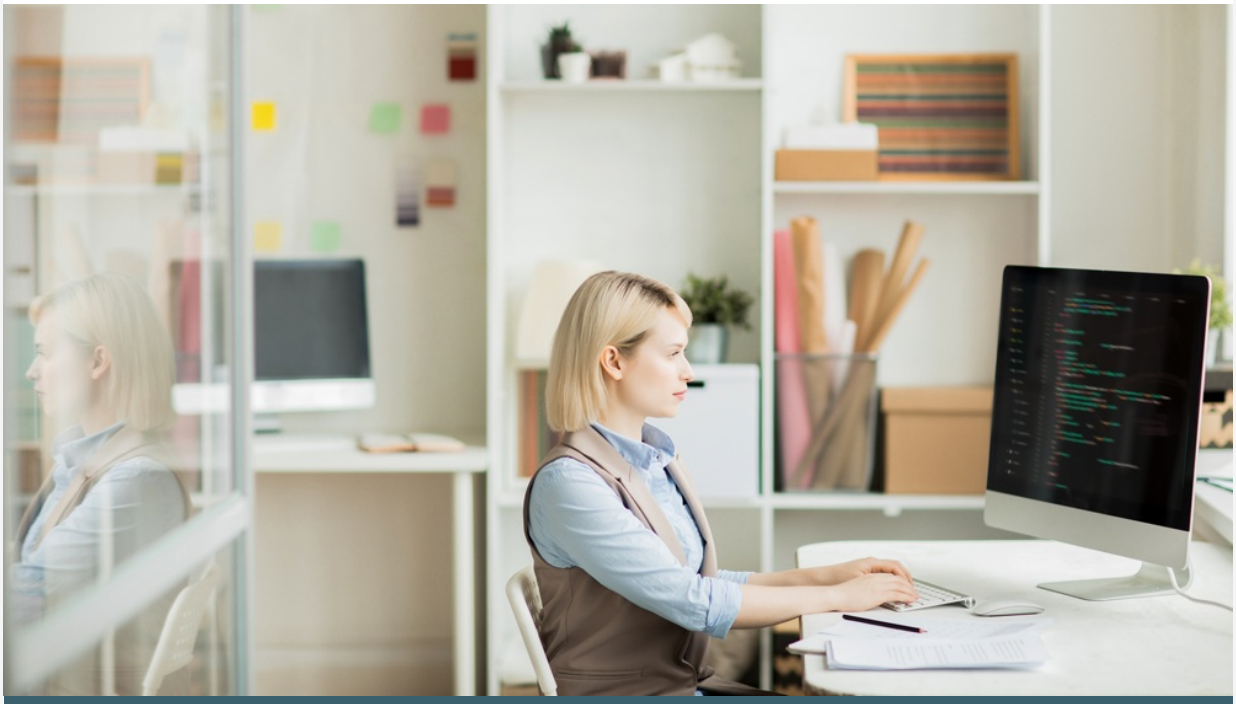
TECHNICAL FRAMEWORK
MANAGED IT & CYBERSECURITY

(970) 372-4940
info@techframework.com
https://techframework.com



TECH INSIDER

Run your business more effectively with our insider advice and techniques for IT.

2022

October

Inside This Issue

SMALL BUSINESSES ARE ATTACKED BY HACKERS 3X MORE THAN LARGER ONES

Have you felt more secure from cyberattacks because you have a smaller business? Maybe you thought you couldn't possibly have anything that a hacker could want? Or perhaps you didn't think they even knew about your small organization.

Well, a new report out by cybersecurity firm Barracuda Networks debunks this myth. Their report analyzed millions of emails across thousands of organizations. It found that small companies have much to worry about

regarding their IT security.

Barracuda Networks found something alarming. Employees at small companies saw 350% more social engineering attacks than those at larger ones. It defines a small company as one with less than 100 employees.
This trend puts small businesses at a higher risk of falling victim to a cyberattack. We'll explore why below.

Why Are Smaller Companies Targeted More?

There are many reasons why hackers see small businesses as low-hanging fruit. And why they are becoming larger targets of hackers intending to score a quick illicit buck.

Small Companies Tend to Spend Less on Cybersecurity

When you're running a small business, it's often a juggling act of where to prioritize your cash. You may know cybersecurity is essential, but it may not be at the top of your list. So, at the end of the month, cash runs out, and it's moved to the "next month" wish list of expenditures.

Small business leaders often don't spend as much as they should on their IT security. They may buy an antivirus program and think that's enough to cover them. But with the expansion of technology to the cloud, that's just one small layer. You need several more layers for adequate security.
Hackers know all this and see small businesses as an easier target. They can do much less work to get a payout than they would by hacking into an enterprise corporation.

Every Business Has "Hack-Worthy" Resources

Every business, even a 1-person shop, has data worth scoring for a hacker. Credit card numbers, SSNs, tax ID numbers, and email addresses are all valuable. Cybercriminals can sell these on the Dark Web. From there, other criminals use them for identity theft.

Here are some of the data that hackers will go after:

- Customer records
- Employee records
- Bank account information
- Emails and passwords
- Payment card details

Small Businesses Can Provide Entry Into Larger Ones

If a hacker can breach a small business's network, they can often make a more significant score.

Many smaller companies provide services to larger companies, including digital marketing, website management, accounting, and more.

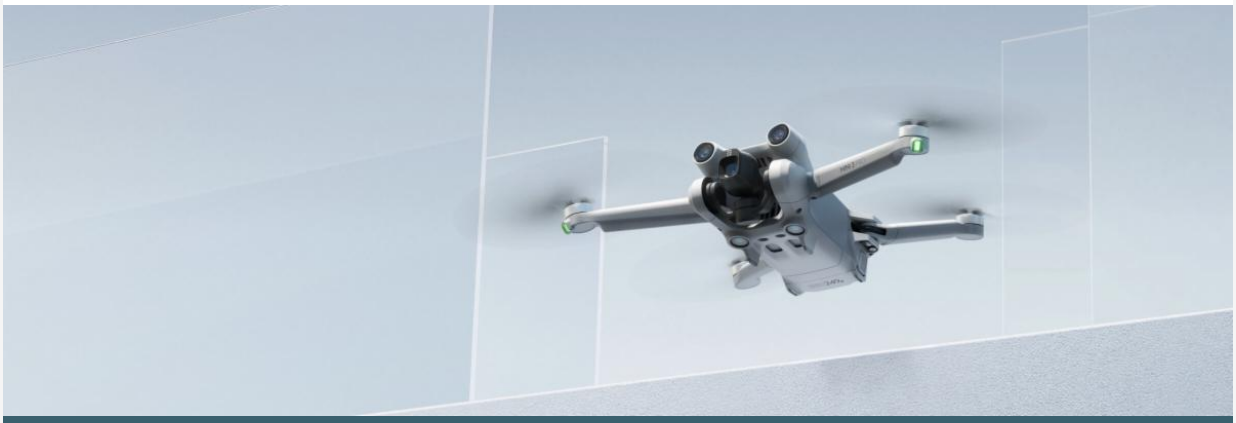
Vendors are often digitally connected to their client's systems. This type of relationship can enable a multi-company breach. While hackers don't need that connection to hack you, it is a nice bonus.

This type of relationship can enable a multi-company breach. While hackers don’t need that connection to hack you, it is a nice bonus.

Small Business Owners Are Often Unprepared for Ransomware

Ransomware has been one of the fastest-growing cyberattacks of the last decade. So far, in 2022, over 71% of surveyed organizations have experienced ransomware attacks.

The percentage of victims that pay the ransom to attackers has also been increasing. An average of 63% of companies pay the attacker money in hopes of getting a key to decrypt the ransomware.



DJI Mini 3 Pro

Lightweight, portable and, best of all, doesn’t require registration in most countries. Plus, its foldable design enables you to take it virtually everywhere with ease.

Includes forward, backward, and downward vision sensors and can avoid obstacles in complicated environments.

Extended flight time of up to 34 minutes and up to 25 km flight distance to cover your aerial photography needs.

Find yours at: https://www.dji.com

View Video

THE BIGGEST VULNERABILITIES THAT HACKERS ARE CURRENTLY EXPLOITING

Software vulnerabilities are an unfortunate part of working with technology.

A developer puts out a software release with millions of lines of code. Then, hackers look for loopholes that allow them to breach a system through that code.

The developer issues a patch to fix the vulnerability. But it's not long before a new feature update causes more.

It's like a game of "whack-a-mole" to keep your systems secure.

Without ongoing patch and update management, company networks are vulnerable. And these attacks are completely avoidable.

82% of U.S. cyberattacks in Q1 of 2022 were due to exploiting patchable vulnerabilities.

What new vulnerabilities are lurking in products from Microsoft, Google, Adobe, and others?

We'll go through several. These were recently noted in a warning by the Cybersecurity and Infrastructure Security Agency (CISA).

Make Sure to Patch Any of These Vulnerabilities in Your Systems

Microsoft Vulnerabilities

• CVE-2012-4969: An Internet Explorer vulnerability that allows the remote execution of code.
• CVE-2013-1331: This Microsoft Office flaw enables hackers to launch remote attacks.
• CVE-2012-0151: This Windows vulnerability allows user-assisted attackers to execute remote code.

Google Vulnerabilities

• CVE-2016-1646 & CVE-2016-518: These Chrome & Chromium engine vulnerabilities both allow attackers to conduct denial of service attacks.

Adobe Vulnerabilities

• CVE-2009-4324: This is a flaw in Acrobat Reader that allows hackers to execute remote code via a PDF file.
• CVE-2010-1297: A Flash Player vulnerability that allows remote execution and denial of service attacks. (Flash Player is no longer supported, so you should remove it).

Netgear Vulnerability

• CVE-2017-6862: This router flaw allows a hacker to execute code remotely.

Cisco Vulnerability

• CVE-2019-15271: This vulnerability impacts Cisco RV series routers, and gives a hacker "root" privileges.

Patch & Update Regularly!

These are a few of the security vulnerabilities listed on the CISA list. You can see all 36 that were added at https://www.cisa.gov

How do you keep your network safe from these and other vulnerabilities?

You should patch and update regularly. Work with a trusted IT professional (like us) to manage your device and software updates.

This ensures you don't have a breach waiting to happen lurking in your network.

WHAT IS MICROSOFT DEFENDER FOR INDIVIDUALS?

When you hear about Microsoft adding security apps to M365, it's often the business versions. But the pandemic has changed the way that we see the workplace.

It's now a world made up of several connected "mini-offices" located in employee homes. 55% of employees use their own devices and software to work from home.

The latest security offering by Microsoft is not for business plans. It's for Personal and Family users of Microsoft 365.

The Basics of Microsoft Defender for Individuals

Microsoft Defender is a new app that Microsoft 365 subscribers can download. It brings many digital protections together into one dashboard.

These include the following:

Online Security Visibility

Microsoft Defender gives you visibility into the security status of all your devices.

Device Safeguards

The app includes extra protections from online threats.

Real-Time Alerts & Recommendations

It provides real-time alerts for security. These also come with recommended actions.

What Devices Can Use It?

• Windows: Windows 10 version 19041.0 and higher
• Mac: Intel Macs from Catalina 10.15 and higher, and Apple silicon-based devices from 11.2.3 and up
• iPhone: iOS 13.0 or later
• Android: Android OS 6.0 or later

Download it for free at https://www.microsoft.com. Just search for Microsoft Defender for Individuals on the top right.

5 MISTAKES COMPANIES ARE MAKING IN THE DIGITAL WORKPLACE

The pandemic has been a reality that companies around the world have shared. It required major changes in how they operate. No longer, did the status quo of having everyone work in the office make sense for everyone. Many organizations had to quickly evolve to working through remote means.

SAVE RECURRING EMAIL TEXT IN OUTLOOK'S QUICK PARTS

Do you have certain emails you send
to customers that have the same paragraphs of text in them?

For example, it might be directions to your building or how to contact support.

Stop retyping the same info every time.

Overcoming the challenges and reaping the benefits takes time and effort. It also often takes the help of a trained IT professional, so you avoid costly mistakes such as:

• Poor Cloud File Organization
• Leaving Remote Workers Out of the Conversation
• Not Addressing Unauthorized Cloud App Use
• Not Realizing Remote Doesn't Always Mean From Home
• Using Communication Tools That Frustrate Everyone

Outlook has a feature called Quick Parts that saves and then inserts blocks of text into emails.

• Create a Quick Part by highlighting the text to save in an email.
• On the Insert Menu, click Quick Parts.
• Save Quick Part.

When ready to insert that text into another email, just use the same menu.

Then click to insert the Quick Part.

INTERNET EXPLORER HAS LOST ALL SUPPORT (WHAT YOU NEED TO KNOW)

After being the main entry to the internet in the late 1990s and early 2000s, Internet Explorer (IE) is gone. As of June 15, 2022, Microsoft dropped the web browser from support.

To ease the transition away from Internet Explorer, Microsoft added IE Mode to Edge. This mode makes it possible for organizations to still use legacy sites that may have worked best in IE. It uses the Trident MSHTML engine from IE11 to do this.

If you haven't yet addressed old copies of IE on your computers, your network could be at risk due to vulnerabilities in the browser no longer being fixed. Here's what you should do:

Migrate Browser Data to Microsoft Edge from IE

1. Uninstall the IE Browser
2. Ensure Employees Know How to Use IE Mode in Edge
3. Train Employees on Microsoft Edge Features