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 2023

Kim Nielsen, CISSP
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!"

Digital Accessibility: What Is It and Why Should You Care?

What is digital accessibility? You already know what "accessibility" is: From designated parking spaces to entry ramps, you can find physical evidence of how the ADA has created equal opportunities since it became law on 26 July, 1990. Just like public spaces in America, the technology that you use every day must be available to (and usable by) everyone who needs it, regardless of their disability status.

This applies to emerging technology, too. Think of the last time you went into a store or restaurant, and they expected you to self-check-out using a point of sale screen, or perhaps had one of the screens that turn around to show you a suggested tip at the register. There are ADA requirements about providing space and assistance for people to use it, like a voice that reads the screen for people or subtitles for any spoken instructions.
Now, digital accessibility expands beyond these small encounters you may have had.

Current State of Digital Accessibility
Since the inception of the American with Disabilities Act (ADA), the Internet and all the ways we access it have transformed more than anyone could imagine in the 1990s.

Subsequently, various additions to the legislation have cropped up to protect disabled Americans' equal opportunity rights while using/being in the digital world.

Do you think you have a grasp on making your online services more accessible? You might be less prepared than you think: In 2021, a stunning 98% of websites were found to be inaccessible. **That**

Continued on pg.2

Continued from pg.1

alienates approximately 61M consumers who, according to Nielsen (not me but the ratings :-)), more often stay loyal to brands that they know can provide them seamless service. It's not just about respect or compliance, but tapping the (largely ignored) market.

Necessary Next Steps

When might you need to be mindful of digital accessibility?

- Digital tools you offer to make your services easier, like 24/7 customer support
- Digital materials you might offer, like videos and how-to files
- Creating a site to attract more web traffic, but which is easy to navigate and read
- Incorporating digital accessibility into your regular compliance assessments and trainings
- Choosing suppliers with ADA-compliant services
- Removing pre-existing barriers that prevent people with disabilities from interacting with your technology as it stands today.

The precise way that this plays out in your business depends on what online services you offer, if any, and which customer touchpoints rely on digital access. Everyone, regardless of ability, should be able to access and use your digital systems – or have the necessary accommodations readily available.

> **In 2021, a stunning 98% of websites were found to be digitally inaccessible.**

Cybersecurity and Accessibility

While making changes to your various technology access points, as well as various trainings you might have in place, you want to make sure to maintain the same level of cybersecurity while still making reasonable accommodations.

In addition, mind the ways that cybercriminals might leverage these digital channels to target your customers who have disabilities and are thus using these alternative avenues to access your service. There's no reason that they should be more exposed to cyberattacks simply because they require these accommodations.

In fact, this would directly conflict with their right to equal opportunity under the ADA. It's important to extend your current cyber-defenses to cover additional forms, landing pages and integrations that you might employ to make your services more accessible, so every customer knows that you have their cybersecurity in top of mind.

Conclusion

When you address inaccessibility in your digital services, ultimately this makes the technology simpler and convenient for *everyone* who uses the device or website. Not all disabilities are visible, either; you never know who might need the extra accommodations, but who may be uncomfortable asking. There are myriad benefits, aside from compliance under the law, to improving digital accessibility in your organization.

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

IT BUYERS GUIDE

What Every Business Owner MUST Know About IT Support Services And Fees

What You Should Expect To Pay For IT Support For Your Business And How To Get Exactly What You Need

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/itbuyersguide123/

Security Corner

**New Year For Cyber Threats–
2 Things Coming Your Way In 2023**

It's the New Year! You made it through another tumultuous year full of cybersecurity threats and defenses. Bad actors developed better weapons, and security teams countered with stronger shields. You can't let your defenses down. Now is the time to start thinking about what cybersecurity threats and defenses will make headlines in 2023.

Zero Trust
Zero-day vulnerabilities are places where the attack surface (that refers to anywhere that a hacker might get into the system) is exposed in a newly-launched program or service.

To help mitigate those kinds of threats, security experts developed what's known as a **zero-trust framework**. This approach assumes your system is vulnerable *until every part of it has been examined and deemed acceptable* to use, i.e., not at risk.

Supply Chain Attacks
Going after a trusted vendor and sabotaging the service is a good way to infect all their users. Supply chain attacks, as they're known, isn't a new tactic for cybercriminals. It has, however, become a more popular method of stealing data in the past few years. Experts predict that this will hold true throughout 2023.

All of this is just a tiny peek behind the curtain of what's to come next year. Threat actors are always looking for new ways to weasel their way onto your systems and exploit you for information or money.

For more information about these and other cyber threats, call us at 248-362-3800 or visit: https://bit.ly/3X3Q6hW

What's Changing In The CyberSecurity Insurance Market?

Cybersecurity insurance is still a pretty new concept for many SMBs. It was initially introduced in the 1990s to provide coverage for large enterprises. It covered things like data processing errors and online media.

Since that time, the policies for this type of liability coverage have changed. Today's cyber insurance policies cover the typical costs of a data breach. Including remediating a malware infection or compromised account.

Cybersecurity insurance policies will cover the costs for things like:

- Recovering compromised data
- Repairing computer systems
- Notifying customers about a data breach
- Providing personal identity monitoring
- IT forensics to investigate the breach
- Legal expenses
- Ransomware payments

The increase in online danger and rising costs of a breach have led to changes in this type of insurance.

No one is safe. Even small businesses find they are targets. They often have more to lose than larger enterprises as well. The cybersecurity insurance industry is ever evolving. Businesses need to keep up with these trends to ensure they can stay protected and insured.

Demand is Going Up
The average cost of a data breach is currently $4.35 million (global average).

In the U.S., it's more than double that, at $9.44 million. As these costs continue to balloon, so does the demand for cybersecurity insurance.

Companies of all types are realizing that cyber insurance is critical. It's as important as their business liability insurance. With demand increasing, look for more availability of cybersecurity insurance.

Premiums are Increasing
With the increase in cyberattacks has come an increase in insurance payouts. Insurance companies are increasing premiums to keep up.

In 2021, cyber insurance premiums rose by a staggering 74%. Insurance carriers aren't willing to lose money on cybersecurity policies.

Certain Coverages are Being Dropped
Certain types of coverage are getting more difficult to find. For example, some insurance carriers are dropping coverage for "nationstate" attacks.

These are attacks that come from a government. Many governments have ties to known hacking groups. So, a ransomware attack that hits consumers and businesses can fall into this category.

In 2021, 21% of nation-state attacks targeted consumers, and 79% targeted enterprises. So, if you see that an insurance policy excludes these types of attacks, be very wary.

Another type of attack payout that is being dropped from some policies is ransomware. Insurance carriers are tired of unsecured clients relying on them to pay the ransom. So many are excluding ransomware payouts from policies. This puts a bigger burden on organizations.

It's Harder to Qualify
Just because you want cybersecurity insurance, doesn't mean you'll qualify for it. Qualifications are becoming stiffer. Insurance carriers aren't willing to take chances. Some of the factors that insurance carriers take into consideration:

- Network security
- Use of things like MFA
- BYOD and device security policies
- Advanced threat protection
- Backup and recovery strategy
- Administrative access to systems
- Anti-phishing tactics
- Employee security training

2 Ways To Refine Work Relationships With Young Employees

The workforce gets younger every day, which can make things more challenging for business owners. Many have recently adapted to meet the needs of new millennial employees, but now even younger generations have started to work. This has required business owners to learn how to build meaningful relationships with these new employees. Here is one way you can do this, too.

Setting Standards Early
One of the most significant concerns for business owners, especially in regard to young employees, revolves around values. It can be hard if values don't align. To avoid this situation, dive deep into this topic during the hiring process so you are well aware ahead of time.

5 VOIP Setup Tips For A More Productive Office

Companies that don't set up their VoIP system efficiently, can experience issues.

This includes things like dropped calls, low bandwidth, and features left unused.

If you've been struggling to make your cloud phone system more efficient, check out these tips below. They provide setup best practices for VoIP.

1. Check Network Capabilities
2. Set Up Departments & Ring Groups
3. Create Your Company Directory
4. Have Employees Set Up Their Voicemail & VM to Email
5. Train Your Team on the Call Handling Process

"Wheeeeeeee!"

CartoonStock.com

4 Ways to Balance User Productivity With Solid Authentication Tools

One constant struggle in offices is the balance between productivity and security. If you give users too much freedom in your network, risk increases. But add too many security gates, and productivity can dwindle.

There are ways to have both secure and productive users. It simply takes adopting some solutions that can help such as:

- Install a Single Sign-on (SSO) Solution
- Recognize Devices
- Use Role-based Authentication