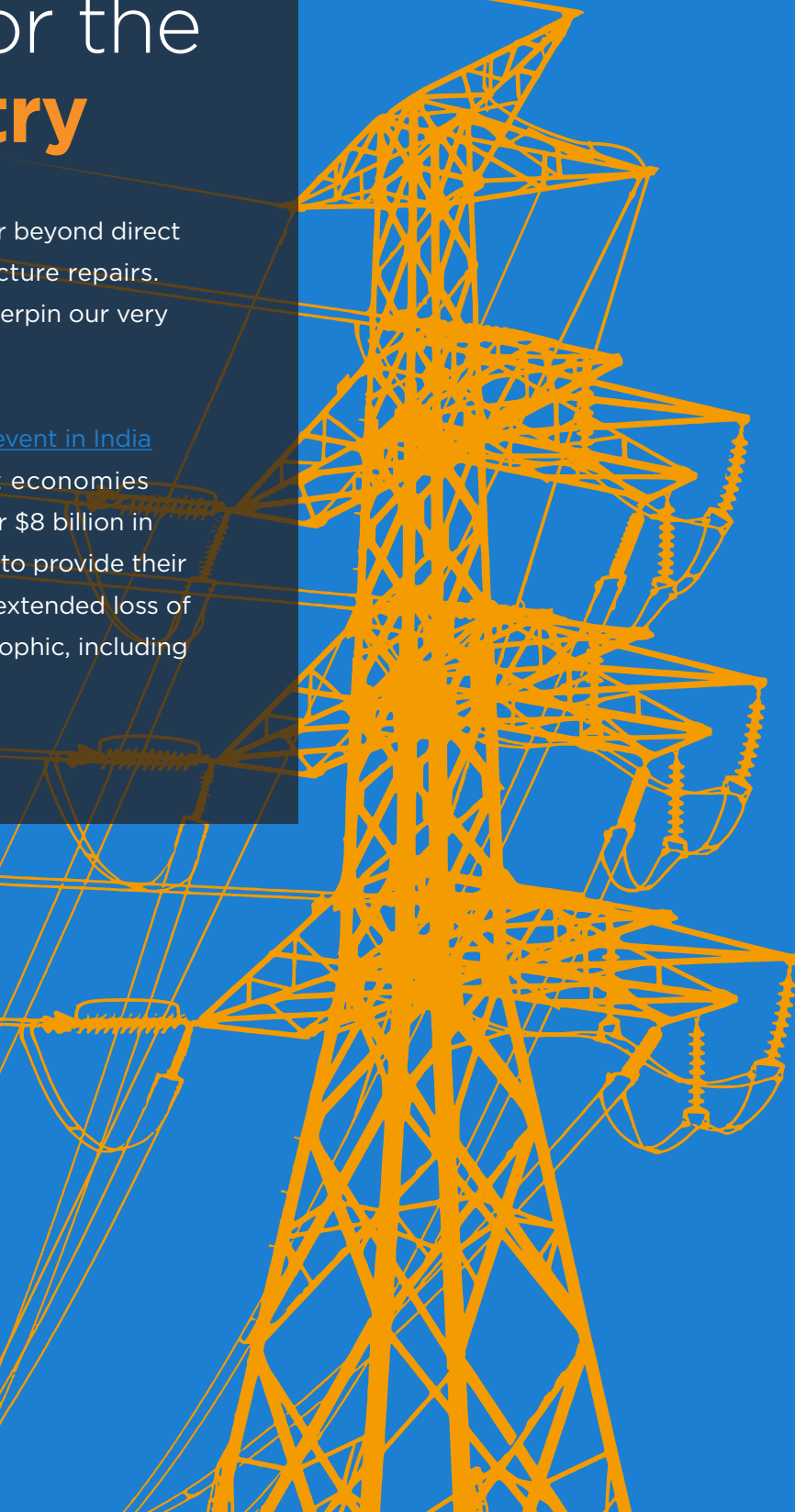


Risk Hunting for the **Utilities Industry**

For utilities, the threat of cyberattacks goes far beyond direct costs, like ransomware payouts and infrastructure repairs. Utilities provide the essential services that underpin our very way of life.

Blackouts can sow social chaos (like the [2012 event in India](#) that impacted 700 million people) and hurt economies (like the [2003 event in the US](#) that caused over \$8 billion in damage). Other industries also rely on utilities to provide their own vital functions. Perhaps most notably, an extended loss of utilities at healthcare facilities could be catastrophic, including extensive loss of life.



CHALLENGES OF CYBER DISRUPTIONS TO ELECTRIC, WATER, AND OIL & GAS SUPPLIERS

Each segment of the utility industry faces its own distinct cybersecurity challenges.



IN THE OIL & GAS SECTOR, cybersecurity concerns revolve around the industrial control systems (ICS) that manage fuel pipelines.

The good news is, pipeline systems have fail-safes and redundancies to prevent cascading failures. They also feature mechanical controls that cyberattacks cannot override.

Still, due to the flammability of hydrocarbons, a single incident could trigger an explosive situation, literally. So while it might be hard to disrupt a pipeline system for long, the scale and psychological impact of a successful cyberattack could be significant.



IN THE WATER SECTOR, distribution is also dependent on ICS, particularly Systems Control and Data Acquisition (SCADA) networks. These systems automate and manage the physical processes required for treating and delivering clean drinking water.

The good news is, water systems are generally not connected to each other. And the vast majority of systems in the US— about 49,000 of 53,000—are small to medium in size. That presents a fragmented attack surface, requiring a significant effort to impact many people.

However, the 4,000 largest drinking water systems in the country serve over 80% of the population, making them attractive targets. And the Department of Homeland Security has reported that cybersecurity “incidents” in the water sector account for more than 8% of all such events in the US.



IN THE ELECTRICITY SECTOR, “smart grid” technology has made power generation-transmission-distribution systems more connected and complex. At the same time, regulations and cyber defenses have varied across jurisdictions. So the US power grid is vulnerable to cyberattacks. And since the grid is vital for every aspect of the US economy, it’s a high-value strategic target for adversaries.

The good news is, government agencies focus intently on the electricity sector, deploying significant resources to protect it against cyberattacks.

On the other hand, that’s because they need to. Advanced persistent threat (APT) actors (especially Russia and China) regularly probe the US electrical grid for ways to exploit weaknesses. According to the US Computer Emergency Readiness Team (US-CERT), the energy industry (led by the electricity sector) records more cyber incidents than any other segment of the US economy.

And because the US power grid is so interconnected, the risk of large-scale cyberattacks is high. Coordinated attacks could spread quickly and cause many simultaneous failures, resulting in massive, cascading losses.

CYBER RISKS TO UTILITIES ARE NOT JUST HYPOTHETICAL

Even more concerning, cyber warfare on power grids has been tested successfully.

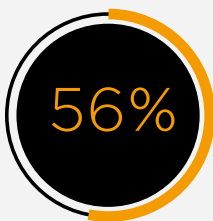
In 2015 coordinated cyberattacks hit Ukraine in a 30-minute span, causing power outages in three regions, affecting 225,000 people. According to an [alert](#) from the US Cybersecurity & Infrastructure Security Agency (CISA), [BlackEnergy malware](#) was found in “a variety of critical infrastructure.”

The attackers took remote control over circuit breakers, using compromised OS admin tools and ICS client software. To interfere with restoration, they also corrupted Serial-to-Ethernet device firmware and disconnected Uninterruptable Power Supplies at electric substations. In the aftermath, the attackers “wiped” systems with [KillDisk malware](#), erasing files and corrupting master boot records, leaving the systems inoperable.

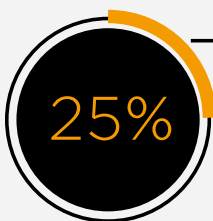
The attacks were most likely initiated via Word and PowerPoint attachments to emails. The malware launched automatically when recipients opened the files. But cyberattacks can also be executed without online connections—particularly through USB “thumb” drives. As noted in the [Harvard Business Review](#), “too often energy companies believe that if they are not directly connected to the internet they are safe from attack.”

Cybersecurity experts blame Russia for the Ukraine cyberattack (and many others, including attempts to compromise the 2017 French elections and 2018 winter Olympics). The US Department of Justice [indicted six members](#) of Russia’s GRU military intelligence unit for these crimes. The cyber-defense community knows these GRU threat actors as Sandworm, Voodoo Bear, Iron Viking, and other aliases.

ACCORDING TO A [JOINT STUDY](#) FROM SIEMENS ENERGY & PONEMON INSTITUTE,
OF THE GLOBAL UTILITIES COMPANIES SURVEYED...



HAD AT LEAST ONE SHUTDOWN OR
OPERATIONAL DATA LOSS PER YEAR



HAVE BEEN IMPACTED BY
MEGA-ATTACKS WITH EXPERTISE
DEVELOPED BY NATION-STATE ACTORS

CYBER RISKS LURKING INSIDE US UTILITIES

A related group, known as [Berserk Bear, Energetic Bear, or Dragonfly](#), has infiltrated US energy infrastructure, including electrical distribution systems and nuclear power plants. It has performed reconnaissance, exfiltrating ICS data and other information.

Perhaps the Russians are waiting for a strategic moment to attack. Or they are sending a message—that they could attack any time—to deter US cyber operations against Russia. Or they just want to provoke a response from [US Cyber Command](#) to tie up resources. Or all of the above.

[Dragonfly used Havex malware](#) to gain administrative control over target computers. Delivery tactics included spear-fishing emails to install remote-access Trojan horses (RATs); “watering hole” attacks to redirect utility personnel from real websites to Dragonfly-controlled servers; and hacks of utility vendors to infect ICS software. [Symantec found](#) that, among other compromised data, the hackers captured screenshots of circuit-breaker control panels.

Perhaps even more distressing is the wide availability of hacking tools on the Dark Web. As the [MIT Sloan Management Review](#) pointed out, “Tools to accomplish attacks are increasingly available... at decreasing costs, including cyber weapons stolen from the NSA and CIA.” Indeed, many of the techniques used in the Ukraine power grid cyberattack were available on the black market.

All of this makes utilities especially vulnerable to ransomware, distributed denial-of service (DDoS) attacks, and malware-induced equipment failures.

Utilities need a better way to understand risk conditions and their potential downstream impacts. More specifically, the industry needs a way to hunt for risks—and mitigate them—before a cyberattack occurs.

RISKS GROW DESPITE IT EFFORTS

Most energy providers follow the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). Many also apply additional standards, like the ISA/IEC 62443 Standards on Industrial Automation and Control Systems Security. And IT organizations do their best with the tools available—they segment networks to isolate devices, use configuration management tools, and scan/patch vulnerabilities.

But these approaches tend to focus on a limited number of technical issues, which account for only about one-quarter of all cyber risks. They do not fully cover wider-ranging problems with misconfigurations, permissions, data exposures, and simple IT oversights that cause security “drift.”

Also, most security tools do not understand technical issues in context with their real-world impacts. So IT teams get bogged down in triage. Overwhelmed with alerts, security analysts cannot prioritize issues by the impact they might actually have on critical utility services.

Analysts often react to the latest tactical “fires,” instead of proactively hunting for strategic risks that pose the grimmest consequences.

WHAT UTILITIES NEED

[ICS-CERT](#) “strongly encourages organizations across all sectors to review” their mitigation strategies. And the [Harvard Business Review](#) spells out how utilities need to shift their cybersecurity focus:



Think ahead with vision and imagination, instead of “fixing the last problem.” Attackers will analyze your response to their cyberattacks to make their next one more devastating.



Emphasize downstream internal impacts over external causes. You can’t control your adversary, who’s always morphing, but you can control many aspects of your own attack surface. So examine your “crown jewels,” understand how attacks could get to them, and identify the best way to pre-mitigate risks internally.







Don’t ignore system interdependence and assume failures will be isolated. You need to map how attacks could transition inside your environment, and look at how multiple failures might occur simultaneously.

Part of the problem is that finding risk conditions in utility environments is difficult. Many network-connected systems and devices do not support software agents, or cannot be scanned at all. And even when possible, vulnerability scans are far from perfect. As noted above, formal “vulnerabilities” make up only about 25% of all risk conditions in a typical environment.

Utilities also need to understand the contextual relationships between their network nodes. A risk that impacts one node could spread to others. Gauging these risk interactions is hard enough, due to the vast number of nodes in utility systems. But it is even more difficult to quantify risks when they can multiply exponentially.

UTILITIES SHOULD BE ABLE TO ANSWER QUESTIONS LIKE:

-  Do we understand the potential entry points for attacks on our network? Where do attacks have the highest probability of success?
-  Do we understand the combinations of technical conditions that allow attacks to succeed? What is the likelihood that our mitigations will be effective in correcting these conditions?
-  Do we understand how attacks can spread? Have we modeled the interrelationships of our assets throughout the environment?
-  If an attack occurs, do we understand which mitigations would minimize the impact?

NEW RISK HUNTING TECHNIQUES OFFER A SOLUTION

“Risk Hunting” tools, like Epiphany Intelligence Platform™, let organizations answer these kinds of questions.

A Risk Hunting platform absorbs data from existing network, security, and domain sources. (Epiphany is agentless; it does not directly interrogate data sources, so it does not disrupt any processes or operations.)

Risk Hunting looks at the current state of all technical risks—including those common IT issues that cause security drift. Risk Hunting also analyzes how those risks could potentially migrate across network paths. And Risk Hunting integrates an understanding of the operational value of each node on the network.

That all translates into an ability quantify cyber risk in context with what is most important to the organization. For utilities, that means understanding what risks could cause the most damage to their business and customers— and how.

With this deeper understanding, utilities can prioritize defenses to better protect against the risk conditions that could make them vulnerable to cyber attacks.



Awareness powers protection.

Contact us today to get started with Epiphany.

Contact Us 

ABOUT EPIPHANY SYSTEMS

Epiphany delivers world-class cybersecurity solutions for enterprises in every sector of government and industry, including the Fortune 500. We are dedicated to reducing technical and business risks through innovative technologies, including artificial intelligence and machine learning.

Our mission is to safeguard our clients' data, assets, and operations across the globe. We assess each client's unique needs and challenges to ensure that their risks are visible, managed, and mitigated. If it's connected, it must be protected.

