Data-Link Associates, Inc.

November 2022

DataGrams

Happy Thanksgiving!

...from our family to yours.
We are thankful to have clients like you, not just on Thanksgiving, but all the year through.

SECTION179.ORG

Remember to get in all those tax deductions for computer hardware/software!
100% Bonus Depreciation will phase out after 2022

WHAT'S INSIDE?

Manufacturers Are Moving Their IT Guys From The Basement To The Boardroom

If your end-of-year boardroom agenda includes discussions to increase productivity, hiring/retention or efficiency, your IT staff could provide valuable insight. When you invite your IT into boardroom decisions, you may be surprised at the solutions they can offer to many (seemingly) non-technical problems such as:

Want to increase productivity? There are many ways your IT guy can improve your staff's productivity including upgrading or adding hardware/software to automate or streamline processes.

Having hiring and retention issues? With your already measured metrics in hand, ask your IT to automate certain tasks to decrease the need for additional staff.

Can't keep up with business growth? Revisit work from home or hybrid work weeks to gain up to 1 1/2 days per week that are currently taken up by travel time and re-focus time. Your IT department can help you determine feasibility and coordinate the project.

Are your invoice, payroll, tax or billing programs slow or not user-friendly? Your IT group can review SaaS applications and software/hardware upgrades and replacements. "Being slow" is not a characteristic of properly functioning software/hardware. If it's broken, time to fix it!

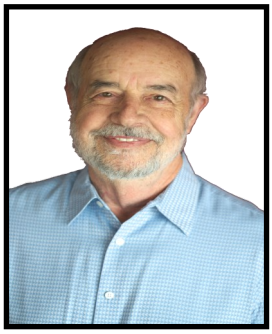
Asset list and roadmap to replacement based on budget. Replacing hardware and software can be costly so you'll want a well-laid plan. Ask your IT what the company *needs* rather than making them work off a budget pulled from thin air with leftover funds. Your company's productivity and security depend on masterful, systematic replacements.

Many interesting ideas can come from your IT department on issues that aren't traditionally in their wheelhouse. Consider bringing them into the boardroom for your big conversations in the future.

We are happy to sit in on a meeting with you and your IT staff to facilitate a discussion of these points and others. Just drop us a line at (630) 406-8969 x574 or sales@datalinkmsp.com.

Scan This Code to Request Your

FREE IT Disaster Recovery Template



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

EMERGENCY

(630) 406-8969

24/7

Coming up in the next issue:

- Introducing: ThreatLocker
- Cyber-Safe Shopping
- Your IT Diagnosis & Prescription
- A Hacker's Quota

Redundant Technology Ensures 100% Uptime

Redundancy in the workplace doesn't stop at cross-training your staff or the process of terminating redundant job roles. (I am reminded of the Bobs in the cult-classic movie, *Office Space.)*

Defined, redundancy is *a system design in which a component is duplicated so if it fails there will be a backup.* In a company's IT network, redundancy can be the only reason you are still producing when the worst happens.

Having backup hardware and copies of your files is the best way to recover after a breach, system failure, natural disaster or rogue employee incident.

If you've known us for any length of time, you've heard us talk about the importance of hardware and data redundancies.

Here are the minimum redundancies you should employ in your company so you don't need to start from scratch in the event of a cyber disaster of any scale-from hackers and theft to flood or fire and just to keep your company producing, overall:

The goal is ZERO downtime.

- Back up your files in 2 or more places.
- Purchase and stage a backup domain controller
- Network failover with alternate network paths implemented through routers and switches.
- An MSP (managed services provider) for back up IT help if you only have one main IT person.
- APC Batteries (for server room and desktops)
- Extra computers and monitors (see chip shortage waits)
- And the "little things" like backup keyboards, mice, cameras, speakers and headphones.

For those who aren't afraid of overkill and want to ensure 100% uptime,

ADD:

- Server redundancy— a replica of a server is created with the same computing power, storage, applications and other operational parameters.

- Multi-Wan internet redundancy— this can double or triple your cost but you will always have internet.

We invite you to

Sign Up For Our Weekly IT Security Tips

to receive timely, relevant cybersecurity tips and news via email every Tuesday morning, AND Critical Cyber News as it comes down.

Thank you for your support! Our list has reached 1,013—consisting of 353 CEOs/ principals and 660 support staff who receive these tips each week.
<—Scan the QR Code to begin. We promise to NEVER spam.

sales@datalinkmsp.com
(630) 406-8969 ext 574

Thank You For Updating Your Phone

Driving The News: A recent report found that half of all Android-based mobile phones used by government employees are running outdated versions of the operating system, exposing them to hundreds of vulnerabilities that can be leveraged for attacks.

The report additionally warns of a rise in all threat metrics, including phishing attacks against government employees, reliance on unmanaged mobile devices, and liability points to mission-critical networks. Analysts say year-over-year, malware distribution is dropping and credential theft attacks are increasing. In 2022, 1 out of 11 government employees monitored were targeted by a phishing attack.

Android users: Android does not force updates so you can go a very long time without the proper patches on your phone. This is what is getting the government employees in trouble.

iPhone users: iPhone is smart and will FORCE your update. If you wait until your phone literally forces you to apply the operating system (OS) update because you ignore the prompts, it's high time you stop doing that.

As soon as you are initially prompted, your current OS is out-of-date and is more vulnerable to attack. The new update has patches to fix vulnerabilities hackers have learned to exploit since the last patch.

I've heard your excuse of "I meant to run the update but I was using my phone at the time" or "my phone is working great right now, the last time I ran an update, it broke something."

Usually, running an update is inconvenient but they apply critical security patches that are way more important to solve than the minor inconvenience of needing to reset your notification settings or some similar insignificant set back.

Please update your phone as soon as possible… same-day… as the release of the update.

To manually update your phone to the latest and greatest update:

Android:
Settings > System >
System Update and follow steps.

iOS:
Settings > General >
Software Update

On behalf of your friends, family, neighbors and collegues, "Thank you for updating your phone", it keeps everyone you communicate with safer.

Install The Latest Windows Update ASAP! Patches Issued for 6 Actively Exploited Zero-Days and How To Protect Your Company While You Wait

NOTE: Clients with Managed Services contracts have had these patches already applied. No action required.

It might surprise you how many engineers we have as clients. It is not only the obvious fact that since we specialize in IT for manufacturers that our clients would have an engineering background but the insistence of engineers who understand the backbones of technology and could probably do basic IT management themselves opt to have us do the work for them– they realize the time it takes to properly secure a network and they would rather spend that time working ON their business, not IN it.

Case in point, and the theme of this article- a whopping 6 ZERO-DAYS were patched in the latest Windows Update. That is a CRAZY amount and it's a surprise we're all still in business today without having a ransom or some other god-awful hacker incident (that we've heard of so far).

If you're new here, a zero-day vulnerability means that security teams at software companies are unaware of a vulnerability in their product and it is currently active and running around "in the wild" (a term we hear often in the industry). Developers have "zero days" to fix the threat before it becomes a threat to the public.

If you don't have an IT company or IT department pushing these patches out, you'll need to do it yourself, ASAP, to protect your devices and your data. Call us if you have questions on this.

In the time between when a zero day is discovered and the point where a patch is released can be days, weeks or even months. In that time, your devices and files are a sitting ducks.

So, how can you protect your company's assets when there's a gaggle of bouncing- baby zero days running around?

This is where your backups and redundancies come in. (see article on page 2)

The best two things to do while you wait for a patch are:

- Ensure files and data are backed up in 2 PLACES for when (one...or two!) get taken out.
- Check for security updates for all devices (computers/phones)

Hacking is an actual business. They have KPIs and quotas to meet like all of us. Your business is not "too small" or "too obscure" to evade hackers and being too busy because you're boot-strapping may be an excuse not to patch your network, but it is not only ineffective but can be harmful to your company's future. A bunch of smaller fish gives the same bounty as one big fish, and the smaller ones are easier to catch.

sales@datalinkmsp.com
(630) 406-8969 ext 574

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!

Network Endpoint Best Practices

Endpoint security is what keeps a company's data safe. Endpoint Best Practices include:

- Asset discovery: Know what is connecting to your network. (see Bring-Your-Own-Device policies)
- Device Profiling: Know and document which servers and applications each device connects to.
- Use next-generation anti-virus/Endpoint Detection and response.
- Coming Soon: Zero-Trust. Nothing in unless you say so. Hackers are pummeling "Trust but verify" environments.

Should You Toss That Stack Of Business Cards In The Trash?

An annual event for me every year during the week between Christmas and New Years is to sort through my stack of business cards collected over the past 12 months and send my 9-word email (no more than 10 words). "Are you still interested in IT Support?" "Did you give up on the Sage upgrade?" "Are you still looking at ERP software this year?" If they're in town, you'll get a quick response.

Are You a Wiz at WORDLE? What your solve rate says about your intelligence.

Does anyone out there still play WORDLE? I'm a *wiz* a Wordle but after a bit of investigation it appears that my ability to solve within 2 or 3 words is not a reflection of above-average intelligence, only an above-average ability to solve puzzles.
Thanks for the buzzkill, Wordle.

Is Masterclass worth the $180/year?

100%, yes! It breaks down to $15/month for in-depth classes delivered by famous experts in their fields from business and writing to sewing and cooking.
Pro tip: Watch *any* of them. They are all useful in areas that might not be immediately apparent. Indra Nooyi and Sir Richard Branson's classes were great.

3 Steps To Talking With A Techie

When you hang out with techies as much as I do, you realize there are productive (and not-so-productive) ways to ask a question to get your problem resolved.

These guys/gals are so smart, solution-focused and tech –minded you'll see your intended 3 minute conversation can get lost in explaining the contingencies and exceptions and before you know it you've been talking for 20 minutes. While usually fascinating, it's not a tremendously good use of everyone's time to know the 16 ways you can get to the same result nor do you need to know what would happen if lightening were to strike on a Sunday afternoon with a tornado warning in the middle of January (the unlikely exception).

Follow these 3 tips to have productive conversations with the tech-minded folks in your life:

1. Include your desired end result within your question.— "Hi Jacob, I'm trying to _[desired end result]_, what do you think would be the EASIEST, MOST ACCURATE WAY ACHIEVE THAT RESULT?"

2. Ask them to slow down—They know the information like the backs of their hands so they tend to speak quickly and repeat themselves. Ask them to slow down so you can take good notes.

3. Resist clarifying the answer—
The reason you need to take good notes in Step 2 is because you will want to resist the urge to clarify what they've already explained to you. Doing so may trigger their automatic response to solve the problem….again… but in a different way. Then you could be looking at another 20 minutes added to the conversation and you'll probably be more confused walking out than when you walked in.

We love our techs! They make our world go round and my workday that much more interesting.

The Internet of Things (IoT) Cybersecurity Risks

Often overlooked in network security, the Internet of Things (IoT) devices should be given equal consideration in cybersecurity.

IoT devices (i.e. printers, security cameras and smart home hubs, smart toilets and smart coffee machines) are connected to the internet which means they can let bugs, viruses and hackers into your network just like a computer.

Did you know a hacker can:

- Access your heating and lighting systems to find out if you're away from home?
- Access your passwords or even your bank account through the info you shared through your Echo device?
- Get into your network through an IoT device and launch a ransomware attack making your IoT smart home unusable until you pay up?
- Use your devices as bots to deliver computing power for a DDOS attack, click fraud, password cracking, or send out spam or mine crypto?