should be thinking about these security risks?

Sharon Chand: Eyes typically turn first to the chief security officer as the organizational leader for cyber and physical security. But the focus must expand to include operational leaders, like the COOs of power companies or product owners at industrial product companies, because that's where the risk lives. These leaders really understand the risks that their business has—and the funding support needed to mitigate those risks. The second thing I'd say is that everyone should be thinking about security risks because all it takes is one person in the organization to click on one link and the ransomware is activated in the environment. Or one person to share a password because his buddy forgot his and has to log onto the work management system and that's where the threat can enter the environment. The focus should be on training and individual responsibility. A "see something, say something" mindset is critical to have everybody be part of the solution.

Mike Kosonog: Everyone needs to double down on energy cybersecurity. The CXOs help drive and administer security at the enterprise level, but responsibility has to extend to support teams—the folks in audit, accounting, regulatory, human resources, supply chain, or production—to help build awareness and security into the organization. Also, including the line organizations and field operations is critical. They hold a lot of the budget, and they need to be the day-to-day face of cybersecurity.

4 What strategies or considerations can help energy organizations take steps toward mitigating these risks?

Sharon Chand: An important strategy is to identify and detect threats specifically targeting your sector or business and then continually monitor—internally, among supplier partners, and in the wider ecosystem—for patterns of abnormal activity that may indicate a threat has entered the environment. Also, look at things like zero trust. Previously, there was a lot of focus on making the perimeter of a company very difficult to get into. That protected the organization's soft center. Now, that perimeter is gone because a company is connected to its cloud provider, the grid system, and other ecosystem partners across the company's footprint. We need to extend cyber controls out to the end points where zero trust has a strong role to play. Finally, resilience planning is essential. This means understanding how to recover and restore operations when there is a cyber incident, or war-gaming so you have that muscle memory of working across the organization to respond and recover quickly in an emergency.

Mike Kosonog: Cyber agents and their threats are continually evolving, so an energy company's cybersecurity model and initiatives must evolve as well. Monitoring, detection, and incident response planning should be ongoing and integrated into a company's information technology and operating environments. Adopting a zero trust security posture is a key mindset shift organizations need to focus on. Never trust and always verify, both inside and outside the organization. Also, home in on the cyber maturity of new technologies, processes, and products. Illuminate ecosystem risks of growing importance and champion security awareness throughout the organization.

5 What sorts of partnerships or alliances can help energy organizations confidently take on these emerging threats?

Mike Kosonog: We are strong advocates of public-private partnerships to share cyberthreat intelligence and mitigation strategies. There are always opportunities for additional information sharing and program support from federal agencies. State governments could assist energy companies with rate cases for cyber investments. Industry consortiums could leverage their resources for mutual advantage.

Sharon Chand: There is a tremendous need for developing more and more cyber talent to keep pace with rapidly escalating threats. Public-private partnerships could provide funding to nurture talent at community organizations, elementary and high schools, and community colleges. The other alliance I'd highlight—and this one is within ER&I companies—is between IT and accounting. How can those two functions work together to formulate budget requests that articulate the value of cyber protection investments?

Want to learn more about cybersecurity in the energy sector? Check out this Deloitte resource:

Managing cyber risk in the electric power sector | Deloitte Insights

Get In Touch:

Mike Kosonog
Partner | Deloitte Risk & Financial Advisory
Energy, Resources & Industrials industry leader

Sharon Chand
Principal | Deloitte Risk & Financial Advisory
Cyber Risk Secure Supply Chain Leader

About Deloitte

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.