



# DataGrams



Proven, Field-Tested **Network Security Strategies** To Help Our Clients Make **Confident, Real-Time** Decisions For Their Company's Cybersecurity

## WHAT'S NEW?

We're coming up on TBR (Technology Business Review) meetings!  
**Pam will schedule with clients for dates in January/February.**  
They will be conducted via Teams and take about an hour including discussion time.

## WHAT'S INSIDE:

**We Won't Get Fooled Again (THIS Year, Right?).....1**

How Cybersecurity Will Change In 2023.....2

Ready To Onboard? What to expect in the first 30 days of your relationship with a new IT support company.....3

How To Secure Your Smart Home....3

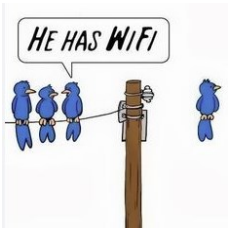
The Most Dangerous Negotiation Is The One You Don't Know You're In.....4

Is The "Ad-Free" YouTube Experience Worth The \$23/Mo?.....4

Beware of 'Malvertising' .....4

Passwords Cannot Change Themselves.....4

**Co-MIT: The Best Security For Your Company.....4**



## “(We) Won’t Get Fooled Again!” -The Who 1978

**1978** was 45 years ago now (yikes!) but we’re still playing this album on vinyl and singing the same old tunes.



Music, overall, is much like network security in that the culture changes over time but we still hang on to the classics.

In 2023, threat actors are (again) expected to come up with new ways to hack into networks world-wide, big and small, (see *How Will Cybersecurity Change In 2023* on page 2), as they have in years past- and there’s really no telling what they’ll come up with– but **their tactics won’t change enough in 2023 to thwart today’s cybersecurity best practices.**

Keeping a network safe is not terribly complicated but it takes a proper amount of expertise, proficiency, tools and common sense to do it well.

**The best thing to remember** is to subscribe to the “classic” ideals- the basic, tried-and-true practices of cybersecurity. They are your best bet to get your company through the next 24 hours without a cyber-incident. The plan isn’t complicated, but it takes focus and consistency to properly implement.

### 1. Employee Phishing Email Training and Security Culture

If your employees have not had \*any\* security awareness training, it should be your immediate focus to enroll every staff member who uses a company device or a company email address into a phishing email training course.

After that, **provide continuous training.** Fortify your network, starting with the

Training on one-time passwords and requesting/sending credentials via Teams or Slack is imperative.

### 2. Utilize A Managed Service Provider

Hire a Managed Service Provider (MSP), (or an in-house IT department– not just one part-time guy). It’s best to account for them in the budget and forget about it.

In this day and age, the companies that take their cybersecurity seriously are the **companies that will survive the next 5 years** without a major cyber attack.

It may sound blunt, but it is the very real, ugly truth. Hackers are obviously after the large businesses, but they know that most small-medium businesses usually cannot find the value in allocating funds to IT resources– they KNOW this. A hundred small fish bring the same bounty as one big fish.

Today, EVERY company needs an advisor and someone watching the network at all times-it doesn’t matter if it’s in- or out-sourced, just make sure they have the knowledge, experience and time to do a good job.

### 3. Back Up Your Data Make a copy. \*AND\* make a copy of the copy.

Is your server hosted in the Cloud? Perfect. Is THAT copy being backed up at another location? Doubtful.

Backing up company data should be prioritized right up there with payroll.



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

## HOW CYBERSECURITY WILL CHANGE IN 2023

We predict a rise in automotive hacking, "Hacking (for kids!)", ransomcloud attacks, work-from-home cybersecurity becomes a top priority, the introduction of SASE and wide-spread Zero-Trust adoption.

### **Our Mission**

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

The automotive hacking community is growing as many vehicles are now equipped with wireless and other cyber vulnerabilities. Hackers can control the steering, breaks, doors, locks, wipers, open/close the trunk or shut down [start] the engine. The future of most modern vehicles is destined to be fully controlled by computer and the internet which makes these sophisticated systems hyper-exposed to hacking threats.

Next, I call this "Hacking (for kids!)" because a 10-year old could literally purchase a ransomware kit, infect/encrypt a real company's data and demand ransom as easily as using an Easy Bake Oven. Banking and Finance, Energy/Utilities, Education, Government and Manufacturing will remain the Top 5 Most Likely Ransomware Targets. (Can you imagine a child holding Amazon for ransom?)

**EMERGENCY**

(630) 406-8969



Do you feel safer using apps in the Cloud? In ransomcloud, cybercriminals block data or the use of applications that are in the Cloud and then demand a ransom to let the organization recover access. They design malware that is specifically designed to be used in the Cloud and it has become highly sophisticated.

In the aftermath of "the plague", many businesses are realizing a priority to focus on increased remote security for their work-from-home workforce. More than ever, personal devices are being used to remotely connect to work networks and a new set of challenges have emerged.

### Coming up in the next issue:

- 2FA Bypass & Credential Stuffing
- **FREE REPORT:** "The CEO's Guide To Co-Managed IT"

SASE (*pronounced "sassy"*) —or secure access service edge— is a network architecture that combines VPN and SD-WAN capabilities with cloud-native security functions such as secure web gateways, cloud access security brokers, firewalls and zero-trust network access. These functions are delivered from the cloud and provided as a service. SASE reduces complexity, improves speed and agility, enables multi-cloud networking and secures the new SD-WAN enabled architecture.

**SECTION179** **.ORG**

Visit [section179.org](https://section179.org) for info.

Don't forget to get all those tax breaks in for the computer hardware and software you purchased in 2022!

As a whole, the manufacturing sector will adopt zero-trust to close the IT and operational technology (OT) gaps that keep them open to attack. The global economic impact of OT cyberattacks is projected to reach \$50 billion in losses this year. Manufacturer's vulnerabilities are becoming more widely known due to rapid growth of new endpoint technologies including IoT, IIoT and remote sensing devices to deliver real-time data. More than half of cyberattacks on manufacturers in 2023 will target those companies without zero-trust controls.

## Ready To Onboard?

*What to expect during the first 30 days of your relationship with a new IT support company*

I can only speak to how *\*our\** client onboarding process goes but all IT firm starts should look something like this...

**Day 1**— Install the RMM and EDR. Expect a tech on-site and have all devices available. On Day 1, a tech will install remote monitoring and maintenance (RMM) and endpoint detection and response (EDR) on every computer. Like an I.V. and monitor at the hospital, all devices are now being monitored by the IT company and they can intervene in case of a breach.

**Days 1-5**— The IT firm will run an in-depth scan of your network to determine number and health of all of devices connected to your network. Any adverse information will be presented to you. Firm requests email addresses for company-wide on-going phishing training (PII Protect) and desired security-levels have been reported to the IT firm.

**Days 5-10**— Any issues with the scan will have an action plan associated to it and solutions will be in progress. The first Patch Tuesday (the first round of many monthly security patches are deployed to protect your computers) should be complete by this time.

**Days 5-20**— PII Protect and ThreatLocker (zero-trust) onboarding are complete. Report any desired changes to your IT firm.

**Days 14-30** Monitoring and maintenance for all company devices is complete. All systems for on-going training are in place.

## How To Secure Your Smart Home

Most of us have those devices and gadgets around the house that makes our home a *smart home*.

With everything connected to the internet, your smart home is, you guessed it, incredibly smart!

Smart Homes use artificial intelligence (AI) and Internet of Things (IoT) technologies- such as connected sensors, lighting and meters to collect and analyze data. This data is used to optimize household infrastructure, utilities and other services to make daily life easier and more efficient.



Smart home devices like Alexa, Ring and Nest (thermostats, smoke detectors, light-bulbs, wireless speakers and more) are **all connected** to the WiFi in your home. **This makes your smart home devices a desired target for hackers.**

Advances in smart home technology since its inception has included upgrades to its security protocols. But contrary to popular belief, security for your smart devices is NOT designed for the protection of the smart device itself, but for the network it is connected to.

If one of your smart devices is hacked, **the hacker can leapfrog onto the other devices in your home**, including your computers if everything is connected to the same wireless network (WiFi).

That is why cybersecurity experts, like us, **recommend using 2 WiFi networks** in your home. One for the smart home devices, One for the computers.

Now, the decision for which of these networks to connect your phones to is a bit more complicated of a question. It will depend on how your specific smart home devices are managed and how they communicate with each other.

If you're making this change, we can help you make a decision that is best for your situation.



**M365 Office will require 2FA as of January 2023** affecting millions of email users worldwide. If you do not already have 2FA enabled, you will be directed to enable it on your next sign-in.

Most people already use 2FA for Amazon and banking apps— M365 2FA is the same,

**For the BEST security, choose the Authenticator option to view your OTP** (one-time password). You will need to download the Authenticator App. If you're lazy about security, you can choose the SMS option to receive a text message.

P.S. Hackers are getting around 2FA with credential stuffing. See February DataGrams to learn how to avoid getting caught up in this type of attack.



### ■ 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!

### ■ The Most Dangerous Negotiation Is The One You Don't Know You're In

How do you know whether or not you're in a negotiation? If you want or need something from the other side—or vice versa—you're negotiating. They say it's best to be nice to someone who can hurt you by doing nothing.

### ■ Would You Pay \$22.99 For An Ad-Free YouTube Experience? (Yet another subscription?)

The price just increased from \$17.99 in November. Since YouTube search is the #2 way people find information (of course Google is #1) it seems to be the most convenient and efficient option to pay to avoid the 30 second, 5 minute, (30 minute!) ads without taking the time to "skip ads". And some, are not skippable. For many of us, time and uninterrupted concentration is more valuable than the \$5-odd dollars per week. We're on board.

### ■ Beware of Malvertising

Hackers are placing malware in what seems to be legitimate ads on search engines. Notice the 1-3 advertisements that pop up when you search? Be sure to double-check if you are clicking on an ad or the genuine website by checking the margins around the headline. An advertisement will say "Ad" or "Advertisement". Once you click, malware could be silently infiltrating your device or it could take you to a real-looking website asking for your credentials. Malvertising is a portmanteau of 'malware' and 'advertising'.

### ■ Passwords cannot change themselves

How can you tell if someone has hacked into your Wi-Fi? If you are having trouble logging into your router's admin setting (and you're absolutely sure you haven't just forgotten your password), that is an immediate sign that your router has been hacked. Since passwords cannot change themselves, a hacker likely used some kind of password hack to break your router's settings.



# Co-Managed IT



## What If Your Internal IT Department Is Overwhelmed, Unable To Keep Up And Facing Projects They Cannot Handle On Their Own, Putting You At Risk For A Significant, Expensive IT Failure?

I know you're tempted to think, "We don't need more IT. Our internal IT department has it handled."

Fact is, your IT department might not be as prepared and capable as you may think to handle the rising complexity of IT systems for your growing company and the overwhelming sophistication of cyberthreats with the current resources, time and skill sets they have.

If true, **your organization IS AT RISK for a significant IT failure**.

To be crystal clear, I'm not suggesting your IT lead and staff aren't smart, dedicated, capable, hardworking people. Fact is, nobody likes to go to the CEO with "bad news" or to constantly ask for more money or help, particularly if they've already been told "there's no budget." Further, it takes a small army to run an IT department for a company of your size and growth – and you may be unfairly expecting too much of them, setting them up for failure.

**If (when?) your company is breached and your IT department doesn't have the requisite knowledge and/or resources to correct it, you can't blame them**

You're big enough to need a professional-grade IT department but can't afford to add significant overhead in IT tools and staff – particularly IT specialists with skills and tools that are only needed part-time.

That's where we can help!

- We don't replace your IT staff, we add to their skill set.
- **This is NOT** about taking over your IT leader's job or replacing your IT department.
- You don't need to add to your head count
- Your IT team gets instant access to the *same* powerful IT tools we use to make them more efficient.
- "9-1-1 On-Site" in the unexpected event your IT leader was unable to perform their job or a disaster were to strike.
- **You Get A TEAM** of smart, experienced IT pros. No one person can know it all.
- Stop worrying (or worry less!) about falling victim to a major cyber-attack, outage or data-erasing event.

**Contact Pam to sign-up or upgrade to Co-MIT today!**

Scan To Sign Up For Our  
**Weekly IT Security  
Tips**



to receive timely, relevant  
cybersecurity tips and news  
via email  
**every Tuesday morning**