



What You Should Expect to Pay for IT Support for Your Business

How to Evaluate Providers, Understand Pricing, and Choose the Partner Who Protects Your Productivity

By Dan Reisig, VP of Technology & Innovation

UVSTechnology.com
316-613-4749
MSP@uvsinc.com
245 N Waco Suite T100, Wichita, KS 67202

WRITTEN FOR BUSINESS LEADERS WHO WANT CLARITY, CONTROL,
AND CONFIDENCE IN THEIR TECHNOLOGY PARTNERSHIPS.

```
1 .box{
2   position: absolute;
3   top: 50%;
4   left: 50%;
5   transform: translate(-50%, -50%);
6   width: 400px;
7   padding: 40px;
8   background: #fff;
9   box-sizing: border-box;
10  box-shadow: 0 15px 30px #000;
11  border-radius: 10px;
12 }
13
14 .box h2{
15   margin: 0 0 30px 0;
16   padding: 0;
17   color: #000;
18   text-align: center;
19 }
20
21 .box h3{
22   margin: 0;
23   padding: 0;
24   color: #000;
25 }
```



FROM THE DESK OF DAN REISIG

Dear Colleague,

If you're exploring outsourced IT support or comparing managed service providers, you've probably noticed how confusing, and inconsistent, this industry can be.

Over the years, we've helped organizations across healthcare, legal, manufacturing, and professional services

navigate this same challenge. Many had overpaid for inconsistent service, signed restrictive contracts, or discovered hidden fees long after the ink was dry. This guide exists to make sure you don't have to learn those lessons the hard way.

It's designed to help you make an informed, confident decision about IT — one that supports your operations, not complicates them. In this guide, you'll find insight from professionals who believe in transparency, prevention, and long-term partnership.

Dan Reisig
VP of Technology & Innovation

WHAT YOU'LL LEARN INSIDE THIS GUIDE

Think of this as your blueprint for evaluating IT providers.

You'll discover:

- The three common IT service models and which one best aligns with your business goals.
- How different pricing structures work and how to recognize hidden costs before they appear.
- What proactive IT really looks like (and how it prevents emergencies instead of billing for them).
- Sixteen questions to ask before signing a service contract.
- Common red flags to recognize

WHY THIS GUIDE MATTERS

The IT industry can be confusing. Pricing models vary widely, and "all-inclusive" contracts often include costly surprises. Our goal with this guide is to simplify what's complex and help you make decisions based on clarity, not sales pressure.

We'll share the knowledge and experience we've gained over decades of managing technology for growing organizations. You'll learn what works, what to watch for, and how to build a partnership that supports your goals long-term.

The Three IT Service Models

Before you can compare providers or pricing, it's important to understand how IT services are typically structured. Most companies fall into one of three categories — or a hybrid of these models. Each has benefits, drawbacks, and ideal use cases depending on your business needs.

1 BREAK-FIX (TIME AND MATERIALS)

In this model, you pay an hourly rate when something breaks or when you need help with a specific issue or project. It's straightforward: you call, they fix the problem, and you're billed for the time.

When It Works Best

- For small businesses with minimal infrastructure.
- For one-time projects, like an email migration or software upgrade

2 MANAGED IT SERVICES

This is the model most modern businesses rely on.

A managed services provider (MSP) acts as your outsourced IT department, offering comprehensive support for your network, systems, and users. Services often include proactive monitoring, cybersecurity, help desk, backups, and strategic planning.

When It Works Best

- For businesses that rely on uptime, compliance, and predictable costs.
- For growing organizations that need expert oversight without hiring a full internal IT team.
- When an in-house IT department wants to augment its team with specialized expertise or outsource certain tasks to focus on strategic priorities.

3 VENDOR-SUPPLIED IT SUPPORT

Some software vendors, especially those offering industry-specific systems, provide limited IT support for their own products. They'll troubleshoot the application, but that support doesn't extend to your entire network.

When It Works Best

- As a supplement to your IT team or MSP.
- For niche applications that require vendor expertise.

“Under the break-fix model, your provider only makes money when something goes wrong. That's not a partnership, it's a reaction.”

Which Model Is Right for You?

Each model serves a different purpose, what matters most is how well it aligns with your goals, risk tolerance, and resources. For most small and midsize organizations, Managed IT Services provide the best balance of value, security, and predictability. This model gives you proactive monitoring, consistent performance, and a clear cost structure that supports growth and compliance.

A Break-Fix approach can still make sense for limited or one-time projects, especially if your team already handles daily IT tasks in-house. However, relying on it long-term often leads to higher costs and greater operational risk.

Vendor-Supplied IT Support is best viewed as a supplement, ideal when specific applications require specialized vendor expertise, but not a complete IT solution on its own.

When evaluating your options, consider three questions:

1. How much downtime can your business realistically afford?
2. Do you need strategic IT planning, or just technical support?
3. Is your current setup helping you stay secure, compliant, and competitive?

Choosing the right model isn't about the lowest rate, it's about long-term reliability, partnership, and alignment with your business objectives.

Managed IT vs. Break-Fix: Which Delivers the Better Value?

Benjamin Franklin famously said, "An ounce of prevention is worth a pound of cure." That principle defines the difference between managed IT and break-fix support.

When your operations depend on technology, the true cost of downtime extends far beyond the repair bill. Lost productivity, missed revenue, and potential data risks can multiply quickly, none of which are covered in a reactive break-fix model.

Managed IT flips that dynamic. Instead of waiting for issues to appear, your provider actively prevents them through monitoring, maintenance, and cybersecurity. Their success is tied to yours: fewer disruptions mean better performance and lower long-term costs.

Why Break-Fix Seems Cheaper (But Isn't)

On paper, break-fix appears flexible: you pay only when you need help. In reality, it often results in:

- Unpredictable costs when problems arise.
- Longer downtime because repairs happen after the failure.
- Limited accountability, you pay whether the issue is fully resolved.
- Misaligned incentives, your downtime becomes their billable time.

“Break-fix is like calling the fire department every time your building catches fire instead of installing a sprinkler system.”



Why Managed IT Outperforms Break-Fix

Managed IT delivers stability through prevention and partnership:

- Continuous oversight that detects and resolves issues before they affect your team.
- Predictable pricing that makes IT expenses easier to budget and scale.
- Aligned incentives—your provider succeeds by keeping your systems running smoothly.
- Strategic oversight that turns IT from a cost center into a growth enabler.

When you invest in managed IT, you're not just buying support, you're securing uptime, data protection, and long-term confidence. The key is choosing the level of coverage that matches your operational risk, compliance requirements, and long-term business goals.

The Bottom Line

Break-fix is a reaction. **Managed IT is a strategy.**

When you invest in managed services, you're not just paying for support, you're buying uptime, security, and peace of mind. This proactive mindset, maintaining systems before they fail, is at the core of what separates strong IT partnerships from reactive vendors.

Why Regular Monitoring and Maintenance Are Critical for Today's Networks

Technology evolves constantly and so do the threats targeting it. In today's connected world, continuous monitoring and maintenance aren't optional; they're the foundation of secure, reliable business operations. Every organization, regardless of size or industry, depends on a healthy network to stay productive, compliant, and competitive.

The Reality of Today's Threat Landscape

Cybersecurity incidents are at an all-time high, and small and midsize businesses are now prime targets. Modern cybercriminals operate more like global corporations with budgets, automation, and AI-powered tools that scan millions of networks for weaknesses and craft phishing messages nearly indistinguishable from legitimate emails.

AI isn't just helping defenders, it's making attackers faster and harder to detect. That's why layered security and proactive monitoring are no longer optional, they're essential.

And cybersecurity isn't the only concern. Natural disasters, hardware failures, and even well-intentioned employee errors can all disrupt operations or cause irreversible data loss.

“ Forget the lone hacker stereotype—today's cybercriminals run full-scale businesses with trained teams focused on one goal: taking your money. ”

Why Proactive Maintenance Matters

Regular maintenance and monitoring catch small problems before they turn into major issues. It's similar to maintaining a vehicle: skip the tune-ups, and you'll eventually need a new engine. IT systems work the same way.

Key benefits of ongoing monitoring and maintenance:

- Early detection of vulnerabilities: Finds gaps before they're exploited.
- Consistent performance: Keeps systems running efficiently, extending hardware life.
- Reduced downtime: Fixes issues before they interrupt productivity.
- Compliance support: Ensures updates meet industry regulations and audit standards.
- Peace of mind: Confirms backups, antivirus, and network protections are working.

The Cost of Neglect

Neglecting proactive maintenance might save money in the short term but creates long-term risk. Unpatched systems invite breaches, inconsistent backups make recovery impossible, and aging infrastructure often fails without warning—costing far more to replace in a crisis than through planned lifecycle management.

Downtime doesn't just halt operations; **it erodes trust, damages relationships, and exposes your business** to financial and regulatory consequences.

A Smarter, Preventative Approach

Proactive monitoring and maintenance transform IT from a liability into a strategic advantage. They reduce unexpected costs, strengthen cybersecurity, and give you visibility into your entire technology environment. When IT works seamlessly, your team can focus on growth, innovation, and client service, not constant troubleshooting.

“The question isn't if something will happen — it's when, and how prepared your organization will be when it does.”

WHAT MONITORING LOOKS LIKE IN PRACTICE

Automated alerts detect unusual activity before it affects users.
Regular updates keep security patches and firmware current.
Verified backups ensure data can be fully restored when needed.
Network health reports provide ongoing insight into performance and risk.

Even with proactive monitoring in place, many business leaders still face a key question:

Should IT be managed entirely in-house or is partnering with a dedicated team the smarter move?

Should You Hire a Full-Time IT Manager?

After recognizing how vital proactive IT management has become, many business leaders naturally ask whether hiring a full-time IT manager is the next logical step. It's a fair question and for some organizations, it can make sense. But for most small and midsize businesses, it's rarely the most cost-effective or comprehensive solution.

Why One Person Often Isn't Enough

Modern IT environments cover networking, cybersecurity, compliance, cloud infrastructure, and user support — disciplines that each require specialized skills. Even a highly capable IT professional can only manage part of that scope. And when that single person takes time off or leaves, the organization temporarily loses all of its institutional IT knowledge and coverage.

Hiring full-time also means paying salary, benefits, and training for one resource, while a managed services partner gives you an entire team of experts for roughly the same or less overall cost.

The Skills Gap and Hiring Challenge

Even large organizations struggle to recruit and retain skilled IT professionals. Demand for cybersecurity and cloud expertise continues to outpace supply, and if you're not a technical expert yourself, evaluating a candidate's depth can be difficult. Many businesses hire someone strong in one area, only to discover gaps in others, especially in compliance, security, or strategy.

You might hire an IT person to “handle everything,” only to realize that “everything” takes a team.

When Internal IT Works — and When It Doesn't

For larger, complex, or highly regulated organizations, maintaining an internal IT department can make sense. Even then, most still rely on external specialists for advanced cybersecurity, cloud architecture, or 24/7 monitoring.

For smaller and midsize businesses, outsourcing or co-managed IT provides broader coverage, faster response times, and scalable expertise without the overhead of additional full-time staff.

The Co-Managed IT Option

Co-managed IT blends the best of both worlds. Your internal staff handles day-to-day issues while your managed service provider delivers strategy, advanced security, and around-the-clock monitoring. It's ideal when you need extra bandwidth, compliance validation, or backup coverage during vacations, upgrades, or transitions.



The Bottom Line

Hiring a full-time IT manager gives you one person. Partnering with a managed services provider gives you a team, one that brings consistency, coverage, and accountability across every area of your technology environment.

Even if you maintain an internal IT role, pairing them with a trusted MSP ensures no single person carries the full responsibility for keeping your business secure and operational.

WHEN CO-MANAGED IT MAKES SENSE

- Your internal IT team lacks cybersecurity or compliance depth.
- Projects or upgrades require more capacity than your staff can handle.
- You need external validation for backups, recovery, or security posture.
- You want seamless coverage during vacations or turnover.

What Should You Expect to Pay?

Even with proactive systems in place, many leaders still wonder whether to build or buy IT expertise. Let's look at how those options compare and what they actually cost.

Pricing varies by business size, systems, and security needs but understanding why it varies helps you compare providers fairly and make confident, informed decisions. Your IT costs should always be clear, consistent, and aligned with your business goals.

Why Pricing Varies So Widely

A five-person law firm with one server and a few laptops has very different needs than a 200 person healthcare network with compliance requirements and multiple locations.

The main factors that influence pricing include:

- **Scope of Services:** Basic support vs. full management including cybersecurity, backup, and compliance.
- **Number of Devices and Users:** More endpoints mean more monitoring, patching, and licensing.
- **Complexity of Environment:** Cloud integrations, hybrid setups, and legacy systems increase risk and time.
- **Response Expectations:** 24/7 help desk or on-site response adds staffing and coverage requirements.
- **Security and Compliance:** Industries like healthcare, legal, and finance demand higher protection levels.

The key is to compare what's included, not just the number at the bottom of the proposal.

— “ —
It's not about finding the lowest price. It's about finding the right level of protection, support, and reliability for your business.

Industry Averages and Typical Pricing

The following are [national industry averages](#), compiled from surveys of IT service providers. They're not UV&S pricing, they're provided to help you understand what's common and reasonable across the industry.

Break-Fix (Hourly Support):

- \$150–\$250 per hour, typically with a one-hour minimum.
- Some firms offer discounted blocks of hours, but costs remain unpredictable because support is reactive.

Managed IT Services (Monthly Support):

Most managed service providers (MSPs) charge a monthly rate based on the number of devices or users supported. Typical ranges include:

- Servers: \$150–\$250 per server per month
- Workstations: \$50–\$150 per workstation per month
- Mobile Devices: \$5–\$15 per device per month

These rates generally include remote monitoring, patch management, backups, help desk support, and cybersecurity tools. Inclusions vary by provider, so always compare scope, not just price.

What's (Usually) Not Included

Even “all-inclusive” contracts have limits. That's not necessarily a red flag unless the provider hides them.

Common exclusions include:

- Hardware purchases (servers, PCs, laptops)
- Software licenses or subscriptions
- Major network rebuilds or cloud migrations
- Special projects and upgrades
- Security assessments or penetration testing

Some “all-inclusive” contracts exclude common services but only reveal that in the fine print. Always ask for an itemized list of included services and review the SLA (Service Level Agreement) before signing.

“
An IT manager can fix problems. A managed partner helps you prevent them — and plan for what's next.
”

What **SHOULD** Be Included (Every reputable MSP should provide)

- Weekly or daily security patches for urgent threats
- Antivirus updates and active monitoring
- Firewall updates and monitoring
- Backup monitoring and test restores
- Spam filter installation and updates
- Workstation and server monitoring for performance or failure
- System optimization for speed and reliability
- Network documentation (software, credentials, and licensing)

Project-Based Work

For one-time initiatives, such as Microsoft 365 migrations, new server deployments, or cybersecurity program development, pricing varies widely depending on scope. When hiring a consultant for project work, insist on:

- A detailed scope of work defining success, functionality, and security.
- A fixed budget and timeline to ensure accountability.
- Transparency about exclusions to prevent hidden costs.

16 Questions to Ask Before Hiring an MSP



The following questions will help you evaluate any IT provider and clarify exactly what you're getting for your investment. Some will matter more to you than others, but all are designed to protect your business from hidden costs, poor service, and untested promises. Use these as your guide before you sign anything — and always get the details in writing.

Customer Service

1 When I have an IT problem, how do I get help and how fast?

You should never have to fight through phone trees or wait days for a response.

Our Take:

We provide multiple ways to reach support — phone, email, or online portal — with guaranteed response times around the clock. During business hours, a **live technician** always answers. After business hours, our on-call team responds to all emergencies.

2 Will I have a dedicated account manager?

Consistency matters. A single point of contact ensures proactive communication and a clear understanding of your goals.

Our Take:

Every UV&S client has a dedicated account manager who stays involved from onboarding through ongoing strategy, someone who knows your business, not just your ticket history.

3 Who actually handles my support and how big is your team?

Some providers outsource help desks or rely on a single technician. That's risky when coverage matters.

Our Take:

All UV&S support is **handled in-house** by our U.S.-based engineering team. We document every environment so any technician can step in seamlessly when your primary contact is unavailable.

IT Maintenance and Managed Services

4 Do you offer true managed IT services and what is included?

Real managed IT focuses on prevention, not just repair. It also requires transparency about what's covered.

Our Take:

Ask if your provider monitors systems 24/7, manages patches and backups automatically, and coordinates with other vendors. We clearly define inclusions and exclusions up front, so there are no surprise charges when you need help most.

5 What isn't included in your managed services agreement?

All-inclusive doesn't always mean what it sounds like. Many IT companies exclude key services from their monthly rate and then bill extra for it.

Our Take:

Before signing anything, ask exactly what triggers additional charges.

For example:

- Is your help desk truly unlimited, or will you be billed per call?
- Does the agreement include support for cloud platforms like Microsoft 365?
- Will they coordinate with third parties, your internet provider, phone vendor, or software company?
- Are on-site visits and support for remote offices included?
- If your team suddenly had to work remotely, would support for home PCs be covered or billed separately?
- If your business experienced a ransomware attack, fire, or flood, would recovery and rebuilds be included in your plan or treated as an extra project?

These details separate transparent, professional providers from those who hide fees behind fine print. At UV&S, our agreements spell out what's included, and what's not, so there are no surprises when you need help most.

6 Do you conduct regular technology reviews?

Proactive IT partners don't just fix problems, they help you plan ahead.

Our Take:

Ask how often they meet with clients for business and technology reviews. We hold strategy sessions to review network health, upcoming projects, budgets, and compliance. These aren't technical check-ins; they're business conversations about performance and growth.

— “

The best IT providers don't hide what's not included, they make it clear from the start.

Security & Compliance

7 How do you protect users and devices from security risks?

Security isn't one tool, it's multiple layers working together.

Our Take:

A strong IT partner uses layered security. Ask if they offer:

- Multi-factor authentication
- Advanced endpoint protection
- DNS filtering
- Phishing defense
- User awareness training

“

Cybersecurity isn't a single product. It's a mindset built on layers of protection that work together.

”

8 Who audits your cybersecurity practices — and how often?

Even IT firms need someone watching over their shoulder. No provider should be the only one checking their own security.

Our Take:

Ask who audits their cybersecurity and how often. If they say “we handle that internally,” that's a red flag. Independent audits by a third-party specialist are essential to catch blind spots and validate security controls.

9 Do you have a Security Operations Center (SOC)?

A Security Operations Center (or SOC) monitors your network for suspicious activity 24/7. Not every IT company has one, and that matters.

Our Take:

Ask if your provider operates a SOC in-house or through a trusted partner. What matters most is that it exists, runs continuously, and uses modern detection tools. UV&S partners with a specialized SOC to deliver real-time threat detection and response.

Documentation & Oversight

10 Will you provide and maintain documentation of our network?

Network documentation is like the blueprint of your business technology. It includes hardware, software, configurations, credentials, backups, and security settings. Without it, you're completely dependent on your provider.

Our Take:

Every professional IT firm should maintain and regularly update your network documentation and you should always be able to request a copy.

11 How often are systems monitored and maintained?

Proactive maintenance prevents problems before they happen.

Our Take:

UV&S continuously monitors systems for performance, updates, and potential vulnerabilities. Routine maintenance keeps your network healthy, secure, and compliant.

12 Do you coordinate with third-party vendors?

Your IT partner should take ownership and help you with an issue, not pass the problem along.

Our Take:

We act as a single point of contact, working directly with your software and hardware vendors so your team doesn't get stuck playing middleman.

Backup, Recovery & Continuity

13 How quickly can you restore operations after a disaster?

When disaster strikes, whether it's ransomware, hardware failure, or a flood, every minute of downtime costs money and reputation.

Our Take:

Ask your IT provider to explain their disaster recovery process in detail, including failover (how fast you can get back online) and failback (how long until everything is restored to normal). Your recovery plan should guarantee that critical systems are back within hours, not days. At UV&S, we build each client's disaster recovery strategy around their operations, to ensure continuity.

14 Do you test backups regularly?

A backup that's not tested is just a false sense of security.

Our Take:

Your IT provider should check backups daily and run regular "fire drill" test restores to make sure data can actually be recovered. The worst time to find out your backups don't work is after a disaster. Ask how often they test restores — monthly is a minimum — and which backup framework they follow. We adhere to the 3-2-2 rule: three copies of your data, on two media types, with two off-site or cloud-based backups.

Try This Yourself: Delete three non-essential files from your server — one recent, one from a week ago, and one from a month ago — and ask your IT company to restore them. How fast they respond will tell you everything you need to know.

15 How would you keep my team working remotely if we couldn't access the office?

Disruptions happen; storms, outages, or worse.

Our Take:

Ask how they handled remote transitions during previous disruptions and how quickly they can securely enable remote access for your team. UV&S ensures every client can transition seamlessly to remote work through secure cloud-based tools that protect data and maintain productivity from anywhere.

“Backups are meaningless if you can't restore them quickly when it counts.”

Onboarding & Partnership

16 What's your process for onboarding new clients?

This is the question that reveals whether a provider truly has their act together. A good onboarding process protects your data, ensures a smooth transition, and sets the tone for your partnership.

Our Take:

Ask to see it, not just hear about it. UV&S follows a detailed onboarding plan that securely collects credentials, audits your systems, and coordinates with your previous provider for a seamless transition.

Use these questions in every IT conversation you have. The best firms will welcome them and provide documented, specific answers. If a provider hesitates or gives vague responses, that's a sign they might not be as ready as they appear.

At UV&S Technology, we believe transparency builds trust and trust is the foundation of every long-term partnership.



Common Red Flags and Contract 'Gotchas' to Watch For

Even experienced business leaders can miss warning signs in IT proposals. Use this checklist to spot the traps that turn predictable partnerships into costly surprises.

1. The *All-Inclusive* That Isn't

If you see words like unlimited or all you can eat, read carefully. Many "flat-rate" plans exclude essential services, the ones most likely to cost you extra later.

Ask specifically if the plan covers:

- On-site and remote support
- Cloud platforms like Microsoft 365
- Ransomware recovery and data restoration
- Vendor management
- Hardware installs, upgrades, and migrations

2. Unclear SLAs (Service Level Agreements)

SLAs define how fast your provider responds and resolves issues but some use vague terms like best effort, which really means **whenever we can get to it**.

Look for clarity on:

- Response times by priority level (critical, high, low)
- Uptime measurement and guarantees
- Whether penalties exist for missed SLAs
- Availability outside business hours

3. Hidden Fees and Hourly Traps

A low monthly rate can hide expensive "extras." If you see variable charges for after-hours support or "emergency" calls, you're not getting flat-rate service.

Watch for charges related to:

- Travel or mileage for site visits
- Weekend or after-hours surcharges
- Small tasks outside the defined scope
- Vendor coordination billed as "consulting time"

4. Vague or Missing Cybersecurity Coverage

Security shouldn't be an add-on buried three pages deep.

Ask if the agreement includes:

- Endpoint protection and monitoring
- Regular vulnerability scans
- Employee phishing and awareness training
- Incident response and breach notification procedures



We believe clients should never be penalized for asking for help. Transparent pricing leads to healthier, longer partnerships.

Common Red Flags and Contract 'Gotchas' to Watch For

5. No Documentation or Data Ownership Clarity

It's shocking how often businesses discover their IT company controls all their logins, passwords, and infrastructure information and won't hand it over. You should always own your network credentials.

Ask early:

- Who owns our network documentation?
- Will we receive updated copies?
- Are administrative passwords shared or stored securely under our control?

6. The "Too-Good-to-Be-True" Proposal

If one quote is dramatically cheaper than others, find out why. It usually means corners have been cut — fewer staff, limited hours, or missing security coverage.

7. No Exit Strategy

Contracts should make it easy to leave if you choose to, without undue penalties or data friction. Professional providers help you transition smoothly because they're confident in their service.

Ask to see:

- Termination notice requirements
- Data transition procedures
- Fees for offboarding or documentation transfer

“
The most trustworthy IT providers make it easy to leave — because they're confident you won't want to.

Spotting red flags is only half the equation, the real value comes from partnering with a provider who eliminates them entirely. When pricing is transparent, communication is consistent, and security is built into every layer, IT stops being a question mark and becomes a strategic advantage.

That's the standard we hold ourselves to at UV&S Technology, clear expectations, measurable performance, and a proactive approach that earns long-term trust.

A Smart Next Step: Your Free Cyber Security Assessment

You've seen what reliable IT should look like and what warning signs to avoid.

The next step is simple: see how your own environment measures up.

Our goal is simple: to help you make confident, data-driven decisions about your technology. That starts with a short conversation and a free cybersecurity assessment.

If you're ready to take the next step, [schedule a 10-15 minute consultation](#) with our team. We'll discuss your current setup, answer your questions, and outline exactly what our free assessment includes.

What You'll Learn from Your Assessment

This assessment is conducted 100% remotely, with or without your current IT company's knowledge. After the assessment, we will go over:

- Whether your data and systems are fully protected from ransomware and breaches.
- If your backups can actually be restored quickly after an emergency.
- How you can strengthen security, communication, and team productivity.

Why It's Worth Your Time

Fresh eyes often reveal what's been overlooked. At a minimum, this assessment provides a credible, third-party view of your IT environment with zero risk or obligation.

Whether you're confident in your current setup or not, you'll walk away knowing exactly where you stand and what to do next.

Take 15 Minutes. Gain peace of mind.

Call or email and mention the cyber security assessment.

MSP@uvsinc.com
316-613-4749
UVSTechnology.com





See What Other Businesses Are Saying:



Consistent, Cost-Effective IT Support Tailored to Our Non-Profit Needs

UV&S has provided our organization with much-needed consistency in an ever-changing IT environment, understanding our limitations as a non-profit and effectively prioritizing upgrades. Their personalized service ensures we never feel overlooked, offering more services at a reasonable rate compared to other IT firms. I am confident in recommending UV&S as they have consistently proven to be the best option through our procurement processes, providing pivotal support during our organization's expansion and ensuring minimal disruptions to our operations.

Dani Hallgren
Chief Executive Officer
Konza Prairie Community Health Center



Invaluable Partnership: Expert, Pressure-Free IT Support with UV&S

UV&S has an in-depth understanding of our systems, providing expert advice on necessary changes and updates without sales pressure. They offer reliable support for daily tasks, emergencies, and significant infrastructure updates, making them an invaluable partner. If someone is undecided about choosing UV&S, I would tell them that having a skilled team like UV&S is invaluable for handling tasks beyond your expertise or staffing capacity. They have consistently supported us in daily operations, emergencies, and significant infrastructure updates, making complex projects manageable and ensuring we are never alone in these endeavors.

Keith Flippin
Chief Information Officer/HPSO
GraceMed Health Clinic



Reliable and Responsive IT Support: UV&S as a Trusted Partner

The single biggest benefit to our company since partnering with UVS has been having a trustworthy resource to help resolve IT issues. UV&S stands out from other IT firms we've worked with due to their responsiveness and quick action. For anyone considering UV&S as their IT firm, I would highly recommend them as a valuable addition to their team, offering reliable and expert IT support.

Bill Mannebach
Murfin Drilling Company



Personalized IT Service with Big-Firm Expertise: UV&S Delivers for Our Law Firm

The biggest benefit to our law firm since UV&S took over our technology needs has been the improved level of customer service and expertise we've received. They are extremely proactive when addressing our technology needs. It's even better to know our account manager by name/face and to trust them for all of our IT needs. UV&S has increased the efficiency and stability of our systems. We feel supported and confident in our IT team and overall infrastructure. As a small to medium-sized firm, we wanted the expertise and representation of a big IT company, but with the personal touch of a family-oriented team we could work with year-round. They deliver as an IT company and provide technology business reviews to offer recommendations and to plan for upcoming IT related expenses. They also offer great response times with accessibility to the team. With UV&S, we get the best of both worlds.

Velinda Quintana
Firm Administrator
Penner Lowe Law Group



Unmatched Emergency Response and Trustworthy IT Service with UV&S

Since partnering with UV&S for our technology needs, the single biggest benefit has been their rapid response during emergencies. Whenever we encounter a critical issue with any of our computers, UV&S makes it easy to reach tech support, and they always provide immediate assistance. Compared to other IT firms we've worked with in the past, UV&S stands out in providing top-tier customer service and insight. To anyone on the fence about choosing UV&S as their IT firm, I would say this: Having known the team at UV&S for a very long time, I can attest to their commitment to customer service and their expertise. Every time we've had an urgent need, they have stepped up and jumped in to help. They don't try to scare us into buying more equipment or services than necessary; instead, they focus on making us effective and efficient.

Stacey Richards
Owner
Five Star Mechanical



If You're Hesitating, Don't...

Since enrolling in UV&S's Managed IT Services program, the biggest benefit has been peace of mind. Our systems run smoothly, updates are handled proactively, and downtime has virtually disappeared, allowing our team to focus on growing the business instead of troubleshooting tech issues. What really sets UV&S Technology apart is their responsiveness and personalized support. They take the time to understand our needs, communicate clearly, and act fast. If you're hesitating, don't. Partnering with UV&S has been one of the smartest decisions we've made. They're reliable, knowledgeable, and genuinely invested in our success. You don't just get IT support; you gain a strategic ally.

Cory Fessenden
Chief Information Office
Iron Insurance Partners

Scott, Kansas Masonic Home

Since 2012, UV&S has continually provided first-class IT and data center services for our organization. They have outstanding technical resources and are responsive to our needs. Most recently, their performance during a time of crisis was exceptional. I would highly recommend you call UV&S if you are in need.

Carol Skaff, Cohlmiia Marketing

I appreciate the professionalism of UV&S staff, the processes they have set up to manage our technology needs, and their fast response times. When I need to purchase technology, they are there to advise me, make the purchases for me, and install the equipment. Most of all, I appreciate that my business technology has minimal downtime under the care of UV&S.

Troy Hagerman, Anderson Management

Our backups were manual, inconsistent and far from disaster-proof before we started working with UV&S. They implemented a hybrid backup solution and now our backups are automatic, regular and absolutely disaster-proof. We can always trust that our critical data and processes will be available if and when we need them. We get quick response times to our inquiries/service calls as well as expert service and advice. Most importantly, they provide us with absolute peace of mind. With UV&S handling our IT, we can focus on our core business. We would recommend UV&S to anyone considering IT services, regardless of how large or small your business is.



Why Organizations Trust UV&S for Managed IT Support

We've built long-term partnerships by delivering clear communication, reliable service, and measurable results. Here's what sets us apart:

- **Proven Track Record.** With more than two decades of IT experience, UV&S has earned client trust through consistent uptime, rapid response, and simplified IT management. Our reputation is built on results, not promises.
- **Live Answering, Real Time Support.** We prioritize live answering for every call. No more navigating endless prompts—we ensure you connect with a technician right away. Your time is valuable, and getting the help you need shouldn't be a hassle.
- **Fast, Reliable Response.** Productivity depends on technology that works. We prioritize quick resolutions, with defined response times and critical issues handled first.
- **Customer-Centric Approach.** Exceptional customer service is at the heart of what we do. We build lasting relationships by prioritizing your needs and working with you to achieve your IT objectives. Trust us to find the right technology solution, giving you back valuable time, whether for work or personal life.
- **Transparent Communication.** We keep you informed at every step — clear updates, detailed documentation, and no surprises. We listen to you and learn the business problems you face so we can offer strategies to resolve the root problem.
- **Comprehensive Protection.** From advanced cybersecurity tools to staff training, we safeguard your systems against threats and ensure your data remains secure.
- **Proactive monitoring.** We use tools to actively oversee the IT environment, identifying and resolving potential issues before they become a problem.
- **Compliance assistance.** We can help ensure that IT systems comply with relevant industry regulations and standards.
- **Solutions for You.** Whether you're adding users, locations, or services, our solutions grow with you — seamlessly and securely.
- **Innovative Technology.** We leverage the latest tools and partnerships to keep your infrastructure ahead of evolving business needs.

Technology changes fast. Trust and accountability don't.

That's why businesses continue to rely on UV&S for proactive, secure, and strategic IT partnership.