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

August 2025

Kim Nielsen, CISSP, CCSA
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!"

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -
P A S S W O R D

5 Types of Multi-Factor Authentication

99.9% of breached user accounts do not have multi-factor authentication equipped in their defense.

While most organizations require MFA for very sensitive accounts and records, such as HR files and security settings. For the everyday user, however, many jobs only require passwords for their specific work accounts.

Let's dive into the vast world of MFA, and all the different methods of identity verification that you might encounter.

How MFA Checks User Identity

The different methods of MFA can be broken down into 5 categories: Something you know, something you have, something you are, somewhere you are, and something you do.

1. Something You Know:
   - Passwords: Traditional passwords or PINs.
   - Security Questions: Answers to personal questions.
2. Something You Have:
   - SMS/Email Codes: One-time passwords (OTPs) sent via SMS or email.
   - Authenticator Apps: Apps like Google Authenticator or Microsoft Authenticator that generate time-based OTPs.
   - Hardware Tokens: Physical devices that generate OTPs.
   - Smart Cards: Cards with embedded chips used for authentication.
   - USB Security Keys: Devices like YubiKey that plug into a USB port.

Continued on pg.2

Continued from pg.1

3. Something You Are:
    - Biometrics: Fingerprint scans, facial recognition, or retinal scans.
4. Somewhere You Are:
    - Geolocation: Verifying the user's location through GPS or IP address.
5. Something You Do:
    - Behavioral Biometrics: Analyzing patterns like typing speed or mouse movements.
    - CAPTCHA: Those puzzles you complete authenticate that you're a human instead of a bot.

Choosing something that can't be replicated or hacked is key.

The Best MFA Method for You

Authentication apps and biometrics are among the safest forms of MFA. The apps use an encrypted program to generate one-time codes, which hackers can't access without having your physical device in hand. By contrast, SMS messages and email accounts tend to be much easier to breach from a distance.

Biometrics are the best choice for multi-factor authentication, and you should opt for this method whenever possible. Your face, your fingerprints, your voice — none of these can be replicated! A thief can steal your phone, but they can't take your thumbprint with them.

Multi-Factor Authentication
Password
Verification
Access

About 23% of users prefer biometric methods as their primary authentication. Let's grow this number together and keep our data safer from cyber-threats!

Conclusion

When choosing the right method of multi-factor authentication for your accounts, remember that it's not only about checking a box to make your employer happy…MFA keeps you cyber-compliant with the latest data privacy regulations, and protects your digital information and systems from most digital threats.

While not impenetrable, multi-factor authentication remains the most secure way to protect your accounts, in addition to creating complex and impenetrable passwords.

Security Corner

3 Common Myths About AI

Artificial Intelligence (AI) is everywhere. Unfortunately, with its rise in popularity, comes a wave of misconceptions about these smart tools.

Let's clear up a few of the most common myths!

Myth 1: "AI is going to replace my job."-It's one of the biggest fears surrounding AI, but it's not really the full picture.

In your workplace, artificial intelligence can: Automate repetitive tasks, help generate content, and quickly analyze large amounts of data

Meanwhile, this helpful technology will not replace the need for human skills like critical thinking, creativity, and collaboration.

Myth 2: "If AI says it, it must be right."-This is also false. While these tools can be incredibly helpful, they are not infallible. Sometimes, it "hallucinates," meaning the machine generates information that sounds plausible but is actually incorrect or made up. That's why you always need to double-check its work by verifying sources and information.

Myth 3: "My office doesn't use AI." Approximately 300M companies currently use artificial intelligence in their daily operations already.
If your team uses Microsoft Word, Gmail, Slack, HubSpot, Canva, or Zoom, you're probably using AI-powered features already. These platforms use artificial intelligence to suggest text, filter spam, enhance images, summarize meetings, and more.

For more information about social media posting, call us at 248-362-3800 or visit: https://tinyurl.com/44prf2cf

Building A Smart Data Retention Policy: What Your Small Business Needs To Keep (And Delete)

The digital world has transformed how small businesses operate. We now have an overwhelming volume of information to manage employee records, contracts, logs, financial statements, not to mention customer emails and backups.

A study by PR Newswire shows that 72% of business leaders say they've given up making decisions because the data was too overwhelming.

If not managed properly, all this information can quickly become disorganized. A solid data retention policy helps your business stay organized, compliant, and save money. Here's what to keep, what to delete, and why it matters.

The Goals Behind Smart Data Retention

A good policy balances data usefulness with data security. You want to keep the information that has the most value for your business.

Some reasons small businesses implement data retention policies include compliance with local and international laws, improved security, efficiency in managing storage, and to gain clarity in how and where data lives across the entire organization.

Instead of storing everything in your active system, data can be tucked away safely in lower-cost, long-term storage.

Creating the Policy Step-by-Step

Here's how to go from idea to implementation:

- **Assemble a team:** Bring together IT, legal, HR, and department heads. Everyone has unique needs and insights.
- **Identify compliance rules:** Document all applicable regulations, from local laws to industry-specific guidelines.
- **Map your data:** Know what types of data you have, where it lives, who owns it, and how it flows across systems.
- **Set retention timelines:** Decide how long each data type stays in storage, gets archived, or is deleted.
- **Determine responsibilities:** Assign team members to monitor, audit, and enforce the policy.
- **Automate where possible:** Use software tools to handle archiving, deletion, and metadata tagging.
- **Review regularly:** Schedule annual (or bi-annual) reviews to keep your policy aligned with new laws or business changes.
- **Educate your staff:** Make sure employees know how the policy affects their work and how to properly handle all types of data.

Clean Up Your Digital Closet

Just like you wouldn't keep every receipt, email, or post it note forever, your business shouldn't hoard data without a good reason. A smart, well-organized data retention policy isn't just an IT necessity, it's a strategic move for protecting your business, lowering costs, and staying on the right side of the law.

IT solutions aren't just about fixing broken computers; they're about helping you work smarter. And when it comes to data, a little organization goes a long way. So don't wait for your systems to slow down or a compliance audit to hit your inbox.

Contact us to start building your data retention policy today and take control of your business's digital footprint.

How IT Services Streamline The New Hire Process

Let's break down how technology can step in and make everything smoother, faster, and more efficient for onboarding.

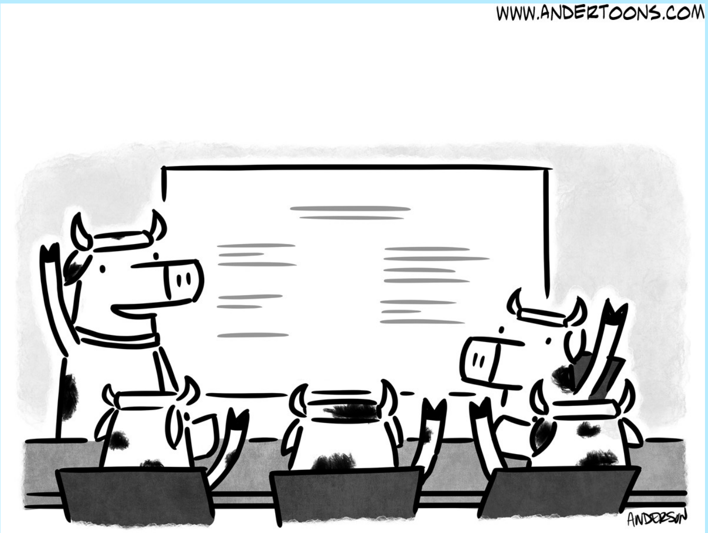
- **Start Before Day 1:** With IT support, you can automate emails, pre-configure accounts, and ship laptops with the necessary software already installed.
- **Automate Tasks:** IT services can automate repetitive HR tasks.
- **Make Training Interactive:** Modern learning platforms, powered by IT, allow companies to deliver engaging training.
- **Create A Central Hub:** A unified onboarding portal pulls everything into one place.
- **Use Analytics to Improve:** IT systems offer dashboards and reports that track time-to productivity, completion rates, satisfaction surveys, and drop-off points in onboarding.

Your Supply Chain Security Checklist

Your suppliers shouldn't be the weakest link in your cybersecurity.

Take control and stay vigilant, with these 7 steps.
1. Map all vendors and their suppliers.
2. Classify vendors by risk and access level.
3. Require and verify vendor security certifications and audits.
4. Make security mandatory in contracts with clear breach notification policies.
5. Implement Zero-Trust access controls.
6. Monitor vendor activity continuously.
7. Consider managed security services for ongoing protection.

By following these steps, you can turn your supply chain into a shield, not a doorway for attackers. Businesses that take a proactive, strategic approach to security will be the ones that avoid disaster.



"Another unanimous vote! Man I love the herd mentality!"

Cloud Cost Optimization Strategies That Work

Control cloud spending and avoid billing nightmares through these strategies:

- **Right-Size Resources:** Analyze patterns and scale resources to match actual demands.
- **Turn Off Idle Resources:** Kill unused instances.
- **Leverage Reserved and Spot Instances:** Both can be cost effective alternatives.
- **Automate Where Possible:** Use automation tools to handle scaling, shutdowns, and cost alerts.
- **Optimize Your Storage:** Use the right storage tier for your needs.
- **Monitor and Adjust:** Track usage and adjust accordingly.
- **Don't Forget Data Transfer:** Be mindful of how and where you are moving data.