the Tech Chronicle

The Official Newsletter of NorthStar Technology Services

212 W. Route 38, Suite 103
Moorestown, NJ 08057

Trusted. Reliable. Secure.

The Official Company Newsletter of NorthStar Technology Services

IN APRIL'S ISSUE

Let's Connect:

northstartechs

northstartechs

NorthStar Technology Services

NorthStar Technology Services

www.northstarsvc.com

(856) 375-1220

info@northstarsvc.com

APRIL 2023 | VOL. 7

the Tech Chronicle

The Official Company Newsletter of NorthStar Technology Services

What Compliance Standards Does Your Business Need To Maintain?

Understanding HIPAA, NIST And CMMC

Maintaining compliance standards is crucial for any business seeking profitability, respect, and legal safety. Not only does it help you avoid legal issues and fines, but it also shows that you're a trustworthy and respectable company. On the other hand, prioritizing compliance promotes ethical conduct and safeguards the rights of your employees, customers, and other stakeholders, ultimately benefiting your business in the long term.

As a business owner or leader, it may be challenging to determine which compliance standards apply to your industry or specific business. Although Occupational Safety and Health Administration standards for workplace safety are a must-follow for most businesses, Environmental Protection Agency regulations for environmental protection must also be met. Additionally, there are compliance requirements concerning the information stored and shared. If you fall under this category, you should be aware of three other compliance standards.

Health Insurance Portability And Accountability Act (HIPAA)

If you've visited a doctor's office in the past twenty years, you're probably familiar with HIPAA. This law was established in 1996 to safeguard the confidentiality and security of individuals' personal health information. HIPAA solely applies to "covered entities," such as health care providers, health plans, and health care clearinghouses. These entities must adhere to HIPAA's guidelines when dealing with protected health information. They must implement administrative, technical, and physical measures to maintain the privacy, accuracy, and availability of this data. During the Covid-19 pandemic, there was uncertainty surrounding HIPAA, resulting in confusion. Some employees claimed that their employers' request for their vaccination status breached HIPAA, which is incorrect since HIPAA only pertains to covered entities. For individuals working in the healthcare sector, it's crucial to have a thorough understanding of HIPAA. Failing to comply with its regulations can lead to penalties, legal complications, and even the revocation of medical practice licenses.

National Institute Of Standards And Technology (NIST)

The NIST, a department under the United States Department of Commerce, is a nonregulatory agency that formulates and encourages standards, recommendations, and optimal approaches to guarantee the security and privacy of information systems. NIST compliance is crucial for entities that handle confidential data, such as financial information, personal data, or intellectual property. In industries like healthcare, finance, and government, which have strict regulations, NIST compliance becomes even more significant. By complying with NIST guidelines, organizations can safeguard against cybersecurity threats, data breaches, and other security breaches while also meeting the regulatory obligations set by HIPAA.

Conforming to NIST standards will enable you to easily pinpoint weaknesses, refine incident response strategies, and prioritize security measures. The NIST has developed a valuable framework, along with numerous publications that offer recommendations for various systems and situations. If you're seeking a specific publication or would like to explore additional NIST resources, visit their website, NIST.gov, for more details.

Continued on pg. 2

CLIENT SPOTLIGHT

specialty fabricators
CUSTOM GROCER FIXTURES

SPECIALTY FABRICATORS

Have you ever wondered who makes that beautiful refrigerated display in your local grocery store? Well, chances are it was made right here in South Jersey by none other than **Specialty Fabricators**. They specialize in custom grocer fixtures and have been in the game since 1995! Based in Wrightstown, Specialty Fabricators are leaders in design and creation, setting the standard in high performance & durability while continuously outperforming their clients' expectations. Although their core competency is in custom fixtures, they offer their clients' a vast array of standard equipment that's competitively priced and of the highest integrity. Specialty Fabricators have the resources and expertise to provide equipment solutions for an **entire grocer**. As a privately held, family owned and operated company, they have enjoyed the flexibility to place their clients' needs first and continually deliver the highest in quality displays. Specialty Fabricators have been a valued client of NorthStar's since 2015!

This monthly publication is provided courtesy of **Eric Williams**, the CEO, Owner, & Founder of NorthStar Technology Services located in Moorestown, NJ.

NORTHSTAR
TECHNOLOGY SERVICES, LLC

Our Mission:

To build a community of successful-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

We are proud to have served the greater Philadelphia Metro Area since 2008.

Continued from pg. 1

Cybersecurity Maturity Model Certification (CMMC)

The CMMC, a framework developed by the U.S. Department of Defense, evaluates and certifies the cybersecurity practices of organizations working with the DoD. It outlines controls and processes that organizations must follow to safeguard sensitive information and systems from cyber threats. The CMMC applies to defense contractors, suppliers, subcontractors, and service providers such as IT, logistics, and engineering. Manufacturers, technology firms, and professional service providers supporting the defense supply chain must also adhere to CMMC guidelines. Non-compliance with CMMC certification may result in losing the opportunity to bid on or win DoD contracts.

No matter the industry, compliance is essential for any business to succeed. It's a smart move to begin by checking out major regulations like HIPAA, NIST, and CMMC to determine their relevance to your business, and then expand your search to other applicable regulations. By taking this step, you'll be setting your business up for success and ensuring that you're keeping up with the latest requirements for your industry.

Tech Tip Recap

Simplify Your Presentation Process

Open your PowerPoint in presentation mode by saving the format as .PPS instead of .PPT

Creating Strong Passwords

Sign up for a password manager, keep the password length long, and create variety in the characters you use (Lik3 th!S) for the best password protection.

Clean Up Your Inbox

We've got a short list for cleaning:

1. Delete old mail
2. Create folders
3. Use filters for incoming mail
4. Unsubscribe from old lists
5. Use 3rd party spam blockers
6. Create a "spam" email account
7. Schedule monthly cleaning time!

Follow Our Socials For Weekly Tech Tips!

Are You Addicted To Work?

Here Are Some Ways To Help Take Your Life Back

If you think this isn't for you... it probably is.

As a business owner or entrepreneur, you may feel compelled to dedicate all of your time and energy to your business in order to ensure its success. However, this can easily turn into an addiction that is detrimental to your mental health. Recent studies have shown that working excessive hours can lead to burnout, chronic stress, and strained relationships, which can negatively impact both your personal and professional life. If you find yourself spending too much time at work, there are steps you can take to address your work addiction.

First and foremost, it's important to **reassess your goals**. Ask yourself why you're working so hard and what you hope to achieve. Are your goals realistic, or are you pushing yourself too hard in pursuit of an unattainable dream? Reflecting on your goals can help you determine if they are still what you want for yourself and your business. If not, it may be time to adjust your goals and set new ones.

Another effective way to combat work addiction is to **trim your task list**. Trying to accomplish too much in a single day can often lead to working long hours and feeling overwhelmed. Take a step back and consider what you can realistically achieve in a typical workday. Don't overload yourself with tasks and responsibilities, and if you have a team supporting you, delegate some of the less important tasks to them. Remember, you don't have to do everything on your own in a single day. Its much better to ask for help before things get to the point where even their help isn't enough to assist you anymore.

It's also hugely important to **prioritize your time and schedule breaks throughout the day**. Taking regular breaks can help reduce stress and prevent burnout, which in turn can help you be more productive and focused when you're working. This extends past the office... just as work life has the potential to impact home life, home life can (and will) do just the same, if not more, to your work life.

Take time to **get enough sleep**... whatever that looks like for you. If you know you need the full 8 hours, prioritize it. If you do well with 6 or 7, take that extra time and dedicate it to other life-giving activities, such as family and friend time, exercise, and hobbies. The "grind" is great, and often necessary for progression and business growth. But you won't even be able to push through if the foundation, your home health, is **not** thriving.

It's essential to **establish clear boundaries between work and personal life**. This could mean setting specific work hours and sticking to them, avoiding checking work emails or taking work calls outside of those hours, or designating certain days of the week as "no work" days.

While it's understandable to want to dedicate yourself to your business, it's important to maintain a healthy work-life balance to avoid burnout and other negative consequences. By reassessing your goals, trimming your task list, prioritizing your time, taking regular breaks, and making time for yourself, you can combat work addiction and achieve a healthier, more fulfilling life.

Comic Corner

"Burnout was our greatest challenge until we changed our mission statement."
CHILL
© Randy Glasbergen / glasbergen.com
GLASBERGEN

Data Backup Is Not Enough.

Since the days of floppy disks, the importance of backing up data has been widely recognized due to the risk of data loss caused by hard drive crashes, viruses, and other mishaps. Data loss has become a common experience for most individuals using any form of technology. In the United States, about 140,000 hard drive crashes occur each week, and every five years, 20% of SMBs suffer data loss due to a significant disaster. This has led to the growth of a robust cloud backup market. However, one major change that has occurred with data backup in recent years is the issue of security. Simply backing up data is no longer enough; data protection is now the norm.

Data protection refers to the need for backups to have robust cybersecurity protection to mitigate the threat of attacks such as sleeper ransomware and supply chain attacks. While cloud-based backup is convenient, accessible, and effective, there is a need for certain security considerations with online services. Companies must prioritize data protection when planning a backup and recovery strategy. The tools used must protect against the growing number of threats to backups.

Modern threats to data backups include:

- Data center outages
- Sleeper ransomware
- Supply chain attacks
- Misconfiguration of security settings

To ensure adequate data protection, a backup solution should have the following features:

- **Ransomware prevention** to restrict automated file changes for documents.
- **Continuous data protection** to back up files as users make changes and mitigate data loss if a system crashes before the next backup.
- **Threat identification**, which is a type of malware and virus prevention tool that identifies malware in new and existing backups to stop sleeper ransomware and similar malware from infecting all backups.
- **Zero-trust tactics**, such as multi-factor authentication and application safelisting, are critical security measures promoted by cybersecurity professionals worldwide.

It's important to note that data protection is not just the responsibility of IT departments or backup solution providers. End-users should also take steps to protect their data, such as ensuring their devices are up to date with the latest security patches, using strong passwords or multi-factor authentication, and avoiding clicking on suspicious links or opening attachments from unknown (or even potentially "known") sources.

By working together, IT departments, backup solution providers, and end-users can help safeguard against modern cybersecurity threats and ensure the continuity of critical data.

To protect against modern cybersecurity threats such as ransomware, supply chain attacks, and misconfiguration, data backup solutions need to evolve from simple backup to comprehensive data protection that includes features such as continuous data protection, threat identification, and zero-trust tactics.

ITS TIME FOR...

Tech Trivia

It's time for Tech Trivia where we ask our readers a question! The answer is posted under the month's newsletter PDF on our website newsletter page, found under the "Resources" tab.

The question this month is:

In what video game series did Microsoft's virtual assistant Cortana make her debut?

Why Aren't Employees Reading My Emails?

How often do you send emails to your team? Have you ever had an employee stumble over a previous message you sent? It happens to the best of us. But before you blame them for not paying attention, consider these reasons why they might be "missing" your emails:

- **Timing**: Sending emails at the end of the day may cause them to be overlooked.
- **Overload**: Too much information can be distracting, so keep emails short and sweet.
- **Clarity**: Make sure your employees know what's expected of them when it comes to reading your emails, and keep content relevant to their role.