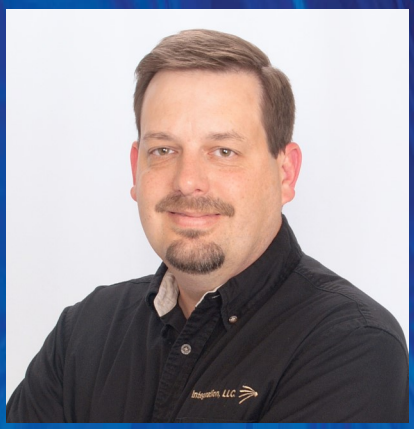
INTEGRATION
WE SIMPLIFY I.T.

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

ISSUE 3 ■ VOLUME 12 ■ MARCH 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!"

Top Ways To Protect Your Business From The #1 Security Threat You Face

Today, cybercrime is more than a potential threat facing your business. It's an unavoidable force of nature.

"It's just like preparing for hurricanes, earthquakes or any type of natural or man-made disaster that could create business continuity issues," says Theresa Payton, the Fortalice Solutions CEO and former White House CIO, in an interview with Cybercrime Magazine. "[It's the] same thing with a digital cyber-event." For many of us, it's easy to imagine these kinds of things happening to "the other guy" and not us. The problem is that cybercriminals go after everyone. They cast a wide net because that gets results.

In fact, according to Roger A. Grimes, 11-year principal security architect for Microsoft and cyber security columnist and speaker, "Eventually every company is hacked." After decades consulting for many businesses, he's come to the conclusion that "every company is completely and utterly owned by a nefarious hacker or easily could be."

Owners of small and midsize businesses might imagine that – lucky us! – we don't have enough cash to justify some faceless hacker's effort. We'd be wrong. The reality is around half of cyber-attacks go after small businesses. These don't really get reported by the media. They're not as flashy as a cyber-attack against a big bank or retailer. But it's the attacks against small businesses that do the most damage. One 2016 study found that 60% of small businesses hit with a cyber-attack closed within six months.

Thankfully, it's not all bad news. While some business owners have no clue what cyber security they have in place, others are looking for ways to shore up their businesses. There are steps you can take to keep the bad guys out.

Two of the best ways to do that are to simply keep all your software up-to-date and keep your team educated about the threats. As Grimes puts it, "The two most likely reasons you will get exploited are due to unpatched software or a social engineering event where someone is tricked into installing something they shouldn't … It would be a stretch to claim every other exploit type in the world, added together, would account for 1% of the risk."

How can you keep your software up-to-date?

…..Continued on Page 2

Continued from page 1…

You can actually automate a lot of it. There are several easy-to-use tools built just for this. Many of them also let you manage your software across your entire network from one set location. Say goodbye to jumping around and coordinating updates. Even better, there are many platforms capable of updating themselves. You just want to keep a close eye on them.

More than that, it's always a good idea to put strong company policies in place. You want to be clear about your security and help inform employees about the dangers posed by malicious files and e-mails, among other things. Take time to educate them on the threats that are out there. And keep the education ongoing, because the threats are ongoing. The bad guys are always looking for new ways to break in.

And don't forget about accountability. Keep the conversation going and talk to your employees about what they know about cyber security. Some businesses go so far as including cyber security training in their onboarding. Education is everything.

Finally, you MUST partner with a highly trained, security-focused managed service provider or other IT organization dedicated to keeping you protected from these constant threats. Some businesses try to do it on their own only to realize they don't have the resources. Others think they need an entire in-house IT team to handle all of these threats.

But the fact is, by outsourcing the work, you save money while keeping out the bad guys optimizing key parts of your network and software. It's a win/win. It's all about being proactive. When you have a group of experts working every day behind the scenes, cyber security stays top of mind in your organization, whether you're thinking about it or not. Really, it's one less thing you have to stress about.

"60% of small businesses hit with a cyber-attack closed within six months."

7 Most Critical IT Security Protections:

- The #1 Security Threat To ANY Business Is… You! Like it or not, almost all security breaches in business are due to an employee clicking, downloading or opening a file that's infected.
- Require STRONG passwords and passcodes to lock mobile devices.
- Keep your network and all devices patched and up-to-date.
- Have A Business-Class Image Backup.
- Don't allow employees to access company data with personal devices that aren't monitored and secured by YOUR IT department.
- A Business-Class Good Firewall And Proper Updates.
- Protect Your Bank Account.

Mark Twain Once Said, "Supposing Is Good, But KNOWING Is Better"

If you want to know for SURE that your current IT company (or IT person) is truly doing everything they can to secure your network and protect you from ransomware, bank fraud, stolen and lost data and all the other threats, problems and costs that come with a data breach, then you need to call us for a **FREE Security And Backup Audit**.

Beware! 60% Of Businesses Lose Their Data Through These Breaches

Sneaky Ways Cybercriminals Attack Your Network

And What You Can Do To Prevent It NOW

Password Exploits:

Many people don't realize how dangerous it is to reuse the same username and/or password for everything– or to never update their passwords. It's very likely that at least one of your active passwords has fallen into the hands of hackers. They may have gotten it years ago from a website that doesn't exist anymore. But if you are still using that same username and password for other websites and accounts, you are putting yourself at risk.

According to Trace Security, nearly 80% of all data breaches are the result of simple or reused passwords. Some of the most popular passwords today include things like "12345," "password" and "qwerty." Even worse, many businesses use passwords like these to protect sensitive data such as banking information and customer records. If a password is old or easily guessed, it offers nearly the same protection as no password at all! Change your passwords at least every 60-90 days and use different but secure passwords for everything.

The great news is that it's easier than ever to protect your business from things like phishing scams, data breaches and so much more. Just because you haven't had any major problems for years, or at all, doesn't mean you should assume nothing will happen in the future. You might also think that you simply don't have the time or resources for good security.

The even better news is that you don't need to spend a lot of time or money to secure your business against hackers and cybercriminals. All you really need to do is partner with an IT services firm that knows cyber security inside out.

When you work with a dedicated IT security company, they take care of you. They can monitor your network 24/7 and make sure the bad guys don't get in. They can make sure your data is backed up to a secured server so that if anything does go wrong, you don't lose a beat. They can even provide you with round-the-clock support should you have any questions or concerns. It's a surprisingly easy and cost-effective way to protect your business and to put the cybercriminals in their place.

Recent List of Data Breaches:

- Facebook—29 Million records
- Equifax—146 Million records
- Marriott Starwood Hotels—500 Million records
- Google Plus—52.2 Million records
- T-Mobile—2 Million records

<u>Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot</u>?

Think again. 82,000 NEW malware threats are being released *every single day* and HALF of the cyber-attacks occurring are aimed at small businesses; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer *embarrassment*.

"... there was a 424% increase in the number of attacks on small businesses."

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

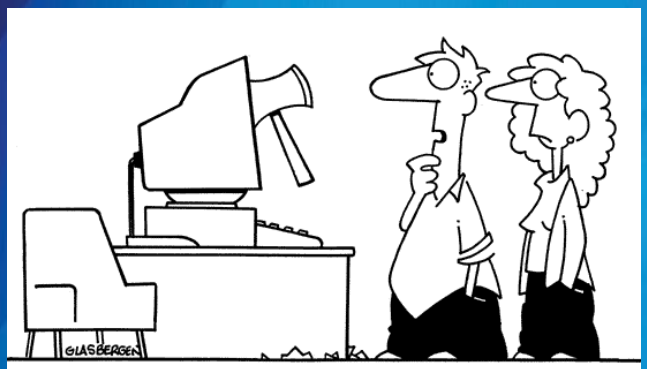
Email, Web & Archiving

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

VOIP (Hosted)

Quotes and Jokes

Hope you enjoy the day...



"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."

Only...
If it was this simple...

BUT...
We know it is not...

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?