1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

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

What's Inside

January 2022

Kim Nielsen
President &
Chief Technology
Strategist at
Computer
Technologies Inc.
(248) 362-3800

"As a business owner, 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!"

Old Technology – It's Costing You Much More Than You Think

When was the last time you updated your technology? Between your hardware and software, if you are still doing business on older technology, you could be putting yourself at risk, and it could end up costing you big. As we begin a new year, it's time to take a close look at the tech you rely on every day.

While many small businesses tend to put off major technology purchases due to the upfront costs, by doing so, you may be opening yourself up to major costs down the road. There are hidden costs that businesses don't always consider when they decide to "hold off" on investing in new equipment or the latest software.

Here are five ways outdated technology can take a toll on your business:

1. It leads to a loss in productivity. Old technology has a habit of getting slow. This means your team has to waste time waiting for their PCs to turn on and their apps to load. Even well-maintained equipment is going to wear out over time. This problem is only compounded when your team has to use software that no longer works as it once did. Eventually, programs that once worked well together start to experience hiccups, and you risk losing time and data.

2. It leads to a loss of customers. Your customers want to know your data (which may also be their data) is secure. If you're using outdated tech, there's a good chance that data IS NOT secure. One Microsoft survey revealed that 91% of consumers would end their relationship with a business that was relying on outdated technology.

3. It leads to a loss of employees. If employees have to deal with slow

Continued on pg.2

Continued from pg.1

hardware and poorly-integrated software every day, they're going to get frustrated. They're going to get even more frustrated if nothing is done about it. The end result is high employee turnover. This alone can be a huge cost for a small business to absorb.

4. It leads to a loss of support. Over time, developers stop supporting their older products so they can focus on their new products. This also means they're devoting more attention to the customers who are using the newer versions. This can leave you in the dark if you run into a problem that you need help with. You may have to call in a third-party specialist to answer your question and fix your problem, and they will charge you accordingly.

5. It leads to a loss of security. A loss in support also means you aren't going to see security patches for your aging hardware or software. This makes you highly vulnerable to all kinds of cyberthreats, including data breaches, malware infections, and all kinds of other cyber-attacks. Hackers want to break into your network, and if you're using outdated tech, you make their job much easier.

When you factor in the costs associated with these losses, it can be staggering! It's enough to put some companies out of business (and it has). After a year that has left many businesses more vulnerable than before, you should be taking steps to avoid these kinds of losses.

> **"One Microsoft survey revealed that 91% of consumers would end their relationship with a business that was relying on outdated technology. "**

Here's what you can do: as we head into a new year. Take stock of your technology. It's unlikely you have to replace everything, but look at where you are most vulnerable. What issues are your employees experiencing? What hardware or software is no longer supported? Where are the gaps in your IT security?

The great news is that you don't have to answer these questions on your own. Even better, you don't have to drop a pretty penny to make it happen! You can work with a managed service provider (MSP) like Computer Technologies, Inc. and we can help bring your business back up to speed. We can even help you identify ways to mitigate some of the cost that comes with upgrading your technology. In the end, you, your employees, and your customers **GAIN** complete confidence in your business as you head into 2022!

Free Executive Guide Download: The Business Owner's Guide To IT Support Services And Fees

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.
- **Claim your FREE copy today at https://www.cti-mi.com/itbuyersguide122/**

Security Corner

Synthetic Identity Fraud Is The Perfect Crime

Synthetic identity fraud occurs **when someone uses a combination of real and fake personal information to create an identity and commit fraud**. For example, a fraudster may combine a stolen Social Security number (SSN) with a fake name, date of birth, and address to create a new identity.

Let's look at this scenario and see if you can spot the red flags:

Steve is an up-and-coming scammer with a new scheme under his belt: he utilizes a real address (7 Smith Street) and a fake name (Steve Scammerling) to open up multiple real accounts and carry out transactions.

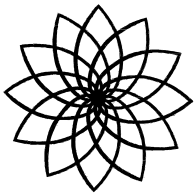
Lauren really lives on 7 Smith Street. She started receiving mail for Steve Scammerling, but thought nothing of it, and threw the junk mail in the trash. Years later, she reviewed her credit report for the first time in a while and noticed some activity that was not hers

Red Flag #1: Lauren suddenly started receiving mail to her address with someone else's name. This should have been a sign that her information was being mingled with other made-up details to commit fraud.

Red Flag #2: Lauren was not regularly checking her credit report. Had she been, she might have caught the suspicious activity much sooner.

For more information Synthetic Identity Fraud, call us at 248-362-3800 or visit us at: https://www.cti-mi.com/

With 2021 in the rearview mirror, it is time to look ahead to 2022. While you have plans to start anew this month, cybercriminals are relying on their same old tricks while also developing new ones. The start of the New Year gives us the opportunity to reflect on cybersecurity's past, and present so you can be better prepared for the future



Review past cybercrimes. By learning where others went wrong, you can avoid making the same mistakes by catching onto cyber-patterns before they catch onto you.

Anxiety Society. If you fear your personal information being compromised, you're not alone. But don't let your worries consume you. Name them, learn more about them, and conquer them.

Reflection Section

Reflection allows for stillness amidst chaos, providing space for the mind to interpret external stimuli and create external meaning.

How Does This Relate To Cybersecurity?

It's a big cyber-world our there, with a lot of information. Some of it may not feel like it relates to you at first glance. But taking the time to look further, create connections, and observe will allow you to develop a cybersecurity mindset which can then inform future actions.

Practice Reflection.

Take time to reflect and consider security tips from all angles to find key takeaways that create meaning within your own world.

Cyber Liability Insurance

With the many cyber events of 2021, many of us are distrusting about all things cyber with the start of the New Year. From ransomware attacks to headlining security breaches, cybersecurity is undeniably front and center. Although cyber liability insurance is meant to protect companies against such vicious losses, this coverage is often as clear as mud. So, let's talk about the importance of cyber liability insurance and uncloud some common cyber terminology.

Why Cyber Liability Insurance Is Vital: When employers sent their teams home to work remotely, cybercriminals saw an opportunity to pounce. Unfortunately, it took an average of 207 days to identify a breach in 2020, and the average cost of a data breach neared $4 million. So, it's no surprise that 68% of company leaders think cybersecurity risks are increasing.

Cyber Liability Insurance: 3rd Party Cyber Coverages : To provide a brief explanation, cyber liability insurance protects companies from third-party lawsuits relating to electronic activities, such as phishing scams, ransomware attacks, etc. Additionally, this coverage provides many recovery benefits, supporting data restoration and reimbursement for income lost and payroll spent. Let's first review some of the most common third-party cyber coverages:

- **Media Liability**: This part is coverage against allegations or errors and omissions in the course of your company's communication of Media Content in electronic (website, social media, etc.) or non-electronic forms (i.e., defamation, libel, slander, emotional distress, invasion of the right to privacy, and copyright infringement).
- **Network Security & Privacy Liability**: It covers against liability claims for actual or alleged failure to prevent unauthorized access to or use of a computer system. This portion also protects against the failure to prevent false communications, such as phishing, that corrupts, deletes, or damages electronic data, as well as theft of data and denial of service attacks against websites or computer systems of a 3rd party.
- **Payment Card Loss**: This portion covers fees and assessments that your company becomes legally obligated to pay due to claims involving your company's non-compliance with PCI Data Security Standards.

Cyber Liability Insurance: 1st Party Cyber Coverages: In addition to 3rd-party coverage, cyber liability provides first-party coverage. Typically, non-tech companies opt for this coverage to protect against conventional risks, such as data breaches. For example, if a business experiences a breach, they will file a claim with their cyber liability insurer providing 1st-party cyber coverage. That said, here are a few of the different coverages you should know about:

- **Cyber incident Response**: This part covers fees and costs incurred by your company and charged by a response provider to investigate an actual or suspected privacy event or system breach and to respond and notify individuals in line with local regulation.
- **Business Interruption Loss**: It covers expenses and revenue impact incurred by your company if you can't access your systems due to a system breach or denial of service attack that interrupts your company's computer system for an extended period.
- **Business Interruption – System Failure**: It covers expenses and revenue impact incurred by your company due to a non-malicious computer-related act that interrupts your company's computer system for an extended period.
- **Reputational Harm**: This part covers expenses related to a PR firm to manage adverse media publication responses to a suspected or actual hack.
- **Digital Data Recovery**: It covers the fees and costs incurred by your company to regain access to or restore/recreate any electronic data on your company's computer system, usually requiring a backup to exist.
- **Network Extortion**: This part covers expenses and payments (including ransom payments) to a 3rd party to avert potential damage from threats made against your company.

Cybercriminals are becoming more sophisticated, targeting all-size businesses with multi-tiered attacks. Nowadays, it's not *if* these hackers will come after your company; it's *when*. To read the full article, visit: https://bit.ly/3JNaTQJ