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



**March 2026**

**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!"

## How Healthcare Data Breaches Fuel Identity Theft and Insurance Fraud

Did you know healthcare data is among the most sensitive and valuable information out there? Unfortunately, it's also a prime target for cybercriminals. When healthcare organizations experience data breaches, the consequences can be far-reaching—not just for the institutions, but for the individuals whose data is compromised.

Let's break down how these breaches on your PHI can lead to disastrous consequences, including identity theft and even insurance fraud!

**What's at Stake in a Healthcare Breach?**

Healthcare records are a goldmine for hackers. Unlike a stolen credit card number, which can be quickly canceled, medical data is deeply personal and often permanent. A typical healthcare record might include your…

- Full name and date of birth
- Social Security number
- Home address
- Health insurance details
- Medical history and diagnoses

This comprehensive profile makes it easy for criminals to impersonate someone and commit fraud. That's one reason that personal health information (PHI) is such an attractive target for thieves. These records sell for as little as $60 on the Dark Web, although the prices can range into the thousands depending on the type of data.

**How PHI Theft Affects You**

Why are healthcare breaches a growing concern? Once cybercriminals get their hands on this data, they can use it to open new credit accounts, file fraudulent tax returns, apply for loans or government benefits, and

*Continued on pg.2*

*Continued from pg.1*

access other services that traditionally require identity verification.

Unfortunately, victims often don't realize their identity has been stolen until they're denied credit, receive unfamiliar medical bills, or notice strange activity on their accounts. That can lead to one of the most dangerous forms of identity theft: Medical identity theft. This happens when someone uses your personal information to get medical treatment, fill prescriptions or submit insurance claims. It can lead to incorrect information being added to your medical records, which could affect future care. It can also result in denied insurance claims or unexpected bills for services you never received.

**Insurance Fraud: Another Costly Consequence**

Threat actors also use stolen healthcare data to commit insurance fraud. This can involve:

- Filing fake claims with insurance companies
- Billing for services that were never provided
- Inflating the cost of legitimate procedures

These fraudulent activities drive up healthcare costs for everyone and can lead to legal trouble for victims who are falsely linked to the crimes.

**Protecting Your PHI**

Meanwhile, the effects of a healthcare data breach can linger for years. Victims may face damaged credit scores, legal disputes over fraudulent charges, hours spent resolving identity issues, and a general loss of trust in their healthcare providers. While you can't always prevent a breach, you can take steps to protect yourself:

- Regularly monitor your credit and insurance statements
- Use strong, unique passwords for healthcare portals
- Be cautious about sharing personal information online
- Consider identity theft protection services

**Conclusion**

Healthcare data breaches are more than just IT issues. They're extremely personal. Unlike other types of cyber events, the personal nature of your medical information makes these incidents especially invasive and extremely difficult to recover from.

The more you know about threats to your PHI, the better you can protect your healthcare data from cyberattacks.

## Free Cyber Risk Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now


At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber risk audit to uncover any loopholes that may exist in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these risk problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are exposed to various threats in a number of areas.

**Claim Your FREE Assessment Today At:**
**https://www.cti-mi.com/cyber-security-audit-326**

# Security Corner

**What Makes Public Wi-Fi a Risk?**

Public Wi-Fi is everywhere. Airports, hotels, coffee shops, and libraries all offer quick and convenient ways to get online when you are away from home or the office. Unfortunately, public Wi-Fi is also one of the most common places where security problems quietly begin.

**Why Public Wi-Fi Is Less Secure**
It's not that public Wi-Fi is always dangerous. The risk comes because you do not control it, and you cannot see what is happening behind the scenes.

**The Hidden Threat of Open Networks**
Many public Wi-Fi networks are open, meaning that they require no password or rely on minimal protections. While this makes them convenient, it also increases the potential for data exposure.

**Simple Habits to Reduce Your Risk**
Using a company-approved VPN, avoiding sensitive logins on open networks, disabling automatic Wi-Fi connections, verifying network names, and keeping devices updated all reduce risk. If you encounter unexpected login prompts, security warnings, or strange redirects, then you should immediately stop and reconsider the situation.

**Conclusion**
Most incidents that occur on public networks blend into routine browsing, everyday logins, and normal work tasks. That's why awareness matters more than fear. By understanding what makes public Wi-Fi risky and adopting a few protective habits, employees can stay productive without turning convenience into compromise.

For more information about this topic, call us at 248-362-3800 or visit: https://tinyurl.com/3awv6erb

# The Hybrid Strategy: Why "Cloud Only" Might Be A Mistake

Since cloud computing became mainstream, promising agility, simplicity, offloaded maintenance, and scalability, the message was clear: "Move everything to the cloud." But once the initial migration wave settled, the challenges became apparent. Some workloads thrive in the cloud, while others become slower, or more expensive. The smart strategy for 2026 is a pragmatic hybrid cloud approach.

A hybrid cloud strategy blends public cloud services like AWS, Azure, and Google Cloud with private infrastructure, whether that's a private cloud in a colocation facility or on-premise servers. The goal isn't to avoid the cloud, it's to use it wisely.

This approach recognizes that one size does not fit all. It gives you the flexibility to place each workload where it performs best, considering cost, performance, security, and regulatory requirements. Treating hybrid as a temporary solution is a mistake, as it is increasingly becoming the standard model for resilient operations.

**The Hidden Costs of a Cloud-Only Strategy**

Relying on a single model can create blind spots. The cloud's operational expense (OpEx) model is fantastic for variable workloads. but for predictable, steady-state applications, it can cost more over time than a capital investment (CapEx) in on-premise equipment. Data egress fees, the cost of moving data out of the cloud, can lead to surprise bills and create a form of "lockin."

Performance can also suffer. Applications that require ultralow latency or constant, high bandwidth communication may lag if they're forced into a cloud data center far away. A hybrid approach lets you keep latency sensitive workloads close to home for optimal performance.

**The Strategic Benefits of a Hybrid Cloud Model**

First, a hybrid cloud strategy is all about balancing resilience and flexibility. For example, during peak periods like a holiday sales rush, you can take advantage of the public cloud's scalability and then scale back to your private infrastructure when demand drops. This approach can significantly reduce costs.

Second, hybrid cloud helps meet data sovereignty and strict compliance requirements. You can keep sensitive or regulated data on infrastructure you control while running analytics or other workloads in the cloud. This setup is often essential for healthcare, government, finance, and legal sectors, where data must remain within a specific legal jurisdiction.

**The Path to a Future-Proof IT Architecture**

Adopting a hybrid mindset creates a future-proof IT architecture. It reduces the risk of vendor lock-in, preserves capital, and provides a built-in safety net. The cloud landscape will keep evolving, and a hybrid foundation lets you adopt new services without a full rip-and- replace.

The goal for 2026 is intelligent placement, not blind migration. Your infrastructure should be as dynamic and strategic as your business plan, and a blended approach can assist in making that happen.

Reach out today for help designing the hybrid cloud model that best fits your business goals.

## Your Essential Employee Offboarding Checklist

- Disable network access immediately: Once an employee leaves, revoke primary login credentials, VPN access, and any remote desktop connections.
- Reset passwords for shared accounts: This includes social media accounts, shared email boxes and workspaces.
- Revoke cloud access: Remove permissions for Microsoft 365, Google Workspace, Slack, project management tools, and other platforms.
- Reclaim all company devices: Have the employee return all company devices and perform secure data wipes before reissuing.
- Forward emails: For a smooth transition, forward the employee's email to their manager or replacement for 30 to 90 days, then archive or delete the mailbox.
- Review and transfer digital assets: Make sure critical files aren't stored only on personal devices, and transfer ownership of cloud documents and projects.
- Check access logs: Review what the employee accessed in the days before leaving. Pay attention to whether sensitive customer data was downloaded and whether it was needed for their work.

## Managing Cloud Waste

Controlling cloud waste is not just about saving money. Every dollar you save can be reinvested in innovation, stronger security, or your team.

1. Use tagging consistently to make filtering, organizing, and tracking costs easier.

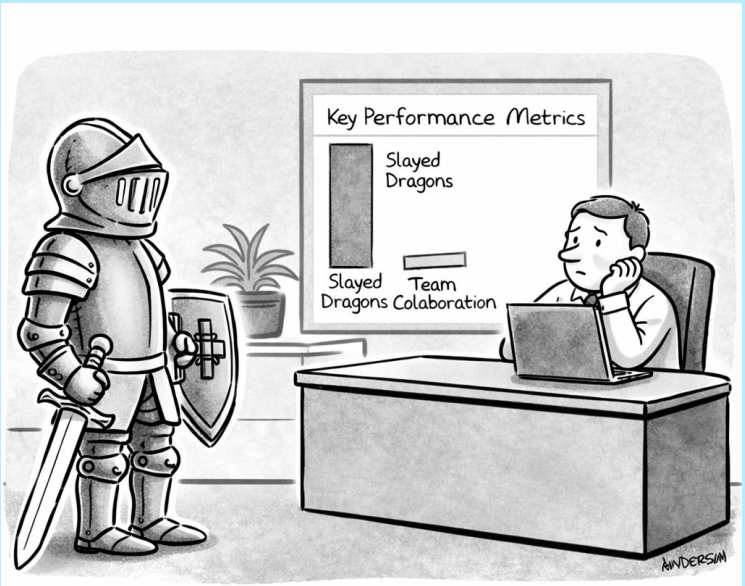
2. Assign every resource to a project, department, and owner.

3. Consider third-party cloud cost optimization tools for deeper insights. They can automatically spot waste, recommend rightsizing actions, and consolidate data into a single dashboard if you're using multiple cloud providers.

4. Automatically schedule nonproduction environments like development and testing to turn off during nights and weekends.

5. Implement storage lifecycle policies to move old data to lower-cost archival tiers or delete it after a set period.

6. Adjust the size of your servers. If the CPU is used less than 20% of the time, the server is larger than necessary, replace it with a smaller, more affordable option.




"Your results are impressive, but we're concerned you're not working with others enough."