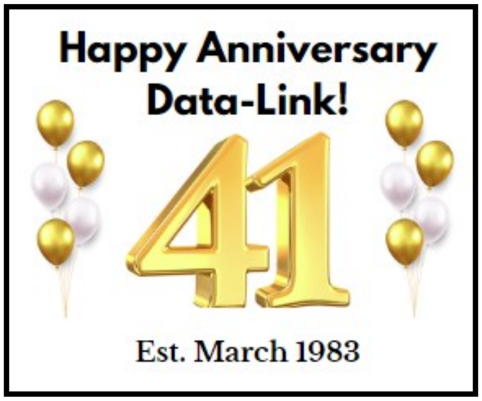
Data-Link Associates, Inc.

March 2024

DataGrams

Proven, Field Tested **Network Security Strategies** To Help Our Clients Make **Confident, Real-Time** Cybersecurity Decisions.



thank you

To our Clients:

Thank you for trusting us with your computer network over the years.

Our success is attributed to your loyalty.

We are grateful for the opportunity to serve you for many years to come.

WHAT'S INSIDE?

You're NOT JUST LUCKY

Sun Tzu wrote, "Victorious warriors win first and then go to war, while defeated warriors go to war first, then seek to win."

Cyber warfare is won by the people you trust to guard the gates and set up defenses. They are in charge of strategy, educating your troops, and stoic leadership in your 11th hour.

The provider you choose will directly impact whether or not your company will survive a cyberbreach or ransomware.

MSPs (Managed Services Providers, like us) are everywhere, hundreds popping up every year due to the exponential increases in ransomware attacks.

With software running the show, every Tom, Dick and Harry is incorporating and calling themselves an MSP.

Some offer independent services, while others are part of larger firms. Some are new to the field, while others have been around for years. There are also "MSPs" that put out slick marketing to grab your attention but make it hard to tell if they really live up to the hype.

Well, we're here to help you cut through the clutter. You want to hire someone who knows what they're doing and will take care of your business the right way. To do that, there are a few questions you should ask every IT expert before you let them anywhere near your network to ensure you'll be in good hands.

1. What's Your IT Experience?

Education and hands-on experience are all important. You want to know your "expert" is actually an expert.
It's all too easy for someone to pass themselves off as an expert when they have limited experience, so you should never hire an individual or company without vetting them first.

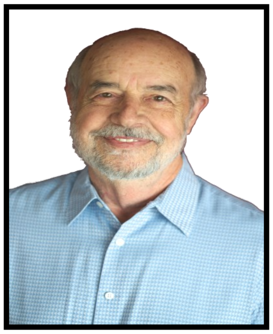
After all, this person (or team) will be handling EXTREMELY sensitive hardware and data essential to the operation of your business. This isn't the time to take risks or give someone the benefit of the doubt.

When you work with an IT services company, or MSP, you can generally expect that the people you work with are educated and experienced, but you should **always** ask. It's okay to dive in and ask them how long they've been doing their job or how familiar they are with your industry. And if you aren't sure what some jargon means, feel free to ask follow-up questions. There's a good chance they'll be more than happy to answer all of your questions, especially if they're a true professional who knows what they're doing!

2. What's Your IT Approach?

There are different approaches to IT and network security. You have the **break-fix** approach and the **managed services** approach. The break-fix approach used to be the staple of the IT industry—it was the business model of just about every IT support firm in the 1990s and early 2000s.

Continued on page 2 →



This monthly publication provided courtesy of Richard Frielink, Founder & President of Data-Link.

Our Mission

To provide IT solutions and services that allow our clients to succeed in an ever changing and challenging business environment.

Richard C. Frielink

EMERGENCY

(630) 406-8969

24/7

If you're new here…

Scan To Sign Up For Our

Weekly IT Security Tips

Data-Link Associates, Inc.

to receive timely and relevant cybersecurity tips and news via email every week!

← Continued from page 1

This approach is pretty straight-forward: something breaks, so you hire someone to come in and fix it. If many things break or something complicated breaks, you could be looking at a hefty bill—not to mention the costs associated with downtime.

The alternative to break-fix is the managed services approach (or a hybrid) which all modern IT services providers offer (and if they don't, look elsewhere). They don't wait for something to break—they're already on it, monitoring your network 24/7, looking for outside threats and internal issues. They use advanced software that continuously monitors end-user devices to detect and respond to cyberthreats like ransomware and malware. They can go to work, proactively protecting your business so you can avoid those hefty bills and long downtimes. Managed Services might not make sense for all businesses, so find an MSP that offers break-fix, managed and co-managed services.

These are companies that are willing to collaborate with you and your business to make sure you're protected, your IT needs are met, and you're getting your dollars' worth.

3. What About Response Time?

This question often gets overlooked, but it's one that can make or break your business—and it can make or break your relationship with your IT services provider.

You need to know that you won't be left in the dark when something goes wrong within your network.

If you experience a cyberattack, the cost to your business can be catastrophic if your IT services provider cannot remediate your situation in a timely manner. The longer you have to wait, the worse it can get.

You need to work with someone who will be on-call in the event of an emergency. You should be provided an after-hours phone number or instructions on how to reach someone in the event of a technical emergency.

They should be doing everything they can to instill confidence that they'll be there for your when you need them. If you're working with an IT company that doesn't have your full confidence, you may need to rethink that relationship.

Cybersecurity isn't a LUCK game. Prepare with experts and your company can recover from anything.

The Die Hard 'Jug Problem'

Brainteaser: If you had an infinite supply of water and a 5-liter and 3-liter bucket, how would you measure exactly 4 liters? The buckets do not have any intermediate markings.

Answer: A lot of wasted water

Workings: You may already know the answer or have worked it out, but we are obliged to give you an answer. Fill the 5-liter bucket first. Then using that bucket fill the 3-liter bucket, being careful not to spill any. This leaves 2 liters in the 5-liter bucket.

Now chuck away the water in the 3-liter bucket and refill with the remaining 2 liters from the bigger bucket. Once again, fill the 5-liter bucket and then use this to fill the second 3-liter bucket. This will leave you with 4 liters in the 5-liter bucket. Simples!

Recommend Us
On Google

We have the best clients!

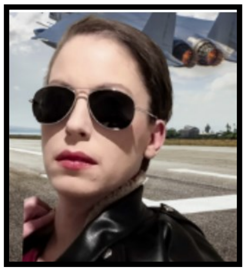
You always have the nicest things to say to us about our people, service and offerings.

Whether we've been together for years, or we're at the beginning of our journey, we invite you to put it in writing and let the world know!

You can do that here:

Thank you kindly!

EDR Is No Longer Optional!
A Rant To The IT Professionals Out There



EDR (endpoint detection and response) is no longer 'nice to have', it's a necessity.

EDR provides the critical visibility needed to maintain proper network security.

Should something go sideways, the EDR provides the telemetry we need for quick action and remediation. We can most often shorten the remediation window and drastically reduce your time spent on incident response with EDR deployed.

EDR is a mature, behavior-based antivirus which detects threats based on threat behavior and then blocks or quarantines it.

EDR is now a key component of cyber defense for EVERY business. It's time to make sure your IT staff or managed services company has EDR deployed on your network.

Those relying on Windows Defender alone (the standard issue antivirus on Windows 10 & 11 operating systems) are opening themselves to attack because someone could leverage Microsoft's own command against its solution to disable it using PowerShell or net commands. When EDR is backed with additional security tools, or an MSP's recommended stack, these threats are better mitigated.

Your Cyber Wingman, Pam

BREAK-FIX NO CONTRACT

FULLY MANAGED IT SERVICES

CO-MANAGED PARNERSHIP

If your business can't afford downtime, you need critical cybernews FAST!

meet us on in

CYBERSECURITY • SINCE 1983 • IT SUPPORT • DLA

Thank You For Calling!

Thank you to those who called in a referral this month, sent topic requests for the Weekly IT Tip emails, requested more information or sat for an appointment. We appreciate you!

US Govt Shares Cyber Defense Tips For Water Utilities

CISA, FBI and EPA published their list of defense measures for US water utilities on February 21st urging all WWS sector and other critical infrastructure organizations to review the fact sheet and implement the actions.

Law Enforcement Agencies From 10 Countries Hack Into The World's Biggest Ransomware Operation, LockBit

On February 19th, authorities took down LockBit's infrastructure, which included 34 servers hosting the data leak website and its mirrors, data stolen from victims, crypto-currency addresses, decryption keys, and the affiliate panel.

On Feb 24, Lock Bit announced it was resuming the ransomware business and released damage control communication admitting that "personal negligence and irresponsibility" led to the breach.

- End-to-end encryption app, **Signal**, rolls out usernames that let you hide your phone number.

For IT Professionals

- On-premise partners of **ConnectWise** (IT management software) are warned to patch their ScreenConnect servers immediately against a maximum severity flaw that can be used in remote code execution (RCE) attacks.
- The White House Office of the National Cyber Director (ONCD) is urging tech companies to switch to a memory-safe programming language, such as Rust, to improve software security but reducing the number of memory safety vulnerabilities.

HUMANS CANNOT REMEMBER RANDOMNESS

Use a password manager

CYBERSECURITY • SINCE 1983 • IT SUPPORT • DLA

Your favorite client probably won't sue you...
but their insurance company will!
Data-Link Associates, Inc.

FREE SPECIAL REPORT

The CEO/CFO's Guide To Co-Managed I.T.