HUFFDATA
MANAGED IT · CYBERSECURITY · CLOUD

FREE IT BUYER'S GUIDE

The Texas Business Owner's Guide to Managed IT Support Services and Fees

What you should expect to pay for IT support, how IT companies price their services, and what to ask before you sign a contract.

Read this guide to discover:

- ✔ The three most common ways IT companies charge for their services, and the pros and cons of each
- ✔ Why hourly "break-fix" billing puts the risk on you
- ✔ Exclusions, extra fees and contract red flags, such as a provider that says it isn't a cybersecurity company and accepts no responsibility for breaches
- ✔ Five ways lower-priced IT firms hide the true cost of their services
- ✔ Why a salesperson's "good enough" can leave your business exposed
- ✔ How to tell basic IT support from a security-first provider that can stop business email compromise, keep your cyber insurance on track and lead you through an incident
- ✔ 21 questions to ask any IT company before signing an agreement

Provided as an educational resource by
Donovan Huff, President & CTO, HUFF DATA SYSTEMS
101 W Goodwin Ave #1118, Victoria, TX 77901 · Victoria 361-570-7240 · Houston 713-493-2051 · www.huffdata.com

About the author

A native Texan with over 25 years in the IT industry, Donovan Huff leads HUFF DATA SYSTEMS, a managed IT, cybersecurity, and cloud services company serving Texas businesses. An InfraGard member, he provides CTO-level leadership that helps organizations reduce risk, protect business operations, and use technology to support growth.

Never ask an IT company "What do you charge?" Ask "What will I get for my money?" and know what to look for before you sign.

HUFF DATA SYSTEMS at a glance

- ✔ All-in managed IT from $175 to $300 per user per month, including a Microsoft 365 Business Premium license and on-site support
- ✔ Reach a person in under a minute, with urgent issues handled within minutes by our own Texas-based help desk
- ✔ 24/7 security operations center monitoring with a five-minute average response
- ✔ Immutable backups with automated restore testing
- ✔ Governance, risk and compliance built in: risk assessments, security policies, compliance evidence and a written incident response plan for every client
- ✔ CTO-led planning, with direct access to our CTO and quarterly reviews in plain language
- ✔ A free review of your current IT contract or any provider's quote

Compare providers with our scorecard →

Who this guide is for

- ✔ Business owners who have an IT provider but aren't sure they're getting what they pay for
- ✔ Leaders who have been surprised by extra charges, slow response or problems that should have been prevented
- ✔ Companies considering a switch that want the right questions to ask first
- ✔ Organizations with compliance or cyber insurance requirements that aren't sure their IT setup measures up
- ✔ Growing companies, including those with their own IT staff, deciding how much IT to outsource
- ✔ Companies of 50 or more people whose IT and security have outgrown a part-time or one-person setup

Why price alone is the wrong way to compare IT companies

One of the first questions business owners ask an IT company is what it charges. It's a fair question, but choosing a provider on price alone, or even making price a top criterion, often leads to overpaying and to risk you didn't know you were taking on. There are three reasons:

1. **There is no standard pricing in IT services.** Two proposals that look alike can cover very different work, so comparing monthly totals tells you little until you compare what is included.
2. **Low quotes often leave out what protects you.** Lower-priced agreements commonly cut corners on cybersecurity, backup and disaster recovery, the areas where a gap costs the most and is hardest for a non-technical buyer to spot.
3. **Value matters more than price, high or low.** The right provider is the one that fits your situation, budget and risk, and helps you reach your goals.

This guide explains how IT services are priced, where hidden costs and coverage gaps tend to appear, and which questions reveal whether a provider is the right fit.

Basic IT support vs. security-first IT

Most IT providers are built to keep computers running. Far fewer are built to stop modern attacks, prove compliance, keep your cyber insurance on solid ground and lead you through a security incident. Both may call themselves "managed IT," so here is what the difference looks like in practice:

Area	Common with basic IT support	HUFF DATA SYSTEMS
Business email compromise	Spam filtering and antivirus, which can't stop a convincing email that carries no malware	**Impersonation filtering, conditional access and strong MFA, 24/7 monitoring for account takeover, and payment-verification rules**
Security monitoring	Alerts checked during business hours, if anyone checks them	**24/7 security operations center with a five-minute average response**
Cyber insurance	Application answered from memory; controls may not match what you told the insurer	**Application reviewed against the controls actually in place, with dual claims coverage available**
Security incidents	No written plan, so the first hours are spent figuring out who to call	**A written incident response plan for every client**
Governance, risk and compliance	Left to you, or described as out of scope	**Risk assessments, written security policies, vendor risk reviews and compliance evidence for HIPAA, the FTC Safeguards Rule, CIS and NIST**
Backups	Backups that report "success"	**Immutable backups with automated restore testing**

Area	Common with basic IT support	HUFF DATA SYSTEMS
Leadership	A ticket queue	**CTO-led planning with quarterly reviews in plain language**

Want a second opinion? Send us your current IT agreement or another provider's quote, and we'll fill in this comparison for you, free. Request a free contract review →

Basic protection leaves a business exposed in exactly the places attackers and insurers look first. The next two sections explain why.

Why basic protection doesn't stop business email compromise

Business email compromise (BEC) is one of the costliest cybercrimes businesses face: in its 2025 Internet Crime Report, the FBI counted about $3 billion in reported BEC losses, second only to investment fraud. A BEC attack often contains no virus at all. It is a convincing message from a lookalike domain, or from a real mailbox an attacker has taken over, asking someone to change bank details or send a payment. Antivirus and a basic spam filter have nothing to catch.

Stopping BEC takes layers that work together: filtering that flags impersonation and lookalike senders; conditional access and strong multi-factor authentication so a stolen password isn't enough; 24/7 monitoring for suspicious sign-ins, new forwarding rules and other signs of account takeover; trained employees; and written payment-verification rules, such as calling back on a known number and requiring two people to approve wires and bank changes. HUFF DATA SYSTEMS includes all of these. Read more about how to stop payment scams.

Do you have a plan for a security incident?

When an incident happens, the first hours matter. Many policies require prompt notice to your cyber insurer and the use of approved response firms. Texas law sets firm deadlines: affected individuals must be notified within 60 days of determining a breach occurred, and the Texas Attorney General within 30 days when 250 or more Texans are affected. A business without a plan loses time it can't get back.

Every HUFF DATA SYSTEMS client has a written incident response plan that spells out who to call, what to do first, and the insurer and legal notification steps. See our Texas data breach response guide for the details.

Comparing apples to apples: how IT services are priced

Most IT companies use one or more of three service models. Some offer a blend; others offer only one.

Time and materials (hourly, or "break-fix")

You pay an hourly rate for a technician to fix a problem when something breaks. Rates vary by provider and the complexity of the problem, and many providers discount a block of prepaid hours.

The same model is often used for projects such as upgrades, cybersecurity improvements or office moves.

A related model is the value-added reseller (VAR), which sells hardware and software along with installation and configuration. VARs typically serve larger organizations with internal IT departments, and many have moved toward managed services.

Managed IT services

A managed services provider (MSP) acts as your outsourced IT department for a monthly fee. A typical agreement covers:

- Troubleshooting IT problems through a help desk for your employees
- Setting up and supporting computers, laptops and mobile devices for new and existing employees, on-site and remote
- Managing Microsoft 365 or Google Workspace and other business applications
- Securing your network, devices, email and data against attackers and ransomware
- Backing up data and helping recover it after a disaster
- Monitoring and maintaining the health, performance and security of your systems

A good MSP also provides a technology roadmap and budget, helps you meet data protection rules such as HIPAA, the FTC Safeguards Rule and PCI DSS, and makes sure your security meets your cyber insurance requirements. Planned projects are usually priced separately from day-to-day support.

Companies with their own IT staff often choose **co-managed IT**, where the provider supplies security, monitoring, after-hours coverage or specialized skills while the internal team keeps its role. If you go this route, get the split of responsibilities in writing. HUFF DATA SYSTEMS offers co-managed IT alongside fully managed service.

Vendor-supplied support

Many software vendors sell help-desk support for their own products. It's often worth having for critical line-of-business applications, but it is limited to that software. It doesn't cover your network, other applications, cybersecurity or backups.

Managed IT vs. break-fix: which costs less?

Break-fix has real advantages: you only pay when you need help, and there's no long-term contract. For a very small business with simple needs and no sensitive data such as medical records, card numbers or Social Security numbers, it can be the most economical choice.

For a growing business, or one that handles sensitive data, the downsides add up:

1. **Major problems get expensive.** A technician who doesn't know your environment takes longer to diagnose problems, and without preventive maintenance, small issues grow into big ones.

2. **Hourly billing rewards slow work.** When the provider is paid by the hour, there is little incentive to solve problems quickly or permanently.
3. **Prevention gets skipped.** Managed services exist largely to prevent outages and security incidents instead of reacting to them.
4. **Budgeting is guesswork.** Emergency calls are unpredictable and often cost more over a year than a planned monthly fee.
5. **You're not the priority.** Providers generally serve contract clients first, so break-fix clients can wait longer when something breaks.
6. **No one is watching security.** Without ongoing patching, monitoring and backup checks, the risk of a successful attack rises, and the cost of ransomware downtime is usually far higher than owners expect. See what ransomware downtime really costs.

For most businesses with more than a handful of employees, or any business that handles sensitive data, a managed agreement with a predictable monthly budget is the more cost-effective choice. Our comparison of managed IT and break-fix support goes deeper.

What should IT services cost?

Pricing varies widely by region, scope and provider, which is exactly why you should understand how a quote is built before comparing numbers.

- **Hourly support** is usually billed per hour, often with a minimum charge per visit or call, and sometimes discounted for a prepaid block of hours.
- **Projects** vary with scope and complexity. Insist on a detailed scope of work that defines success (performance, workflow, security and access), and on a fixed price and timeline. Be cautious of open-ended hourly estimates that let a provider bill for "unforeseen" work; accurately scoping the job is the provider's responsibility.
- **Managed services** are usually quoted as a monthly fee based on the number of users, devices and locations supported.

As with most services, you tend to get what you pay for. Providers that include serious cybersecurity, compliance support, technology planning and experienced staff generally cost more than those that don't. Paying more doesn't guarantee good service, but if a quote is far below others, ask what it leaves out.

How HUFF DATA SYSTEMS does it

How HUFF DATA SYSTEMS prices managed IT

We use all-in, per-user pricing: typically **$175 to $300 per user per month**. One predictable monthly fee covers the services below, so you aren't billed by the hour for everyday support or charged extra when someone needs to visit your office.

Every user includes:

- A Microsoft 365 Business Premium license
- Unlimited help-desk support by phone and remote session, with no hourly charges or ticket limits
- On-site support
- Cybersecurity: endpoint detection and response monitored 24/7 by a security operations center (SOC), email security, multi-factor authentication and Microsoft 365 security management
- Backups of servers, computers and Microsoft 365 email, OneDrive, SharePoint and Teams, with restore testing
- Security awareness training and phishing tests for employees
- Network and firewall management, monitoring and patching
- Setup for new employees and devices, and offboarding when people leave
- Vendor management with your internet provider, phone vendor, printers and line-of-business software vendors
- CTO-level planning: regular strategy meetings, a technology roadmap and an IT budget

After-hours work is billed unless it is scheduled work that is part of your included services. Security incident response, projects (such as migrations, office moves or new locations), hardware and a one-time onboarding fee are also billed separately. A three-year agreement offers the best value and a reduced onboarding fee.

Because Microsoft 365 Business Premium is included, compare our price with other quotes *plus* the cost of your Microsoft 365 licenses. Where your business falls in the range depends on what you need protected and managed, such as your security and compliance requirements, your backup and recovery needs, and the number of locations and systems we support. You'll see the exact price and what it covers in writing before you sign.

When a security incident happens: cyber insurance that works with us

We get every client ready for cyber insurance, starting with a review of your insurance application against the controls actually in place, so your answers hold up if you ever file a claim. HUFF DATA SYSTEMS clients can also apply for a cyber liability policy through our insurance partner's program, which is built around dual claims coverage.

What dual claims coverage means: usually, a business and its IT provider are insured by different carriers. After a breach, each insurer may try to show the other side is responsible, and the business can be caught in the middle while its claim is delayed. In a dual claims program, your policy and your IT provider's coverage sit within the same program and work in tandem. That is designed to remove the conflict, speed up the claims process and, where the policy allows your IT provider to respond, let recovery start right away instead of waiting for an outside response team.

Security incident response is billed separately, but for clients covered under the program, those invoices and related covered losses are typically submitted under the policy. Coverage, eligibility and pricing are always subject to the insurer's underwriting and policy terms. Learn more about cyber liability insurance for our clients.

Our response times

- **Getting through:** for more than 25 years, clients who call for support have reached us in under a minute, and urgent issues have an instant support option.
- **Urgent issues are handled within minutes.** Urgent means anything that stops people from working, outages and other incidents, and security incidents.
- **Security incidents:** our 24/7 security operations center averages a five-minute response. It is staffed by security experts, including former military cyber professionals, and is independently audited under the AICPA SOC 2 framework.
- **Moves, adds and changes,** such as new users, equipment moves and permission changes, are scheduled through our normal support queue within one to two business days.

5 ways lower-priced IT firms hide the true cost of their services

Unless you're technical, it's hard to tell whether a quote is insufficient, overpriced or simply incomplete. These are the items most often left out of low quotes:

1. **Inadequate cybersecurity and compliance protection.** Basic antivirus is no longer enough. Cyber insurers now commonly expect multi-factor authentication, endpoint detection and response, and security awareness training before they'll provide coverage. Ask exactly which security tools and services are included, and who watches the alerts.
2. **Inadequate backup and disaster recovery.** Make sure servers, workstations and cloud applications such as Microsoft 365 are backed up daily. Cloud services keep your data available, but their recycle bins are not long-term backups; deleted SharePoint and OneDrive items, for example, are kept for 93 days. At least one backup copy should be immutable, and many insurers now ask about that.
3. **Extra charges for on-site and after-hours support.** Ask whether on-site visits and after-hours work are included or billed separately. This surprises many business owners after they sign. HUFF DATA SYSTEMS includes on-site support in its managed IT agreements.
4. **No vendor coordination.** Some providers bill hourly to deal with your internet provider, phone system, printers, cameras or software vendors. Ask what's included.
5. **Inexperienced staff and no account management.** Lower-cost providers may rely on junior or contract technicians and have no one assigned to plan with you. Good account management includes an IT budget, a roadmap, and regular reviews of security and compliance. See [why technician skill matters].

Why technician skill matters as much as price

Many IT providers staff their help desks with technicians who have little experience in business environments and little training in cybersecurity or compliance. The risk isn't only slow fixes. A technician under pressure to close tickets will often choose what is fast and easy over what is secure: leaving default settings and passwords in place, giving users administrator rights, opening

remote access or firewall rules "temporarily," or turning off a security control that gets in the way. Each shortcut can be the opening an attacker needs, and the difference between an attack that is stopped and one that succeeds.

This isn't hypothetical. When NSA and CISA red and blue teams listed the ten most common cybersecurity misconfigurations they find in large organizations, number one was default configurations of software and applications, followed by improper separation of user and administrator privileges. Weak or misconfigured multi-factor authentication and poor credential hygiene made the list too.

Ask any provider you're considering:

- Who will actually work on our systems, and what business and cybersecurity experience do they have?
- Which security standards do you configure to, such as CIS or NIST, and how do you document changes?
- Who reviews changes to firewalls, administrator accounts and remote access before they're made?
- How do you keep technicians trained on security and compliance?

HUFF DATA SYSTEMS takes a CTO-led approach: security decisions get leadership-level oversight instead of being left to whoever picks up the ticket, and our work is grounded in recognized frameworks such as CIS and NIST, so systems are configured to stop attacks, not just to close tickets.

Watch out for "good enough": who is selling you IT?

Many managed IT contracts are sold by salespeople, not engineers. A salesperson may describe a lower-priced plan as "good enough," "fine" or "the same as what you have now" without understanding cybersecurity, or what a gap could cost your business. The difference rarely shows up in the proposal. It shows up later, when it is most expensive.

What "good enough" can end up costing:

- **Lost cash flow.** When systems are down, the business can't invoice, ship, schedule or serve customers, and the losses add up by the hour. See what ransomware downtime really costs.
- **Fines and legal costs.** Regulated data that isn't protected the way HIPAA, the FTC Safeguards Rule or Texas breach law requires can bring penalties, notification costs and lawsuits. See our Texas data breach response guide.
- **A cyber insurance problem.** If the controls on your insurance application aren't really in place, a claim can be challenged, or coverage can be harder to get at renewal. See how to avoid a denied claim.
- **Pressure to pay criminals.** When ransomware encrypts systems and the backups weren't protected, businesses can be pushed toward paying a ransom to recover their data. The FBI

does not support paying a ransom, and paying doesn't guarantee you'll get your data back.

Before you sign, ask the person selling the contract:

- Who designed this proposal, and can I talk with them?
- Exactly what is different between this plan and our current one, or a higher-priced option?
- Which security controls does our cyber insurance require, and does this plan include every one of them?
- If ransomware hit tomorrow, how would we recover, and how long would it take?
- Which compliance requirements apply to us, and how does this plan help us meet them?

HUFF DATA SYSTEMS takes a CTO-led approach: our recommendations start from your risks, your cyber insurance requirements and your compliance obligations, and we explain what is needed and why in plain language before you sign. Our free IT contract and quote review applies the same lens to any proposal you're considering.

What your service agreement should spell out

It's easy for one provider to look less expensive than another until you read what you're actually getting. Your agreement should clearly define:

- ✔ The services provided, in plain terms
- ✔ Response times for minor and major problems
- ✔ Which services cost extra, such as on-site visits, after-hours work and projects
- ✔ Contract length and renewal terms
- ✔ How you can end the agreement if services aren't delivered as promised
- ✔ Liability limits and protections for both parties
- ✔ Payment terms

Pay special attention to the limitation of liability and to which security responsibilities stay with you. Our article on what your MSP contract really says explains what to look for.

Contract red flags that should give you pause

The sales pitch says what a provider will do. The master services agreement says what it is responsible for, and the two are often very different. Read the contract for these terms before you sign:

- **"We are not a cybersecurity company."** Some providers state outright that security is outside their scope, or sell it only as an optional add-on. If the company managing your systems disclaims security, no one is responsible for protecting them.
- **No responsibility for breaches, ransomware or data loss.** Many agreements exclude security incidents, "events beyond our control" and lost data, even though the provider holds administrator access to everything you run.

- **A liability cap of a few months of fees.** If something goes wrong, the most you can recover may be a small fraction of what an incident actually costs, and lost profits and downtime are often excluded entirely.
- **Nothing about your cyber insurance.** The provider disclaims responsibility for breaches but never asks whether you carry cyber insurance, or whether the controls on your application are really in place.
- **Your insurance pays first, and you cover their costs.** Some agreements require your policy to respond before theirs and make you indemnify the provider for claims tied to your environment.
- **Declined recommendations used to shift blame.** A signed form showing you turned down a security control can put the entire loss on you after an incident.
- **Compliance left entirely to you,** with no help meeting HIPAA, the FTC Safeguards Rule or your insurer's requirements.
- **No incident response plan and no notification commitment,** so no one has agreed how fast you will be told about an incident or what happens next.

Why this combination is so dangerous

Each term may look reasonable on its own. Together they create a gap no one owns: the provider controls your systems but says security isn't its job, accepts no responsibility for a breach, caps what it would pay at a few months of fees, and never confirms you have cyber insurance. When ransomware or a business email compromise hits, your business pays for all of it: incident response, recovery, downtime and lost revenue, customer notification, legal costs and possible fines, often with pressure to pay criminals to get data back. If you do have a policy but your application answers don't match the controls in place, the claim can be challenged too.

Close the gap before you sign:

1. Ask the provider to state in writing which security responsibilities it owns, which stay with you and which are shared.
2. Carry cyber insurance, and have someone compare your application answers with the controls actually in place.
3. Make sure the contract, your security controls and your insurance policy all agree on who does what.
4. Have your attorney review the limitation of liability, indemnification and security exclusions.

HUFF DATA SYSTEMS is built to close that gap: security-first managed IT with a 24/7 security operations center, a written incident response plan for every client, and a review of every client's cyber insurance application. Clients can also apply for coverage through our partner's dual claims program, where your policy and ours work in tandem instead of against each other. Our article on what your MSP contract really says goes deeper, and our free IT contract and quote review will show you where your current agreement stands.

Compare providers: a scorecard to take to every meeting

Fill in the blank columns as you talk with other IT providers. The PDF version prints cleanly for meetings.

Question	HUFF DATA SYSTEMS	Provider A	Provider B
Monthly price per user, and what it includes	$175 to $300, all-in		
Microsoft 365 licenses included?	Yes, Business Premium		
On-site support included?	Yes		
After-hours support	Billed, unless scheduled and part of included services		
Time to reach a person	Under a minute		
Response to urgent issues	Within minutes		
Who answers the help desk?	Our own Texas-based staff		
24/7 security operations center?	Yes, SOC 2 audited, five-minute average response		
Immutable backups?	Yes, for every client		
Restore testing	Automated, built into the backup platform		
Security training and phishing tests	Included		
Business email compromise protection	Impersonation filtering, conditional access, 24/7 account-takeover monitoring, payment-verification rules		
Written incident response plan	Yes, for every client		
Risk assessments, security policies and compliance evidence	Included		
CTO-level planning and budget	Included, with direct access to our CTO		
Regular reviews and reporting	Quarterly reviews in scheduled meetings; detailed reports on request		
Cyber insurance application review	Yes, for every client		
Compliance support	HIPAA, FTC Safeguards Rule, CIS and NIST		

Question	HUFF DATA SYSTEMS	Provider A	Provider B
Co-managed option for in-house IT	Yes		
Onboarding fee	One-time; reduced with a three-year agreement		
Service promise	Make-it-right promise		

Want a second opinion? Send us your current IT agreement or another provider's quote, and we'll fill in this comparison for you, free. Request a free contract review →

21 questions to ask before you sign

Some of these will matter more to you than others. For the ones that matter most, such as response times, insurance, cybersecurity and compliance, get the answers in writing.

CUSTOMER SERVICE

1. How do you request support?

Ask exactly how employees get help: phone, email, a portal or all three. If support requires a ticket from a computer, ask what happens when the internet is down or the laptop won't start. Make sure there is a way to reach a person for urgent problems.

> **How HUFF DATA SYSTEMS answers:** Call us. For more than 25 years, clients have reached a person in under a minute, and urgent issues have an instant support option.

2. Is there a written response time for support requests?

Slow callbacks are one of the most common complaints about IT providers. Ask for response targets in writing for urgent, high and normal requests, including after hours, and ask how the provider reports on whether it meets them. See our response times for how HUFF DATA SYSTEMS answers this.

3. Do they explain things in plain language?

Your team should be able to ask simple questions without being made to feel foolish. Pay attention to how the provider explains things during the sales process; it is usually how they will explain things after you sign.

> **How HUFF DATA SYSTEMS answers:** Most clients don't want to manage the technical details, and they shouldn't have to. We explain what is needed and why in plain language, then take care of it with our CTO-led approach.

4. Do they build an IT roadmap and budget, and review it with you regularly?

Ask whether you will meet regularly, at least quarterly, to review risks, aging equipment, security, compliance and upcoming projects, and whether you will get a written roadmap and budget. Help-desk support alone is not technology planning.

> **How HUFF DATA SYSTEMS answers:** Yes. Strategy meetings, a technology roadmap and an IT budget are included, with direct meetings with our CTO whenever you request them or the situation requires it.

5. Are invoices clear and accurate?

Ask to see a sample invoice. You should be able to tell what you are paying for, what work was done and why, and which charges are recurring versus one-time.

6. Do they carry insurance that protects you?

Your IT provider has administrative access to your systems and data. Ask whether they carry errors and omissions (professional liability) and cyber liability insurance, and ask for a certificate of insurance.

> **How HUFF DATA SYSTEMS answers:** Through our cyber insurance partner's program, our coverage and yours can work in tandem under dual claims coverage. See how it works.

7. Who is your day-to-day contact, and who is accountable for your account?

Ask who you call for help, who reviews your environment and plans with you, and who is responsible when something goes wrong. Get names, not just a department.

> **How HUFF DATA SYSTEMS answers:** Our CTO-led approach means you aren't left to figure out IT decisions on your own: you have direct access to our CTO for planning.

CYBERSECURITY AND COMPLIANCE

8. Can they help you meet the security rules that apply to your business?

Many businesses have specific obligations: the FTC Safeguards Rule for non-bank financial businesses such as tax preparers, mortgage brokers and many auto dealers, HIPAA for healthcare, PCI DSS for card payments, and Texas breach notification law for nearly everyone. Ask which ones the provider has supported and how, and remember that no provider can make you compliant without your participation.

> **How HUFF DATA SYSTEMS answers:** We help clients meet HIPAA, the FTC Safeguards Rule and the CIS and NIST frameworks with risk assessments, written security policies, vendor risk reviews and the compliance evidence auditors, regulators and insurers ask for.

9. Will you get regular reports showing your systems are patched and protected?

Ask for a sample report. It should show patch status, security alerts, backup results and which devices are protected, so you can see the work is being done instead of assuming it.

> **How HUFF DATA SYSTEMS answers:** Yes. We review your security, patching and backup status with you in scheduled quarterly meetings, in plain language: what matters, what is needed and why. Detailed reports are available any time you want them.

10. Will you receive written documentation of your network, or do they keep the keys to the kingdom?

Your business should own its domain, Microsoft 365 tenant, licenses and administrator credentials, and have current documentation of its hardware, software and network. If only the provider knows how things are set up, you are dependent on them.

> **How HUFF DATA SYSTEMS answers:** Yes. Network documentation and your administrator credentials are provided whenever you ask, and when the relationship ends.

11. Does the leadership team understand the regulations in your industry?

Ask about specific experience with HIPAA, the FTC Safeguards Rule, PCI DSS or other requirements that apply to you, and how they document the controls they manage. Our Texas cybersecurity compliance guide covers the common ones.

> **How HUFF DATA SYSTEMS answers:** Yes. Governance, risk and compliance is part of our CTO-led approach, not an add-on; see basic IT support vs. security-first IT.

12. Have they reviewed your cyber insurance application?

Cyber insurers ask detailed questions about MFA, endpoint protection, backups and training, and they rely on your answers. If your controls don't match your application, a claim can be challenged. Ask whether the provider will review your application against what is actually in place. See how to avoid a denied cyber insurance claim.

> **How HUFF DATA SYSTEMS answers:** Yes, for every client. We review your cyber insurance application against the controls actually in place.

BACKUP AND DISASTER RECOVERY

13. Do they insist on backups that attackers can't change or delete?

Ransomware groups routinely target backups. Ask whether at least one copy of your data is immutable or offline, so it can't be encrypted or deleted even with stolen administrator credentials. Many cyber insurers now ask about this too.

> **How HUFF DATA SYSTEMS answers:** Yes. Every client has immutable backups.

14. Do they test restores on a schedule?

A backup that reports "success" is not proof you can recover. Ask how often they restore files and full systems as a test, and ask to see the results. See how to know you can get your data back.

> **How HUFF DATA SYSTEMS answers:** Backups are verified with automated restore testing built into our backup platform.

15. Do they back up systems before projects and upgrades?

Before a server upgrade, migration or major change, a fresh, verified backup should be standard practice so a failed change can be rolled back.

16. Is there a written plan for recovering from a major disaster?

If your office flooded or ransomware hit tonight, how would you get back to work, and how long would it take? Ask for a written recovery plan that names what gets restored first, where, and by whom.

> **How HUFF DATA SYSTEMS answers:** Every client has a written incident response plan, and immutable backups with automated restore testing support a fast recovery.

TECHNICAL EXPERTISE AND SERVICE

17. Who answers the help desk?

Ask whether support is provided by the company's own staff or outsourced to a third party, and where the people who access your systems are located.

> **How HUFF DATA SYSTEMS answers:** Our own staff, based in Texas.

18. Do their technicians keep current certifications and training?

Technology and threats change constantly. Ask how the team keeps its skills current and who handles complex problems when the first person can't solve them.

19. Do their technicians conduct themselves professionally?

Technicians will be in your office and talking with your staff. Ask how the provider sets expectations for communication, courtesy and follow-through.

20. Will they work with your line-of-business software vendors?

Ask whether the provider will act as the liaison with your accounting, ERP, practice-management or other critical software vendors, or whether your staff will be left to sort out problems between them.

> **How HUFF DATA SYSTEMS answers:** Yes. Working with your line-of-business software vendors is included.

21. When the internet, phones or printers fail, do they own the problem?

Ask whether the provider will coordinate with your internet provider, phone vendor and other suppliers, and whether that is included or billed hourly. "That's not our problem" is costly when your business is down.

> **How HUFF DATA SYSTEMS answers:** Yes. Coordinating with your internet provider, phone vendor and printers is part of your agreement.

How HUFF DATA SYSTEMS can help

HUFF DATA SYSTEMS has supported Texas businesses since 2001. From our headquarters in Victoria and across the Houston area, we provide managed IT, cybersecurity, Microsoft 365 management, business continuity and CTO-level technology leadership, led by Donovan Huff, President & CTO.

Three ways to see how your current IT measures up, at no cost:

1. **A free IT contract and quote review.** Send us your current IT agreement or another provider's quote, and we'll show you what is covered, what isn't and where the risk sits.
2. **A cyber insurance application review.** We'll compare your application answers with the controls actually in place.
3. **A complimentary business technology assessment** that shows:

- ✔ Whether your systems and data are protected from attackers and ransomware, and where you're exposed
- ✔ Whether your data is backed up in a way you can actually recover from quickly
- ✔ Where your security may fall short of compliance or cyber insurance requirements
- ✔ How to get more from your IT investment in security, performance and productivity

Our make-it-right promise: if an issue covered by your agreement isn't resolved to your satisfaction, we keep working on it at no extra charge.

Our managed IT agreements include on-site support and a Microsoft 365 Business Premium license for every user, and a three-year agreement comes with a reduced onboarding fee. Call Victoria at 361-570-7240, Houston at 713-493-2051, or choose a time online.

What our clients say

“From risk assessments to advanced threat detection, they know exactly what it takes to safeguard a business in today’s digital landscape. Highly recommended for any company looking for top-tier cybersecurity solutions!”

Google review

“They helped us with our IT and cybersecurity; HIGHLY RECOMMEND THEM”

Google review

“Very knowledgeable when it comes to all things cybersecurity”

Google review

“These guys not only know their stuff, they actually take cybersecurity seriously. I finally feel like I have real professionals on my side.”

Jeff MANAGER

“Every time we’ve had an issue, a senior tech steps in, understands the problem immediately, and resolves it right the first time.”

John CEO

“We thought all IT support was the same, but these guys proved otherwise with smarter tools and real results.”

Brian SALES MANAGER

This guide is general information to help you evaluate IT providers. It is not legal advice; have your attorney review any contract before you sign.

Next steps

Three ways to see how your current IT measures up, at no cost:

1. **A free IT contract and quote review.** Send us your current IT agreement or another provider's quote.
2. **A cyber insurance application review.** We compare your answers with the controls actually in place.
3. **A complimentary business technology assessment** of your support, security, Microsoft 365 and backups.

Scan to get started

www.huffdata.com/contact/

Victoria: 361-570-7240
Houston: 713-493-2051

HUFF DATA SYSTEMS · 101 W Goodwin Ave #1118, Victoria, TX 77901

Managed IT and cybersecurity for businesses within about 60 miles of Victoria and Houston, Texas, since 2001.