WHAT EVERY BUSINESS OWNER MUST-KNOW ABOUT HIRING AN

HONEST, COMPETENT, RESPONSIVE, AND FAIRLY PRICED IT & CYBERSECURITY SERVICES FIRM

Xact IT Solutions
Grow To Your Next Level

COURTESY OF XACT IT SOLUTIONS INC.

This Business Advisory Guide Will Arm You With 21 Critical Questions You Should Ask Any IT or Cybersecurity Company Before Giving Them Access To Your IT Systems

WWW.XITX.COM

READ THIS GUIDE AND YOU'LL DISCOVER:

- The "dirty little secret" of the IT support industry that most people don't know and will never be told by their IT guy (this will surprise you).
- 21 revealing questions that will help you instantly spot an unethical or grossly incompetent IT support technician in minutes.
- 4 costly misconceptions most business owners have about IT services – and what you need to consider when selecting an IT firm.
- Hackers, ransomware and data theft: what you REALLY need to know to protect yourself from a costly, devastating ransomware attack.

Xact IT Solutions
Grow To Your Next Level

PROVIDED AS AN EDUCATIONAL SERVICE BY:

BRYAN HORNUNG- CEO

XACT I.T. SOLUTIONS INC.

HTTPS://WWW.XITX.COM/

856-282-4100

AN OPEN LETTER TO ALL BUSINESS OWNERS AND LEADERS WHO OUTSOURCE IT SUPPORT

From: Cybersecurity Expert and CEO of Xact I.T., Bryan Hornung

Dear Fellow Business Owner or Executive,

Choosing the right IT company is a daunting task. Pick the wrong one and you could end up locked into a contract where frustrations and costs mount as you get hammered with constant IT problems and horrible service.

Pick the right one and you'll breathe a sigh of relief as your IT problems disappear and you gain complete peace of mind that your data and company are protected. Problem is, they all sound good and promise to be proactive, responsive and professional, but how can you really know who the good guys are until you sign a contract and turn over the "keys" to your company's network?

You can't, and that's why we wrote this executive guide. We want to help business owners avoid the frustration and losses that can result in hiring the wrong IT firm by asking the right questions and knowing what to look for in advance. There are signs, but you have to know what to look for.

Sadly, there's no shortage of horror stories about incompetent IT "gurus" bungling jobs and causing MORE problems as a result of their gross incompetence, lack of qualified staff and poor cyber security skills. I'm sure if you talk to your friends and colleagues you will get an earful of the unfortunate experiences they have encountered in this area.

Part of the problem is that the IT services industry is not regulated like most other professions, which means ANYONE can claim they are an "IT expert." This means you, the consumer, must be far more diligent about who you choose to do IT support and arm yourself with the information contained in this report.

From misleading information and unqualified technicians to poor management and terrible customer service, we've seen it all... and we know they exist in abundance because we have had a number of customers come to us to clean up the disasters they have caused.

The information in this guide is provided to help raise standards within the IT support industry and to give YOU useful information to help you guard against the lack of ethics or incompetence of some IT companies and technicians.

Dedicated to securing your assets,

Bryan M Hornung

ABOUT THE AUTHOR

Bryan is the CEO of Xact IT Solutions, an award-winning certified firm, and has earned the coveted CompTIA Security+ Trustmark Certification. He is a recognized cyber security expert featured in CNN, Fox Business, Fox News, Fortune Magazine, Forbes, and many others.

Bryan is the author of the Checkmate book. This cyber security book presents the critical information you need today to protect your business, your assets and your livelihood from cybercrime! Bryan also has co-authored two bestselling cybersecurity books, Under Attack and Adapt & Overcome. Under Attack helps businesses with the challenge of securing data and systems and provides practical advice to help companies identify risk and the best way to address it. Adapt & Overcome similarly helps businesses but looks at the current cybersecurity landscape related to the challenges brought on by the COVID-19 pandemic and remote work. Bryan built a strong reputation developing software for the U.S Navy and currently heads up a top cyber security firm. Bryan uses his experience to help others make rock-solid cyber security programs that keep hackers away, move the business forward, and keep you out of reputation-shattering headlines.

His business is one of only 35 other firms that has earned the CompTIA Security+ Trustmark Certification. Earning the Security Trustmark+ demonstrates a genuine commitment to address the challenges of security compliance facing our industry today. He has worked with hundreds of firms, including the U.S. Navy, Northrup Grumman, and BET365.
He was a featured panelist with executives from Zoom & Upwork at the Running Remote Conference. He hosts a weekly cyber security Podcast, “Security Squawk,” and has over 1500 followers on his YouTube channel.

21 QUESTIONS YOU SHOULD ASK YOUR IT SERVICES COMPANY OR CONSULTANT BEFORE HIRING THEM FOR IT SUPPORT

CUSTOMER SERVICE:

Q1: WHEN I HAVE AN IT PROBLEM, HOW DO I GET SUPPORT?

OUR ANSWER: When a client has a problem, we log the issue in our IT management system so we can properly assign, track, prioritize, document and resolve client issues. However, some IT firms force you to log in to submit a ticket and won't allow you to call or e-mail them. This is for THEIR convenience, not yours. Trust me, this will become a giant inconvenience and thorn in your side. While a portal is a good option, it should never be your ONLY option for requesting support.

Also, make sure they HAVE a reliable system in place to keep track of client "tickets" and requests. If they don't, I can practically guarantee your requests will sometimes get overlooked, skipped and forgotten.

Requesting support should also be EASY for you. So be sure to ask how you can submit a problem to their support desk for resolution. We make it easy. Calling, e-mailing, or submitting a ticket via our portal puts your IT issue on the fast track to getting resolved.

Q2: DO YOU OFFER AFTER-HOURS SUPPORT, AND IF SO, WHAT IS THE GUARANTEED RESPONSE TIME?

OUR ANSWER: Any good IT company will answer their phones LIVE (not voice mail or phone trees) and respond from 8:00 a.m. to 5:00 p.m. every weekday. But many CEOs and executives work outside normal "9 to 5" hours and need IT support both nights and weekends. Not only can you reach our after-hours support any time and any day, we GUARANTEE a response time of one hour or less for normal problems, and within 30 minutes for problems marked "emergency," such as a network being down or a critical problem that is significantly impacting your ability to work.

Q3: DO YOU HAVE A WRITTEN, GUARANTEED RESPONSE TIME FOR WORKING ON RESOLVING YOUR PROBLEMS?

OUR ANSWER: Most IT firms offer a 60-minute or 30-minute response time to your call during normal business hours. Be very wary of someone who doesn't have a guaranteed response time IN WRITING – that's a sign they are too disorganized, understaffed or overwhelmed to handle your request. Our written, guaranteed response time is two hours or less at worst, in some cases, it's 15 minutes but usually less than that. We track this stuff, and a good IT firm should also be able to show you statistics from their professional services automation software, where all client service requests get responded to and tracked. Ask to see a report on average ticket response and resolution times.

Q4: WILL I BE GIVEN A DEDICATED ACCOUNT MANAGER?

OUR ANSWER: Smaller firms may not offer this due to staff limitations, and the owner may tell you they will personally manage your account. While that sounds like great customer service, the owner is usually so busy that you'll only be given reactive support instead of proactive account management. Rest assured, from initial call to final resolution, you will work with our SAME dedicated account manager who will know you, your business, and your goals.

Q5: DO YOU HAVE A FEEDBACK SYSTEM IN PLACE FOR YOUR CLIENTS TO PROVIDE "THUMBS UP" OR "THUMBS DOWN" RATINGS ON YOUR SERVICE? IF SO, CAN I SEE THOSE REPORTS?

OUR ANSWER: If they don't have this type of feedback system, they may be hiding their lousy customer service results. If they DO have one, ask to see the actual scores and reporting. That will tell you a lot about the quality of service they are providing. We are very proud of our positive client feedback scores and will be happy to show them to you (they're actually right on our Web site).

IT MAINTENANCE (MANAGED SERVICES):

Q6: DO YOU OFFER TRUE MANAGED IT SERVICES AND SUPPORT?

OUR ANSWER: You want to find an IT company that will proactively monitor for problems and perform routine maintenance on your IT systems. If they don't have the ability to do this, or they don't offer it, we strongly recommend you look somewhere else. Our remote network monitoring system watches over your network to constantly look for developing problems, security issues and other problems so we can address them BEFORE they turn into bigger problems.

Q7: WHAT IS NOT INCLUDED IN YOUR MANAGED SERVICES AGREEMENT?

OUR ANSWER: Another "gotcha" many IT companies fail to explain is what is NOT included in your monthly managed services agreement that will trigger an invoice. Their so-called "all you can eat" option is RARELY true – there are limitations to what's included and you want to know what they are BEFORE you sign.

It's very common for projects to not be included, like a server upgrade, moving offices, adding new employees and, of course, the software and hardware you need to purchase.

But here's a question you need to ask: If you were hit with a costly ransomware attack, would the recovery be EXTRA or included in your contract? Recovering from a cyber-attack could take HOURS of high-level IT expertise. Who is going to eat that bill? Be sure you're clear on this before you sign, because surprising you with a big, fat bill is totally and completely unacceptable.

Other things to inquire about are:
Do you offer truly unlimited remote help desk? (Make sure you are not nickel-and-dimed for every call.)
Does the service include support for cloud service licenses such as Microsoft 365?
Do you charge extra if you have to resolve a problem with a line-of-business application, Internet service provider, phone system, leased printer, etc.? (What you want is an IT company that will own the problems and not point fingers. We are happy to call the vendor or software company on your behalf.)
What about on-site support calls? Or support to remote offices? How are they handled?
If our employees had to work remote (due to a shutdown, natural disaster, etc.), would you provide support on their home PCs or would that trigger a bill?
If we were to get ransomed or experience some other disaster (fire, flood, theft, tornado, hurricane, etc.), would rebuilding the network be included in the service plan or considered an extra project we would have to pay for? (Get this IN WRITING. Recovering from such a disaster could take hundreds of hours of time for your IT company's techs, so you want to know in advance how a situation like this will be handled before it happens.)

Our managed services agreement is completely transparent and cover everything you need to drive your business forward and remain secure in face of massive cyber-attacks.

Q8: IS YOUR HELP DESK LOCAL OR OUTSOURCED?

OUR ANSWER: Outsourced helpdesk can be frustrating if not the I.T. provider cannot manage it correctly and your I.T. documentation isn't up to par. Poor I.T. operations shine through no matter if the helpdesk is performed locally or if it is outsourced. You certainly don't want the same problems cropping up over and over, longer resolution times, and you having to spend time educating the tech on your account.

Fortunately, we've mastered the help desk function in our company. All of our technicians know you and your company, as well as your preferences and history. When you work with our help desk technicians, they'll be more capable of successfully resolving your IT issues and handling things the way you want.

Q9: HOW MANY ENGINEERS DO YOU HAVE ON STAFF?

OUR ANSWER: Be careful about hiring small, one-person IT firms that only have one or two techs or that outsource this critical role. Everyone gets sick, has emergencies, goes on vacation, or takes a few days off from time to time. We have more than enough full-time techs on staff to cover in case one is unable to work.

ALSO: Ask how they will document fixes, changes, credentials for you organization so if one tech is out or unavailable, another can step in and know your network settings, history, previous issues, etc., and how those issues were resolved. This is important or you'll be constantly frustrated with techs who are starting over to resolve a known issue or may screw up something because they don't understand or have a blueprint of your computer network.

Q10: DO YOU OFFER DOCUMENTATION OF OUR NETWORK AS PART OF THE PLAN, AND HOW DOES THAT WORK?

OUR ANSWER: Network documentation is exactly what it sounds like: the practice of maintaining detailed technical records about the assets you own (computers, devices, software, directory structure, user profiles, passwords, etc.) and how your network is set up, backed up and secured. Every IT company should provide this to you in both written (paper) and electronic form at no additional cost and update it on a quarterly basis.

Why is this important? There are several reasons:

First, it shows professionalism and integrity in protecting YOU. No IT person or company should be the only holder of the keys to the kingdom. Because we document your network assets and passwords, you have a blueprint you can give to another IT person or company to take over if necessary.

Second, good documentation allows the engineers working on your account to resolve problems faster because they don't waste time fumbling their way around your network trying to find things and uncover accounts, hardware, software licenses, etc. Third, if you had to restore your network after a disaster, you'd have the blueprint to quickly put things back in place as they were.

Finally, and most important, if you ever need to switch IT providers, your replacement company will be able to take over quickly because the network has been documented properly.

All our clients receive this in written and electronic form at no additional cost. We also perform a quarterly update on this material and make sure certain key people from your organization have this information and know how to use it, giving you complete control over your network.

Side note: You should NEVER allow an IT person to have that much control over you and your company. If you get the sneaking suspicion that your current IT person is keeping this under their control as a means of job security, get rid of them (and we can help to make sure you don't suffer ANY ill effects). This is downright unethical and dangerous to your organization, so don't tolerate it!

Q11: DO YOU MEET WITH YOUR CLIENTS QUARTERLY AS PART OF YOUR MANAGED SERVICES AGREEMENT?

OUR ANSWER: To us, there's nothing more important than face-to-face time with our clients. Therefore, we make it a priority to meet with all our clients at least quarterly (sometimes more often) to provide a "technology review."

In these meetings, we provide you with the status updates of projects you're working on and of the health and security of your network. We also make recommendations for new equipment and upgrades you'll be needing soon or sometime in the near future. Our quarterly meetings with you are C-level discussions (not geek-fests) where we openly discuss your business goals, including your IT budget, critical projects, compliance issues, known problems and cyber security best practices.

Our goal in these meetings is to help you improve operations, lower costs, increase efficiencies and ensure your organizational productivity stays high. This is also your opportunity to give us feedback on how we're doing and discuss upcoming projects.

Q12: IF I NEED OR WANT TO CANCEL MY SERVICE WITH YOU, HOW DOES THIS HAPPEN AND HOW DO YOU OFFBOARD US?

OUR ANSWER: Make sure you carefully review the cancellation clause in your agreement. Many IT firms hold their clients hostage with long-term contracts that contain hefty cancellation penalties and will even sue you if you refuse to pay.

We would never "force" a client to stay with us if they are unhappy. Therefore, we make it easy to cancel your contract with us, with zero contention or fines. Our "easy out" agreements make us work that much harder to exceed your expectations every day so we keep your business.

CYBER SECURITY:

Q13: WHAT CYBER SECURITY CERTIFICATIONS DO YOU AND YOUR IN-HOUSE TEAM HAVE?

OUR ANSWER: It's important that your IT firm have some type of recent training and certifications, and they should be able to answer this question, which demonstrates a dedication to learning and keeping up with the latest cyber security protections. If they don't have any, and they aren't investing in ongoing training for their engineers, that's a red flag. Some business owners won't invest in training and give this excuse: "What if I spend all this money in training my employees and then they leave us for another job?" Our response is, "What if you DON'T train them and they stay?"

You can feel confident that our in-house team has among the most advanced cyber security training and certifications available, including the CompTIA Security Trustmark+. We are one of 35 firms in the world to attain the only I.T. industry cybersecurity certification. You can read more about this highly coveted certification here: https://www.xitx.com/security-plus-trustmark/

Q14: HOW DO YOU LOCK DOWN OUR EMPLOYEES' PCS AND DEVICES TO ENSURE THEY'RE NOT COMPROMISING OUR NETWORK?

OUR ANSWER: As above, the question may get a bit technical. The key is that they HAVE an answer and don't hesitate to provide it. Some of the things they should mention are:
2FA (two-factor authentication)
Security & Awareness Training Program
Advanced end-point protection, NOT just antivirus
Password Management Tool

Because a combination of these lockdown strategies is essential to protecting your network and data, we employ ALL of these for our clients. Effective cyber security should never compromise between choosing this OR that. It should feature every weapon in your arsenal.

Q15: WHAT CYBER LIABILITY AND ERRORS AND OMISSIONS INSURANCE DO YOU CARRY TO PROTECT ME?

OUR ANSWER: Here's something to ask about: if THEY cause a problem with your network that causes you to be down for hours or days, to lose data or get hacked, who's responsible? What if one of their technicians gets hurt at your office? Or damages your property while there?

In this litigious society we live in, you better make darn sure whomever you hire is adequately insured with both errors and omissions insurance, workers' compensation, and cyber liability – and don't be shy about asking them to send you the policy to review!

If you get hit with ransomware due to their negligence, someone has to pay for your lost sales, the recovery costs and the interruption to your business operations. If they don't have insurance to cover YOUR losses of business interruption, they might not be able to pay, and you'll have to end up suing them to cover your costs. If sensitive client data is compromised, who's responsible for paying the fines that you might incur and the lawsuits that could happen? No one is perfect, which is why you need them to carry adequate insurance.

True story: A few years ago, a company that shall not be named was slapped with several multimillion-dollar lawsuits from customers for bad behavior by their technicians. In some cases, their techs were accessing, copying, and distributing personal information they gained access to on customers' PCs and laptops brought in for repairs. In other cases, they lost a client's laptop (and subsequently all the data on it) and tried to cover it up. Bottom line, make sure the IT firm you are hiring has proper insurance to protect YOU.

Rest assured, we make it a priority to carry all the necessary insurance to protect you, including world class cyber liability insurance that protect your company as well as our own. Simply ask, and we will be happy to show you a copy of our policy.

Q16: WHO AUDITS YOUR COMPANY'S CYBER SECURITY PROTOCOLS AND WHEN WAS THE LAST TIME THEY CONDUCTED AN AUDIT?

OUR ANSWER: Nobody should proofread their own work, and every professional IT consulting firm will have an independent third party reviewing and evaluating their company for airtight cyber security practices.

There are many companies that offer this service, so who they use can vary (there's a number of good ones out there). If they don't have a professional cyber security auditing firm doing this for them on at least a quarterly basis, or if they tell you they get their peers to audit them, DO NOT hire them. That shows they are not taking cyber security seriously.

You can be confident in the effectiveness of our cyber security because we are audited by CompTIA's cyber security auditors, and we have just recently been audited in November 2021.

Q17: DO YOU HAVE A SOC AND DO YOU RUN IT IN-HOUSE OR OUTSOURCE IT? IF OUTSOURCED, WHAT COMPANY DO YOU USE?

OUR ANSWER: A SOC (pronounced "sock"), or security operations center, is a centralized department within a company to monitor and deal with security issues pertaining to a company's network.

What's tricky here is that some IT firms have the resources and ability to run a good SOC in-house (this is the minority of outsourced IT firms out there). Others cannot and outsource it because they know their limitations (not entirely a bad thing).

But the key thing to look for is that they have one. Less experienced IT consultants may monitor your network hardware, such as servers and workstations, for uptime and patches, but they might not provide security monitoring. This is particularly important if you host sensitive data (financial information, medical records, credit cards, etc.) and fall under regulatory compliance for data protection.

Rest assured, we do have a fully staffed SOC to provide proactive security monitoring for our clients to better prevent a network violation or data breach.

BACKUPS AND DISASTER RECOVERY:

Q18: CAN YOU PROVIDE A TIMELINE OF HOW LONG IT WILL TAKE TO GET MY NETWORK BACK UP AND RUNNING IN THE EVENT OF A DISASTER?

OUR ANSWER: There are two aspects to backing up your data that most business owners aren't aware of. The first is "fail over" and the other is "fail back." For example, if you get a flat tire, you would fail over by putting on the spare tire to get to a service station where you can fail back to a new or repaired tire.

If you were to have a disaster that wiped out your data and network – be it a ransomware attack or natural disaster – you want to make sure you have a fail-over solution in place so your employees could continue to work with as little interruption as possible. This fail-over should be in the cloud and locked down separately to avoid ransomware from infecting the backups as well as the physical servers and workstations.

But, at some point, you need to fail back to your on-premise network, and that's a process that could take days or even weeks. If the backups aren't done correctly, you might not be able to get it back at all.
So, one of the key areas you want to discuss with your next IT consultant or firm is how they handle both data backup AND disaster recovery. They should have a plan in place and be able to explain the process for the emergency fail-over as well as the process for restoring your network and data with a timeline.

In this day and age, regardless of natural disaster, equipment failure or any other issue, your business should ALWAYS be able to be operational with its data within six to eight hours or less, and critical operations should be failed over immediately.

We understand how important your data is and how getting your team up and running quickly is essential to your business success. Therefore, in the event of any disaster, we can confidently get your network back up and running in 24 hours or less.

Q19: DO YOU INSIST ON DOING PERIODIC TEST RESTORES OF MY BACKUPS TO MAKE SURE THE DATA IS NOT CORRUPT AND COULD BE RESTORED IN THE EVENT OF A DISASTER?

OUR ANSWER: A great IT consultant will place eyes on your backup systems every single day to ensure that backups are actually occurring, and without failures. However, in addition to this, your IT company should perform a monthly randomized "fire drill" test restore of some of your files from backups to make sure your data CAN be recovered in the event of an emergency. After all, the WORST time to "test" a backup is when you desperately need it.

If you don't feel comfortable asking your current IT company to test your backup OR if you have concerns and want to see proof yourself, just conduct this little test: Copy three unimportant files onto a thumb drive (so you don't lose them) and delete them from your server. Make sure one was newly created that same day, one was created a week earlier and the last a month earlier. Then call your IT company and let them know you've lost three important documents and need them restored from backups as soon as possible. They should be able to do this easily and quickly. If not, you have a problem that needs to be addressed immediately!

Verifying your backups daily and testing them on a regular basis is a cornerstone of a successful overall IT strategy. These are the lengths we go to for all our clients, including multiple random "fire drill" test restores to ensure ALL your files are safe because they are always backed up.

Q20: IF I WERE TO EXPERIENCE A LOCATION DISASTER, PANDEMIC SHUTDOWN OR OTHER DISASTER THAT PREVENTED ME FROM BEING IN THE OFFICE, HOW WOULD YOU ENABLE ME AND MY EMPLOYEES TO WORK FROM A REMOTE LOCATION?

OUR ANSWER: If Covid taught us anything, it's that work-interrupting disasters CAN and DO happen when you least expect them. Fires, floods, hurricanes, and tornadoes can wipe out an entire building or location. Covid forced everyone into lockdown, and it could happen again.

We could experience a terrorist attack, civil unrest or riots that could shut down entire cities and streets, making it physically impossible to get into a building. Who knows what could be coming down the pike? Hopefully NONE of this will happen, but sadly it could.

That's why you want to ask your prospective IT consultant how quickly they were able to get their clients working remote (and securely) when Covid shut everything down. Ask to talk to a few of their clients about how the process went.

Here's how we handled our clients' needs when it seemed everyone needed to work remote, get laptops and implement security measures almost overnight. First, we led with security and provided solutions for our clients who seemingly had none. We provide three different ways companies could provide secure remote access to their staff. We were one of the first to implement multifactor authentication on remote access and to this day we work with our clients on improving the work from home experience while making it more secure.

Q21: SHOW ME YOUR PROCESS AND DOCUMENTATION FOR ONBOARDING ME AS A NEW CLIENT.

OUR ANSWER: The reason for asking this question is to see if they HAVE SOMETHING in place. A plan, a procedure, a process. Don't take their word for it. Ask to SEE it in writing. What's important here is that they can produce some type of process. Further, they should be able to explain how their process works.

One thing you will need to discuss in detail is how they are going to take over from the current IT company – particularly if the current company is hostile. It's disturbing to me how many IT companies or people will become bitter and resentful over being fired and will do things to screw up your security and create problems for the new company as a childish way of getting revenge. (Sadly, it's more common than you think.) A good IT company will have a process in place for handling this.

If you consider us as your next IT services firm, we will gladly share our new client onboarding process and documentation. I think you'll be impressed.

OTHER THINGS TO NOTICE AND LOOK FOR:

ARE THEY GOOD AT ANSWERING YOUR QUESTIONS IN TERMS YOU CAN UNDERSTAND AND NOT IN ARROGANT, CONFUSING "GEEK-SPEAK"?

Good IT companies won't confuse you with techno-mumbo-jumbo, and they certainly shouldn't make you feel stupid for asking questions. All great consultants have the "heart of a teacher" and will take time to answer your questions and explain everything in simple terms. As you interact with them in the evaluation process, watch for this.

Our technicians are trained to take time to answer your questions and explain everything in simple terms. Just look at what Virginia Kelly & Trevor Gettmann had to say:

"The team at Xact I.T. is awesome as always comes in remotely does their thing in a flash and back out so I am right back to work! Love Xact IT Solutions!"
-Virginia Kelly – Blumberg & Wolk Trial Lawyers

"The team at Xact I.T. Solutions have done a tremendous job the last 3 months. Xact has been our IT management for 20+ years but they have really out done themselves during the stay at home order. I would highly recommend them to anyone looking for someone to help them with cybersecurity and I.T. in their business large or small."
Trevor Gettmann – American Insurance Agency

DO THEY AND THEIR TECHNICIANS PRESENT THEMSELVES AS TRUE PROFESSIONALS WHEN THEY ARE IN YOUR OFFICE? DO THEY DRESS PROFESSIONALLY AND SHOW UP ON TIME?

If you'd be embarrassed if YOUR clients saw your IT consultant behind your desk, that should be a big red flag.

How you do anything is how you do everything, so if they cannot show up on time for appointments, are sloppy with paperwork, show up unprepared, forget your requests and seem disorganized in the meeting, how can you expect them to be 100% on point with your IT? You can't. Look for someone else.

Our technicians are true professionals who you would be proud to have in your office. They dress professionally and show up on time, and if they cannot be there on time (for some odd, unforeseen reason), we always notify the client immediately. We believe these are minimum requirements for delivering a professional service.

DO THEY HAVE EXPERTISE IN HELPING CLIENTS SIMILAR TO YOU?

Do they understand how your business operates the line-of-business applications you depend on?
Do they understand the compliance requirements you have around cybersecurity and what failing to meets those requirements means to you and your business?
Are they familiar with how you communicate, get paid, service your clients or patients and run your business?

We have many medium and large-sized businesses that we love to work with and help them tackle the compliance challenges in their industries. The reason we work well with them is that we understand that as the person in charge of the I.T. you wear many hats and sometimes it can feel like getting all of this stuff done can seem impossible. You might not have the man power, or the budget – that's where we come in. We make you look like a super hero every day – we do all the heavy lifting while you take all the credit.

Here's what Ken Wilson had to say:

"The team at Xact IT has been a valuable partner for our business. We were a startup in 2015 and Xact IT has been with us from year one and we have been very successful as we continue into our sixth year. We are a global business with offices in the US and Europe. Our client base is the pharmaceutical industry. This means we have a very demanding customer group with very high standards for data security and IT policies and procedures. The Xact IT team has helped us grow and maintain very high capabilities such that we can grow our base of business with some of the largest companies in the world. Bryan and his team have always been very responsive and have acted as our consultants or business advisors. We are very happy with this relationship and look forward to many years of working together."

THE 4 MOST COSTLY MISCONCEPTIONS ABOUT IT SERVICES

MISCONCEPTION #1: MY IT NETWORK DOESN'T NEED REGULAR MONITORING AND CYBER SECURITY MAINTENANCE (MANAGED SERVICES).

This is probably one of the biggest and most costly misconceptions that business owners have. Usually this is because they've been fortunate enough to have never encountered a major system failure that caused data loss from human error (or a disgruntled employee), failed hardware or even a ransomware attack, but that's just like someone thinking they don't need to wear a seat belt when driving a car because they've never had an accident.

IT networks are complex and dynamic systems that need regular updates and maintenance to stay up, secure, running fast and problem-free – especially now with the proliferation and sophistication of ransomware and hacker attacks. Here are just a FEW of the critical updates that need to be done on a weekly – if not daily – basis:

Security patches, updates and management
Antivirus updates and monitoring
Firewall updates and monitoring
Backup monitoring and test restores
Spam-filter updates
Operating system updates, management
Monitoring hardware for signs of failure
Alignment of cybersecurity standards

If your IT support tech does not insist on some type of regular, automated monitoring or maintenance of your network, especially for cyber protections, then DO NOT HIRE THEM.

Either they don't know enough to make this recommendation, which is a sure sign they are grossly inexperienced and unprofessional, or...

They recognize that they are profiting from your IT problems and don't want to recommend steps toward prevention, which would reduce the number of issues they are paying you to resolve.

Either reason is a good one to get as far away from that person as possible!

MISCONCEPTION #2: MY NEPHEW/NEIGHBOR'S KID/BROTHER-IN-LAW/OFFICE MANAGER KNOWS THIS IT STUFF AND CAN TAKE CARE OF OUR NETWORK.

Most people look for a part-time "guru" for one reason: to save a few bucks. But this often comes back to haunt them. We frequently get calls from business owners who desperately need our help to get them back up and running or to clean up a mess that was caused by an inexperienced employee or friend who was just trying to help.

If the person you have working on your IT systems does not do IT support for a living, there is a good chance they won't have the knowledge or experience to truly help you – they are a hobbyist at best. And do you really want a part-time, inexperienced person responsible for handling something as important as your data and IT network? As with everything in life, you get what you pay for. That's not to say you need to go broke to find a great IT firm, but you shouldn't be choosing someone based on price alone.

MISCONCEPTION #3: YOU SHOULDN'T HAVE TO PAY "THAT MUCH" FOR IT SERVICES.

We all know you get what you pay for. A cheap hourly rate (under $250 per hour, which is the average fee for professional IT firms in Philadelphia) usually means a cheap job. Like every other profession, good IT engineers and techs do NOT work cheap because they are in high demand. When you see low IT services fees, it's because of one of the following:

They are a small shop just getting started. Usually they will have only one to two techs working for them (or they are a solo shop). That size of company may be perfectly fine for a small business that is not regulated, doesn't have sophisticated IT requirements and/or has only 10 or fewer PCs to support. This would not be a good choice for a larger organization that needs professional IT services for their growing company.

They are hiring inexperienced (cheap) college kids or newbie technicians because they will work for next to nothing, OR they allow interns to support your network because they don't have to pay them at all – but what you don't realize is that an inexperienced technician like this can end up costing more because:

They improperly diagnose problems, which means you're paying them to fix the wrong thing and they still won't resolve your issue. Case in point: A few years ago a TV reporter went undercover to IT services companies in LA with a perfectly working PC, but simply disconnected a cable in the back (a fix that the average tech would have caught in minutes with a visual inspection). Several shops improperly diagnosed the problem and wanted to charge them up to $275 to fix it!

They could take three to five times as long to do the same repair an experienced technician could fix quickly. Again, you're paying for those extra hours AND you're frustrated and unproductive while you wait for the SAME problem to be fixed!

They could do things that put your security and data in jeopardy. True story: An inexperienced engineer of a competitor turned off all security notifications his client's network was producing because it was "too much work" to sift and sort through them. Because of this, the company got hacked and ended up having to pay a ransom to get their data back, not to mention suffered downtime for days while they scrambled to recover. Don't let a cheap, inexperienced tech do this to you!

With your client data, accounting records, e-mail and other critical data at stake, do you REALLY want the lowest-priced shop working on your machine?

We take the view that most people want value for their money and simply want the job done right. You will find that we are not the cheapest, but we don't apologize for that. As the owner, I decided a long time ago that I would rather explain our higher rates ONE TIME than make excuses for POOR SERVICE forever. That said, we're not the most expensive either. We simply feel that we should offer a good service at a fair price. That's why we have been able to stay in business for over 18 years and have many customers who've been with us that entire time.

MISCONCEPTION #4: AN HONEST IT SERVICES COMPANY SHOULD BE ABLE TO GIVE YOU A QUOTE OVER THE PHONE.

I wish this were true, but it isn't. Just like a good doctor, an honest and professional technician will need to diagnose your network before they can quote any price over the phone; consider the example above where all that was needed was to plug in a simple cable. If someone brought that to us, we would just plug it back in and not charge them, but without SEEING the computer, we could have never diagnosed that over the phone.

3 MORE RECOMMENDATIONS TO FIND A GREAT IT COMPANY YOU'LL LOVE

Ask to speak to several of their current clients. Check their references! Don't just take the sales guy's word that they are good – ask to speak to at least three or four clients that are similar to you in size and scope. If they hesitate or cannot provide you with references, don't trust them!

Another good sign is that they have good online reviews and client testimonials on their website. A lack of this may be a sign that they don't HAVE clients who are happy enough to provide a good reference – again, a warning sign.

Look for a company that is not too small as can leave your company and reputation at risk.

Choose an IT consultant who certified in cybersecurity

A FINAL RECOMMENDATION

I hope you have found this guide to be helpful in shedding some light on what to look for when outsourcing IT for your company. As I stated in the opening of this report, my purpose in providing this information was to help you make an informed decision and avoid getting burned by the many incompetent firms offering these services.

If you are looking for someone you can trust to take over the care and maintenance of "all things digital" in your office, we'd love the opportunity to EARN your business. To that end, we'd like to offer you a Cyber Security Risk Assessment and IT Systems Checkup at a deep discount.

I can only afford to discount a handful of these each month. But you have to act quick as they usually go fast! This comes with no expectations for you to hire us unless you feel that is the right thing for you to do. Here's how this works...

We'll meet by phone (or Zoom) to have a brief conversation about your current situation; what you are frustrated by, looking for in an IT company and any concerns and questions you have. We'll ask you a few questions that you should easily be able to answer. Depending on what we discover, we can move to the next step, which is to conduct a quick, non-invasive, CONFIDENTIAL investigation of your computer network, backups and security protocols.

Your current IT company or team DOES NOT NEED TO KNOW we are conducting this assessment, or we can involve them. (The choice is yours, but we recommend NOT letting them know this inspection is happening so we can get a truer read of how secure you are. After all, the cybercriminals won't tip you off that they're about to hack you.)

Your time investment is minimal: 15 minutes for the initial phone consultation and one hour in the second meeting to go over what we discover. When this Risk Assessment is complete, here's what you will know:

If your IT systems and data are truly secured from hackers, cybercriminals, ransomware and even sabotage by rogue employees.

If your current backup would allow you to be up and running again fast if ransomware locked all your files – 99% of the computer networks we've reviewed failed this test.

If you and your employees' login credentials are being sold on the dark web right now and what to do about it. (I can practically guarantee they are, due to a recent 8.4 billion credentials being sold on the dark web. What we find will shock you.)

Answers to any questions you have about a recurring problem, an upcoming project or change or about the service you are currently getting.

When done, we'll provide you with a "Report Of Findings" and Network Health Score that will show you where you are vulnerable to cyber-attacks, problem devices, backup issues, etc. We'll also provide you with an Action Plan, for free, on how to remediate any less than favorable situation or problem we discover – and if you choose, we can assist you in its implementation.

After doing this for 18 years, I can practically guarantee I will find significant and preventable security loopholes in your network and problems with your backups. Like Sherlock Holmes, we never fail. If nothing else, our Risk Assessment is an easy and cheap (free) way to get a valid third party to verify your security and give you peace of mind.

HOW TO REQUEST THIS RISK ASSESSMENT:

Go online to: https://www.xitx.com/getmycyberaudit/
Call me direct at 856-282-4100
E-mail me directly with questions: bhornung@xitx.com
Dedicated to securing your critical assets,

Xact I.T. Solutions Inc

READ ON TO HEAR WHAT OUR CLIENTS HAVE TO SAY:

ELLYN FISHER – YARDLEY MAKEFIELD EMERGENCY UNIT
"Xact IT Solutions always has the best interest of the customer in mind when providing services. As times change and business runs a little different, I can count on Xact IT Solutions to resolve problems and suggest the most cost-effective solutions. This is important for a busy 911 rescue squad. Xact IT Solutions is highly recommended by our organization."

DAVID K. SCHEURING, SR. – ADMIN PARTNERS
"Xact I.T. Solutions have worked with Admin Partners to upgrade our entire infrastructure. Our network is more secure and tech issues have been dramatically reduced thanks to their efforts. The team wants things to be done the right way and works with you to make prudent decisions about technology."

SAM GREEN – APPAREL MACHINERY
"Xact, IT has been our IT partner for at least 10 years. The team is always responsive whenever an issue arises, big or small. They keep us informed of potential issues and make appropriate recommendations knowing we are sensitive to costs. As the CFO of our company, I am very pleased with their service and know IT is one less thing I have to worry about because XACT IT has our back. If you are considering a new IT partner, I strongly suggest contacting Xact IT Solutions to discuss your situation; it will be time well spent....."

STEVE SARKISIAN – PAUL TRIPP MINISTRIES
"I have been dealing with this company for 20+ years. They have always solved my problem. They are integrity which is important when dealing with people in this industry. I am very thankful I have someone to take care of keeping my companies safe."

PATTI LEVY – GOLDEN EAGLE CLEANING SERVICES
"Our business has used Xact IT Solutions for over 5 years. They are very dependable and we can leave our business knowing that Xact IT can remedy any computer issue that happens in our absence. They are very quick to respond to all our questions and needs."

TREVOR GETTMANN – AMERICA INSURANCE AGENCY
"The expert team has done a tremendous job the last 3 months. Xact has been our IT management for years but they have really out done themselves during the stay-at-home order. I would highly recommend this company to anyone looking for someone to help them with their business large or small."