# INTEGRATION
## We Simplify I.T.

*"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"*

ISSUE 5 ■ VOLUME 122 ■ MAY 2021

## What's New



This monthly newsletter is provided courtesy of Kevin Bowling, CEO of Integration.

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*!

Call us and put an end to your IT problems finally and forever!"

# Ensuring Security Across Your Remote Workforce

## 1 Year Later—Let's Make Sure You Have It ALL Covered

The COVID-19 crisis as we have seen has been with us for a while. Organizations and their employees was forced to make tough decisions rapidly, and enabling a remote workforce is one of those decisions. There are risks involved in accomplishing this at speed, but the security of your networks, devices and data shouldn't be among them. One year later have you checked your network for security breaches?

**Comprehensive Visibility.** Knowing who and what are on your network is foundational to proactive security management. It is critical to have complete visibility of every device connecting to the network regardless of where it is connecting from.

**Highest Level of Security**. 100% cloud -delivered security architecture ensures that you can protect every workload everywhere, including workloads outside of the firewall, even if they are offline, and provide real-time security functionality with the highest level of efficacy along with compliance status information. Threat hunting across every device, especially those that are not on the network, is critical.

**Cost-Effectiveness.** Architecture that is built for the cloud from the ground up flexes with the demands of customers and provides enormous storage and computing power to drive real-time protection, regardless of where your employees are connecting from. Working with a cloud security architecture ensures that additional resources can be provisioned as needed.

Globally, 50% of employees are working outside of their main headquarters for at least 2.5 days per week, according to the latest International Workplace Group report. However, COVID-19 challenging more — perhaps all — organizations to embrace a remote work style still today. Aside from the pressure this office exodus puts on IT teams, network architectures and even equipment suppliers, there are real cybersecurity challenges organizations need to consider especially now.

Six key factors that can help ensure remote worker cybersecurity:

- Make sure you have a current cybersecurity policy that includes remote working.
- Plan for BYOD (bring your own device) devices connecting to your organization.
- Sensitive data may be accessed through unsafe Wi-Fi networks.
- Cybersecurity hygiene and visibility will be critical.
- Continued education is crucial, as coronavirus-themed scams escalate.
- Crisis management and incident response plans need to be executable by a remote workforce.

We can give you help to give peace of mind that this transition was made and ensure security as you moved your workforce from office to home.

# Digital Security While Working Remotely

**Avoid public Wi-Fi; if necessary, use personal hotspots or some way to encrypt your web connection.**

Public Wi-Fi introduces significant security risk and should be avoided if possible. If you need to access the internet from a public Wi-Fi location, you have two essential problems to solve. First, other people have access to that network and, without a firewall between you and them, threat actors can pound away at your computer from across the room. Second, any interested observers on either the current network or any other public networks your data hits between you and your workplace can monitor your traffic as it goes by. It is important to find a way to protect your PC and encrypt your traffic. One good option is to use a personal hotspot from a dedicated device or your phone. Although your web traffic will be unencrypted between the hotspot and its destination, using a hot spot does eliminate the problem of getting hacked by people on the same public Wi-Fi.

For many remote access applications, you should use a VPN. VPNs provide a flexible connection to connect to different services (web pages, email, a SQL server, etc.) and can protect your traffic. Keep in mind that not all VPNs are worth the money; it's a good idea to evaluate your must-haves before you choose a VPN technology.

**Block the Sight Lines.**
If you are at a coffee shop, pay attention to your sight lines. If someone is behind you, they can see everything you are typing. Furthermore, someone with the right observational skills (like a cybercriminal) could easily watch what you are doing and identify confidential information.

# Physical Security While Working Remotely

**The things we know but sometimes just don't think about:**

**Lock Your Doors.**

This is Security 101: if you bring your work computer home or tend to work remotely, confidential corporate information could be at risk. When you get in the habit of always locking your doors, you have taken a key step toward improving your home office's security. A friend once had his work computer stolen from his 3rd floor walkup when he didn't lock the door! Don't subject yourself to the stress of a stolen work computer or harm your company by letting its data out into the wild.

In heavily regulated industries, like healthcare, losing specific data could result in huge fines.

**Never Leave Your Devices or Laptop in the Car.**

We advise our clients and employees to never leave their work computers or devices in a vehicle. It's a best practice to keep work laptops and devices on your person at all times while on the road. And the trunk of your car is not any safer. There may be criminals watching the parking lot from afar, waiting for their next victim. Putting valuables in the trunk may make life a little bit easier in the short-term - but why take that chance?

**Don't Use Random Thumb Drives.**

A classic hacking technique is to drop a number of large capacity thumb drives near the company you are hoping to attack. The chances that an unwitting employee will pick up the thumb drive and use it are surprisingly high. Anecdotally, one of our employees ran a test on this at a previous job and a shocking percentage of people actually opened the files on the drive. If you are a hacker, BINGO - that's payday.

These tips should help employees act safely with corporate devices and information no matter where they are working.

# Mobile Workforce

Staying in touch is critical for business success. Missed calls are missed opportunities. VoIP's find me / follow me feature allows Individuals to add mobile or other numbers to the user portal to make sure they are reached at a secondary number if they are not at their desk. Then, users can integrate their service with a softphone mobile app. Softphones enable VoIP calls to be made from the mobile device, but using the business caller ID. This is an important features to allow separation between the business and personal persona of the caller. With Bring Your Own Device (BYOD) becoming more popular, this allows employees and businesses a way to conduct business on a single device.

# Save Money and Switch to VoIP

Eliminate the hassle and expense of owning and operating your own phone system. With Hosted Voice over IP (VoIP), simply connect your new office phones to your existing network—and access high-quality calling, advanced features, and easy management for one low monthly price.

To understand your potential savings, how much you are currently spending — and how much you can save by switching to a Cytracom VoIP solution by Integration just contact us today at karen@integration-llc.com or call for an appointment, 256-536-5805.


# 4 Cyber Security Myths Business Owners Need To Know


**Myth:** Cyberattacks only come from external sources.

**Reality:** Upward of 60% of data breaches can be traced back to employee error. They may leave sensitive data on unsecured hardware rather than behind digital walls. They may open malicious files that copy and send data to an external location. Employee IT security training goes a long way to fix this.

**Myth:** Simple antivirus software or firewalls are enough to protect your business.

**Reality:** Cybercriminals use sophisticated tools to get what they want. The fewer security solutions you have in place, the easier it is. Antivirus software can't do anything to stop a motivated hacker, and firewalls should never be considered a primary line of defense. Web scanning and malware detection software can give you more protection on top of these.

**Myth:** Your business is too small or niche to be a target.

**Reality:** Cybercriminals don't care about the size or type of your business. They target everyone because they know they'll eventually break through somewhere. Small businesses are more appealing because they often lack serious cyber security solutions.

**Myth:** You don't collect payment or financial data, so you aren't worth targeting.

**Reality:** They aren't just looking for credit card details. They want usernames, passwords, e-mail addresses and other personal identifying information they may be able to use elsewhere because people have a bad habit of reusing passwords for other accounts, including online banking. *Inc.*

## Computer Service

⇒ Pro-Active Customer Care
⇒ Onsite Computer Service/Support
⇒ Network Management/Support
⇒ Network & Server Installations
⇒ Network Security & Firewalls
⇒ Cloud Solutions & Hosted Email
⇒ Secure Remote Access / VPNs

## Healthcare Services Provided

⇒ Medical, Dental, Radiology
⇒ Software & Hardware Integration
⇒ Security Solutions

## Backup & Disaster Recovery

⇒ Business Continuity
⇒ Secure & Compliant Offsite Backup
⇒ HiTech BDR

## Specialize in DFAR planning

## Email, Web & Archiving

⇒ Spam Filtering
⇒ Email Hosting
⇒ Email Encryption & Archiving
⇒ Website Hosting
⇒ Customer Hosting Server

## VOIP (Hosted)

## *Quotes and Jokes*

*Hope you enjoy the day...*


**"Well, it's not the worst I've seen."**


# Integration

Po Box 5526
Decatur, AL 35601
Phone: 256.536.5805


**Ask us about—Managed Services**

How would you like to pay a flat rate and have us take 100% responsibility?

How would you like new equipment, service and support for a flat rate and refresh every 3 years?