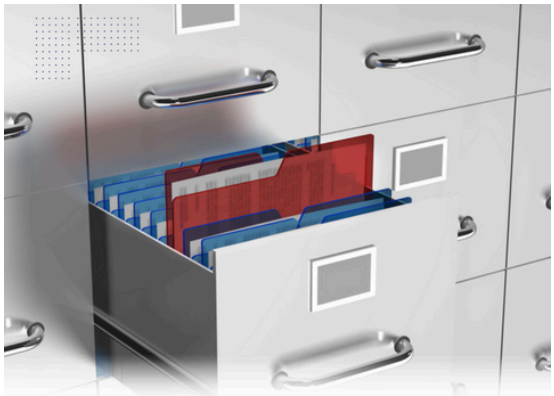
Monthly Newsletter

THE TECH CHRONICLE

Volume 16

July 2024 www.centrend.com Monday

WHAT'S INSIDE?



TECH TIP

IMPLEMENT A COMPANY WIDE FILE NAMING SYSTEM

@centrendtechnology

Centrend

Enjoy a Hack-Free Vacation

We all deserve a break. A chance to unwind, explore new destinations, and recharge. But cybercriminals don't take vacations! They often see travel seasons as prime opportunities to target unsuspecting victims

Here are some essential cybersecurity measures you can take to ensure a relaxing and hack-free vacation:

Before you go:

Secure your home: Before you jet off, ensure your home Wi-Fi network is secure. Use a strong password and enable two-factor authentication. Consider smart home features that allow you to monitor your property remotely for added peace of mind.

Back up your data: A lost or stolen device can be a nightmare. Back up all your important data (photos, documents, etc.) to a secure cloud storage service or external hard drive.

Update software: Cybercriminals exploit vulnerabilities in outdated software. Before you leave, update your devices (phones, laptops, tablets) to the latest versions.

Be mindful of what you share: Are you excited about your trip? Avoid oversharing on social media. Wait until you return to post detailed updates and photos, especially those that might reveal your location or absence from home.

While you're away:

Secure your devices: Update software and enable strong passwords. For public Wi-Fi, use a VPN for an extra layer of encryption.

Be mindful of online sharing: Limit vacation posts on social media and wait until you return to avoid tipping off potential burglars.

Beware of phishing scams: Don't click on suspicious links or attachments, even if they seem vacation-related.

Enable Two-Factor Authentication (2FA): Add an extra layer of security to your accounts by requiring a code from your phone in addition to your password.

By following these simple steps, you can minimize cybersecurity risks and focus on what truly matters: creating unforgettable vacation memories.

Bon voyage!

5 Steps to Ensure You Get The Newsletters You Want

In today's digital world, email management can be overwhelming, especially with newsletters filling our primary inboxes. These newsletters are valuable but can bury important emails from contacts. Here's how to organize the newsletters to ensure you see the ones that matter most.

Step 1: Identify Newsletter

First, recognize which emails are newsletters. They often come from companies or subscriptions and have consistent senders or subject lines.

Step 2: Create a Filter

Use your email provider's filter or rules feature to sort newsletters automatically:

- **Gmail:** Go to Settings > See all settings > Filters and Blocked Addresses > Create a new filter. Enter the sender's email or keywords, select "Never send it to Spam," and choose "Categorize as: Primary." Click "Create filter."
- **Outlook:** Go to Settings > View all Outlook settings > Mail > Rules > Add new rule. Name your rule, set conditions (like sender or keywords), choose "Move to folder," and select "Inbox" or "Focused Inbox." Click "Save."

Step 3: Move Existing Newsletters

Drag existing newsletters from "Promotions" (Gmail) or "Other" (Outlook) to "Primary" or "Focused" to train your email to categorize them correctly.

Step 4: Review and Update

Regularly check and update filters to keep up with changes in newsletters' sending addresses or subject lines.

Step 5: Enjoy a Cleaner Inbox

Organizing newsletters in your primary or focused inbox helps you stay on top of essential emails without missing critical communications.

Taking control of your inbox boosts productivity and reduces stress. Start organizing today and streamline your digital life!

Data Recovery Strategies for Seamless Work Operations: Are You Prepared?

Imagine this: you come into work, ready to tackle a busy day, only to discover a critical data loss. Projects vanish, important documents disappear, and your team grinds to a halt. Data is the lifeblood of any business. A data loss incident can be disastrous, leading to lost productivity, financial setbacks, and even reputational damage.

The good news? You can be prepared. By implementing effective data recovery strategies, you can minimize downtime and ensure your operations continue seamlessly, even in a data disaster.

Are you prepared?

Here are some key questions to ask yourself:

- **Do you have a data backup plan?** Regular backups are the cornerstone of data recovery. Ensure you have a comprehensive plan that includes frequent backups and secure off-site storage.
- **Have you conducted a risk assessment**? Understanding your vulnerabilities is crucial. Identify potential threats like hardware failures, cyberattacks, or human error.
- **Do you have a disaster recovery plan?** A well-defined plan outlines the steps to take in case of a data loss. This includes designating a recovery team, establishing communication protocols, and outlining the recovery process itself.

Taking Action: Building a Robust Strategy

- **Implement a Backup Solution:** Choose a reliable backup solution that meets your specific needs. This could involve cloud-based backups, local backups, or a combination of both.

- **Test Regularly:** Don't assume your backups work! Test them regularly to ensure you can restore data quickly and efficiently.
- **Invest in Training:** Educate your employees on data security best practices and how to prevent accidental data loss.
- **Stay Informed:** The data security landscape is constantly evolving. Stay updated on the latest threats and adapt your strategies accordingly.

By prioritizing data recovery, *you're investing in the future of your business. With a robust strategy in place, you can face any data disaster with confidence, minimizing downtime and ensuring seamless work operations. Remember, data recovery isn't a matter of "if" but "when." Be prepared!*

The Ultimate Guide to Investing in Quality IT Support Services

Your IT infrastructure is the backbone of your business. Like any investment, choosing the right IT support services can make all the difference. Here's a sneak peek at our ultimate guide to help you make an informed decision:

- **Know Yourself:** Before diving in, assess your company's IT needs. What are your pain points? What kind of ongoing maintenance is required? Are you looking for remote or on-site support?
- **Define Your Expectations:** Set clear benchmarks for service level agreements (SLAs) that outline response times, resolution timeframes, and the specific services covered.
- **Location, Location, Location:** Consider the pros and cons of local versus remote support. Local providers may offer a more personalized touch, while remote services can tap into a wider talent pool for specialized needs.
- **Beyond the Break-Fix:** Look for a provider that offers proactive maintenance to prevent problems before they arise. This can save you time, money, and frustration in the long run, and provide you with a sense of reassurance and peace of mind.
- **Communication is Key:** Ensure the provider offers clear communication channels and informs you about issues and resolutions.

By following these tips, you'll be well on your way to finding a quality IT support partner. Remember, investing in IT support is an investment in your business's smooth operation and future growth.

How Massive Layoffs Are Heightening Cybersecurity Risks for Businesses

Downsizing isn't just about saving costs. Recent large-scale layoffs can create gaps in your cybersecurity defenses. Here's why:

- **Knowledge Drain:** Departed employees take their business knowledge with them. This can leave your team scrambling to understand complex systems.
- **Stretched Resources:** The remaining staff juggle more tasks, leaving less time for critical security diligence.
- **Disgruntled Employees:** Dismissed workers may hold grudges, increasing the risk of insider threats.

Mitigate the Risk:

- **Cross-Training:** Before layoffs, ensure some knowledge redundancy exists within your security team.
- **Prioritize Security:** Emphasize the importance of cybersecurity even during a downturn.
- **Exit Procedures:** Implement procedures to ensure departing employees don't retain sensitive data.

Cybersecurity shouldn't be a casualty of downsizing. By being proactive, you can maintain a strong defense even in a challenging economic climate.