Mirazon

GUIDE

The Utility Provider's Cybersecurity Survival Guide

How Utility Providers Can Strengthen Reliability, Reduce Risk, and Protect Critical Infrastructure

www.mirazon.com
(502) 240-0404
info@mirazon.com

Keeping the Lights On Isn't Getting Easier

Most utility providers didn't get into this business because they wanted to worry about ransomware.

They worry about outages. They worry about reliability. They worry about keeping essential services running for the communities that depend on them.

But today's reality is different from what it was ten or even five years ago.

Your substations are connected. Your field crews rely on mobile devices. Vendors need remote access. Operational systems share data with business systems. Customers expect digital experiences.

And cybercriminals know exactly how important those systems are.

That means cybersecurity is no longer just an IT issue. It's an operations issue, a reliability issue, and a public trust issue.

When a utility experiences downtime, the impact reaches far beyond the server room. Customers, businesses, and communities all feel it.

The good news? You don't need to become a cybersecurity expert overnight.

You need a strategy that helps you reduce risk, improve resilience, and keep critical systems running when it matters most.

That's exactly what this guide is designed to help you do.

Why Utilities Have Become a Prime Target

If you were a cybercriminal, where would you focus your attention?

A company that can afford a little downtime? Or a utility provider that supports thousands of homes, businesses, and critical services? Unfortunately, criminals already know the answer.

Utility organizations are attractive targets because disruption carries real-world consequences. When people depend on you for essential services, even a brief interruption can create challenges that ripple far beyond your organization.

What makes utilities especially vulnerable isn't usually a single weakness. It's the reality of managing a complex mix of systems, technologies, and infrastructure that have evolved over time and all need to work together reliably.

Most utility environments contain:

- Operational Technology (OT)
- Industrial Control Systems (ICS)
- SCADA Platforms
- Business Applications
- Customer Systems
- Legacy Equipment
- Third-Party Vendor Connections
- Cloud Services

Each system serves an important purpose, but every connection also creates another potential entry point for risk.

The challenge isn't eliminating technology or avoiding innovation. It's making sure the systems your organization depends on every day are managed securely, monitored appropriately, and positioned to support reliable operations well into the future.

The Hidden Risks Inside Utility Environments

Legacy infrastructure isn't going anywhere.

Most utilities still rely on systems that were built with reliability in mind long before cybersecurity became a primary concern. And honestly, that makes sense. When equipment works and continues to support critical operations, replacing it isn't always practical or financially justified.

Many utility providers are balancing the need to modernize with the reality of maintaining systems that have been supporting their operations for years.

The trouble comes when older systems become connected to newer technologies without the proper protections in place. As networks, applications, and operational systems become more interconnected, it can be difficult to maintain visibility and manage risk across the entire environment.

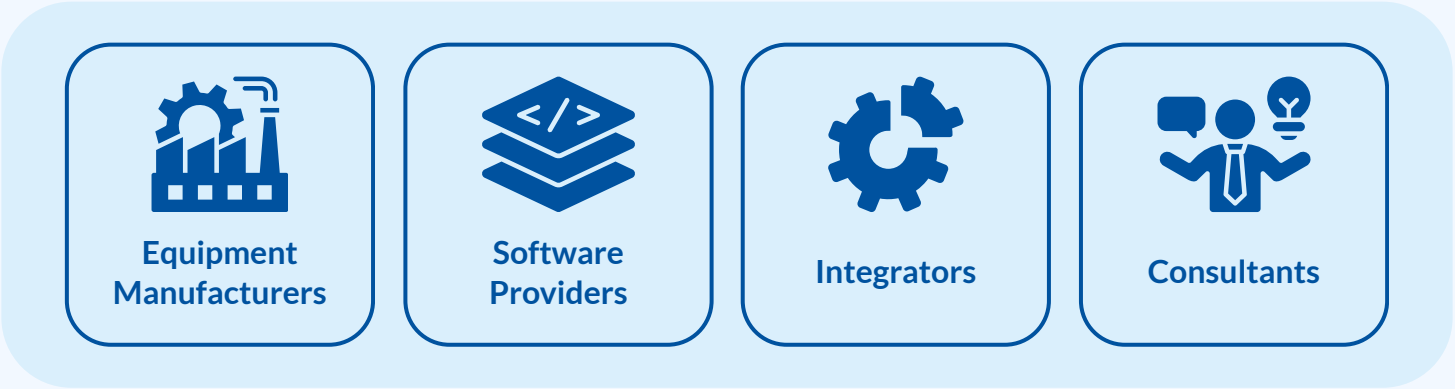
These challenges can include:

- Unsupported Operating Systems
- Older Network Equipment
- Limited Visibility Into Operational Environments
- Inadequate Segmentation Between Systems
- Inconsistent Patching Processes

None of these challenges are unique to the utility industry, and they don't necessarily mean an organization needs to start from scratch. It's about understanding where risk exists, prioritizing improvements, and taking practical steps that strengthen security while supporting the reliability and uptime your operation (and community) depends on.

Vendor Access Creates Opportunity

Modern utility providers depend on outside partners who often require access to critical systems:



Whether it's a software vendor troubleshooting an issue, a contractor supporting a project, or a manufacturer maintaining equipment, third-party access is simply part of day-to-day operations. That access helps keep everything moving, but it can also create risk if it's not properly managed.

The key is making sure that access remains secure, appropriate, and aligned with business needs as your vendor relationships evolve. Questions worth asking include:

- **Who currently has access?**
- **Is access reviewed regularly?**
- **Is Multifactor Authentication (MFA) required?**
- **Are vendor activities monitored?**

The fewer unknowns you have, the stronger your security posture becomes. On the other hand, the more unknowns you have, the greater the risk is to your environment.

DID YOU KNOW?

"Cyberattacks against U.S. utilities increased 70% in 2024 compared to the same period in 2023."

Source

Reliability Starts With Cyber Resilience

Too many organizations think cybersecurity is about stopping every attack, but that's not realistic. The organizations that perform best understand a different truth: Attacks may (and most likely will) happen, but preparation determines the outcome.

That's where cyber resilience comes in. **Cyber resilience** means your organization can continue operating, recover quickly, and minimize disruption when something goes wrong.

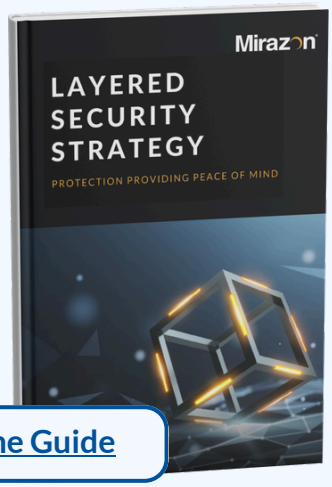
Build a Layered Security Strategy

Think of security like the safety systems in a utility operation.

You wouldn't depend on a single breaker, alarm, or backup system. Cybersecurity works the same way. Effective protection requires multiple layers working together, including:

- Endpoint Protection
- Next-Generation Firewall (NGFW)
- Email Security
- Multifactor Authentication (MFA)
- End-User Training/Security Awareness Training (SAT)
- Assessments and Monitoring
- DNS Filtering

Layered security reduces risk because attackers must overcome multiple controls instead of just one.



Download the Guide

Segment Critical Systems

One compromised device should never provide access to your entire environment. Segmentation helps isolate critical systems and limit the spread of threats. For utilities, that means creating separation between:

- Corporate IT systems
- Operational Technology (OT)
- SCADA environments
- Vendor connections
- Remote access services

When combined with layered security, segmentation creates multiple barriers that help contain threats, minimize downtime, and keep critical business operations running smoothly.

Compliance Matters. But Compliance Isn't Security.

Many utility providers spend a significant amount of time and resources preparing for audits, documenting controls, and meeting regulatory requirements. And that's a good thing.

Compliance frameworks create accountability and establish minimum security expectations. They help organizations build consistency into their processes and reduce unnecessary risk.

But compliance should never be mistaken for complete protection.

Think of it this way: Passing a driver's license test doesn't automatically make someone a safe driver. In the same way, meeting regulatory requirements doesn't automatically make an organization secure.

Many organizations discover this the hard way after suffering a cyberattack despite being fully compliant. That's because **compliance frameworks are designed to establish a baseline**.

Cybercriminals aren't interested in whether you've checked the right boxes. They're looking for vulnerabilities, oversights, and opportunities to gain access.

That's what makes cybersecurity so challenging. The threat landscape changes constantly. Attack techniques evolve, new vulnerabilities emerge, and business environments grow more complex every year.

At the same time, many compliance frameworks move at a much slower pace. While they provide an important foundation, they aren't designed to keep up with every new threat as it appears. That creates a gap between being compliant and being truly secure.

The Compliance Trap

One of the most common mistakes organizations make is adopting a "we passed the audit, so we're good" mindset. Unfortunately, that's where risk often begins.

Real cybersecurity requires organizations to look beyond annual audits, documentation reviews, policy requirements, and regulatory checklists.

It requires an ongoing commitment to assessing risk, improving processes, and continuously strengthening defenses.

What Security Maturity Looks Like

Organizations with mature cybersecurity strategies typically go beyond compliance requirements and focus on practical risk reduction. That includes:

Continuous Monitoring

Threats don't wait for annual reviews. Continuous monitoring provides visibility into unusual activity, suspicious access attempts, and potential security issues before they turn into major problems.

Vulnerability Management

New vulnerabilities are discovered every day. A mature security strategy includes regular reviews, remediation efforts, and prioritization of the risks that matter most.

Security Awareness

Employees remain a common target for cybercriminals. Security-conscious organizations invest in regular training and reinforcement (we'll talk more about this a little later).

Incident Response Planning

When an incident occurs, everyone knows:

- Who is responsible
- What actions need to happen
- Which systems take priority
- How communication should occur

That level of preparedness helps reduce confusion when every minute matters. Is your incident response plan solid? Here are five ways to find out.

Security Is a Journey, Not a Destination

The reality is simple: Cybersecurity isn't something you finish. It's something you continuously improve.

Organizations that stay resilient understand that compliance is an important milestone, but it's never the final goal.

The goal is maintaining the reliability, stability, and trust your customers depend on every day.

Disaster Recovery Is About More Than Backups

Let's talk about a question every utility provider should be able to answer:

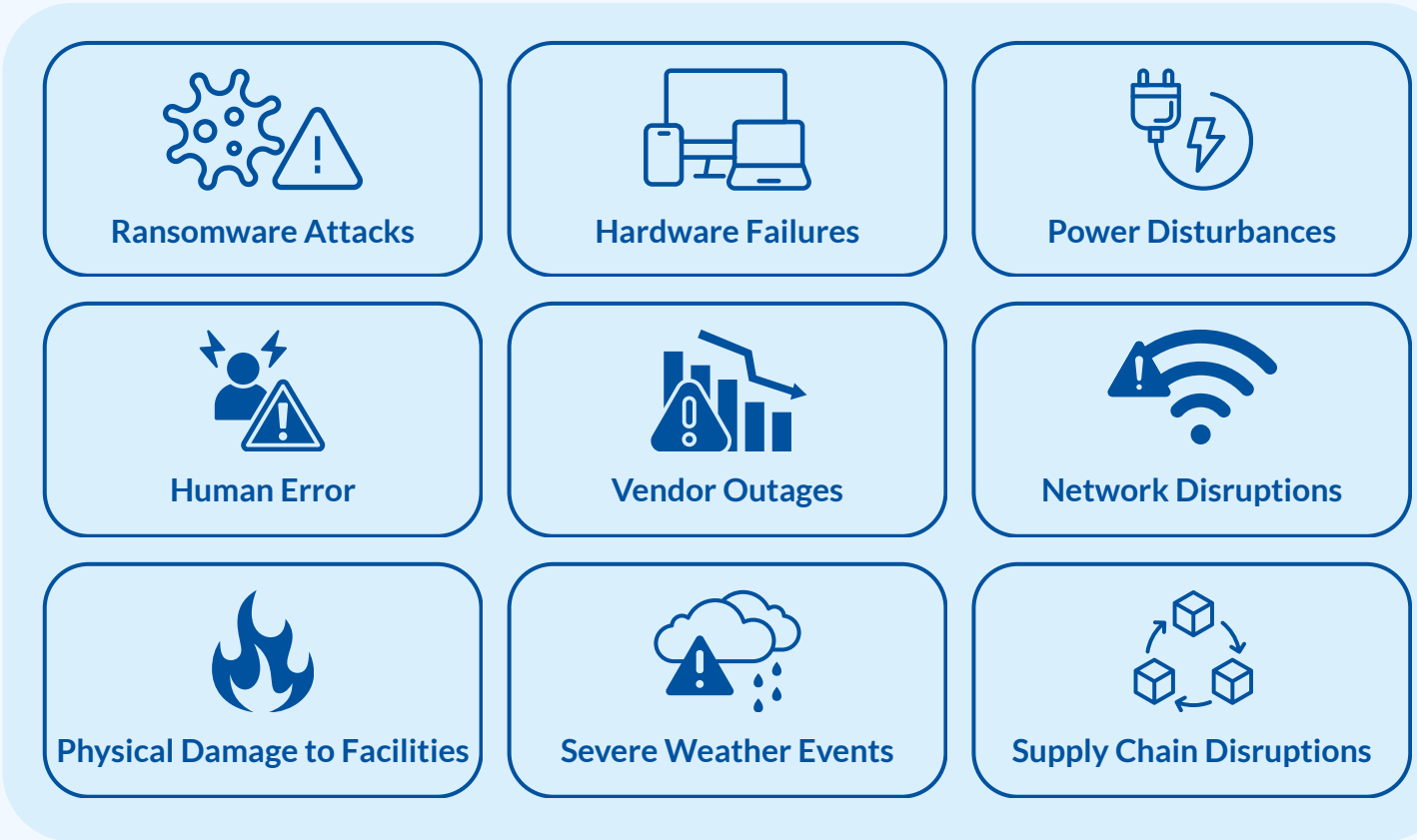
If a critical system failed right now, how quickly could we recover?

Most organizations immediately think about backups, and backups are important. They're essential. But they are only one piece of the puzzle.

A backup without a recovery strategy is like owning a spare tire without knowing how to change it. You're better off than having nothing, but you're still not ready for the situation.

Utility Organizations Face Multiple Types of Disasters

When most people hear the word "disaster," they usually picture severe weather events. But for utilities, disasters come in many forms. Examples include:



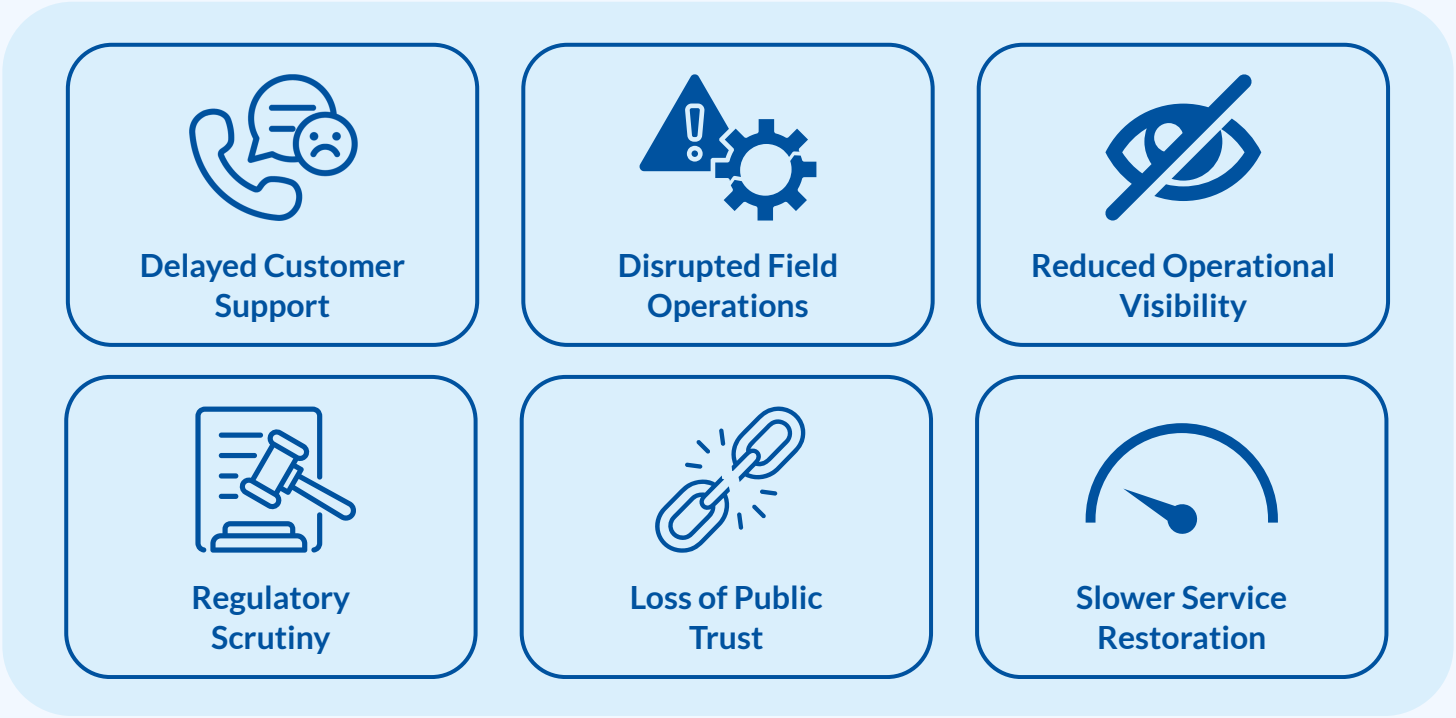
The cause may vary, but the result is often the same: Critical operations are interrupted, customers are affected, and pressure rises quickly. That's why having a disaster recovery plan in place is so important. It gives your organization a clear path to restore critical systems, minimize downtime, and keep the business moving when the unexpected happens.

Downtime Costs More Than Money

Every organization understands that downtime can be expensive. However, utility providers face a unique challenge because the impact extends far beyond lost productivity or revenue.

When critical systems become unavailable, customers, field crews, and the communities you serve can all feel the effects.

When systems become unavailable, the consequences can include:



That's why resilience matters. While no organization can prevent every disruption, a well-defined disaster recovery strategy can help minimize operational impacts, accelerate recovery efforts, and maintain confidence during challenging situations.

At the end of the day, disaster recovery isn't about avoiding every problem. It's about being prepared to respond effectively when problems occur (because there's no doubt that they will).

DID YOU KNOW?

"The energy and utilities sector saw an 80% year-over-year increase in ransomware activity, with spear phishing and credential theft identified as common initial access methods."

Source

The Four Questions Every Utility Provider Should Answer

A strong disaster recovery strategy begins with four simple questions:

What Systems Matter Most?

Not every system carries the same level of risk. Understand which applications, operational systems, and infrastructure are truly mission-critical.

How Long Can We Operate Without Them?

Different systems require different recovery priorities. Some applications may tolerate hours of downtime. Others may require near-immediate restoration.

How Will We Recover?

Recovery should never depend on tribal knowledge or a single employee. The process should be documented, tested, and repeatable.

Have We Actually Tested It?

This is where many plans fall short. Organizations often discover gaps only *after* an actual incident occurs. The strongest recovery strategies are tested regularly so those gaps can be identified and remediated *before* something happens.

Building Recovery Confidence

A resilient recovery strategy should include:

- Documented recovery procedures
- Offline backup protection
- Immutable backup storage
- Recovery testing
- Secondary recovery locations
- Communication plans
- Defined recovery objectives
- Clear leadership responsibilities

The goal isn't perfection. The goal is confidence.

When a disruption occurs, your team should know exactly what happens next.

Organizations that routinely test and improve recovery strategies are significantly better positioned to minimize downtime and maintain business continuity.

Your Employees Are Part of the Security Strategy

Technology gets most of the attention. Firewalls, security tools, monitoring platforms, and advanced threat detection all play important roles.

But here's a truth that often surprises people: **Many cyberattacks begin with a human being.**

Not because employees are careless or untrained, but because they're busy doing their jobs and solving problems. And attackers know it.

That's why social engineering remains one of the most effective techniques in a cybercriminal's toolbox.

Attackers Target People First

Cybercriminals understand that compromising a person is often easier than compromising a server.

Attackers frequently rely on:

These attacks aren't always obvious. In fact, they rarely are.

Most of the time they're sophisticated, convincing, and designed to create a sense of urgency.

One click. One downloaded file. One compromised password. That's often all it takes.

Building a Security-First Culture

The organizations with the strongest cybersecurity strategies don't treat security as an annual training requirement. They make it part of their **culture**.

That means security becomes everyone's responsibility. Not just IT's. Not just leadership's. Everyone's.

Every employee plays a role in protecting the organization, whether they're reviewing an invoice, opening an email, sharing files, or approving a request. Small actions taken by attentive employees can stop potential threats before they become major security incidents.

Employees should feel comfortable:

Recognizing and reporting potential threats before they become business disruptions.

Questioning requests that seem unusual, even when they appear to come from trusted sources.

Verifying identities and intentions before sharing sensitive information or granting access.

Escalating suspicious activity quickly so security teams can investigate and respond effectively.

Serving as an extra layer of protection, helping identify risks that technology alone may not catch.

It’s not about creating security experts out of every employee. It's about creating a workplace where people stay aware, trust their instincts, and understand that speaking up is always the right move.

Learn more about Security Awareness Training (SAT) here.

Quick Self-Assessment

How Many Best Practices Can You Check Off?

Check every statement that applies to your organization.

- [ ] Critical systems are running on supported, up-to-date software
- [ ] Operational and business networks are properly segmented
- [ ] Multifactor authentication (MFA) is enabled wherever it should be
- [ ] Vendor access is monitored, documented, and easy to track
- [ ] Employees receive regular cybersecurity awareness training
- [ ] Incident response plans are tested and updated on a regular basis
- [ ] Backup recovery processes are tested frequently and successfully
- [ ] Network activity is monitored with strong visibility across the environment
- [ ] Cybersecurity roles and responsibilities are clearly defined
- [ ] A complete and current inventory of assets is maintained

The more boxes you can check, the stronger your security foundation likely is.

If there are a few gaps, don't panic. Every utility provider has opportunities to strengthen their cybersecurity posture.

The key is identifying what's missing, prioritizing improvements, and taking action before a threat becomes an incident.

The Bottom Line

Utility providers have always focused on delivering dependable service to the communities they serve. While the technology behind that service continues to evolve, the goal remains the same: **keeping operations running smoothly and being ready for whatever comes next.**

The organizations that are best positioned for the future aren't necessarily the ones with the newest technology. They're the ones taking a thoughtful, proactive approach to risk, investing in their people and processes, and making strategic decisions that support long-term reliability.

By strengthening your cybersecurity posture today, you're not just protecting systems. You're building confidence in your organization's ability to adapt, respond, and continue delivering the service your customers count on every day.

How Resilient Is Your Utility Environment?

Cyber threats continue to evolve, and the technology supporting utility operations continues to grow more complex. At the same time, regulatory expectations and operational demands keep rising. That's a lot to manage.

The good news is you don't have to navigate those challenges alone.

Contact Mirazon today to start the conversation. We'll help you explore opportunities, address challenges, and build a technology roadmap that supports your goals both today and in the years ahead.

Contact Us

Mirazon®

www.mirazon.com
(502) 240-0404
info@mirazon.com