# NEWSLETTER

I.T.INSIGHTS NEWSLETTER - ISSUE #01 - OCTOBER 2024



i.t. 30 now

We Make It Look Easy

# STAY AHEAD OF CYBER THREATS

## ESSENTIAL CYBERSECURITY PRACTICES FOR 2024

Cybersecurity isn't just an IT concern—it's a business-critical priority. Failure to implement these best practices can result in data breaches, financial losses, and reputational damage. By taking action now, you safeguard your business from costly disruptions. For more tips, check out our blog posts on phishing threats and cybersecurity resilience.

As cyber threats continue to evolve, businesses must strengthen their defenses to remain secure. Below are three critical practices to help you safeguard your operations:

**Multi-Factor Authentication (MFA)**:
Passwords alone are no longer enough. Implementing MFA ensures that users verify their identity through multiple methods, such as a phone code or biometric data, significantly reducing the risk of unauthorized access.

**Regular Software Updates**:
Outdated software is a common entry point for hackers. Regularly updating your systems helps close security gaps and ensures you're protected from the latest vulnerabilities.

**Backup and Disaster Recovery**:
Cyberattacks, especially ransomware, can cripple your business by locking your data. Regularly backing up your data and having a disaster recovery plan can minimize downtime and ensure business continuity.

# CLIENT SUCCESS STORY

## ZENITH FAMILY HEALTH CENTER ENHANCES IT SECURITY WITH I.T.NOW

Zenith Family Health Center faced several challenges with their IT systems, including frequent downtime, which affected their ability to deliver patient care efficiently. Data security was also a concern, given the sensitive nature of their records.

**Riverton & Zenith Family Health Center**

"i.t.NOW takes a lot of headaches off my hands. We've grown from one location to three, and ITNOW keeps us up and running all the time. It's just a no-brainer. I would absolutely recommend i.t.NOW for any kind of IT concerns."

**— Aaron Monson**

### How i.t.NOW Helped:

**Improved System Uptime**: i.t.NOW implemented robust IT solutions, minimizing downtime and allowing staff to focus on patient care.

**HIPAA Compliance**: We ensured that Zenith met all HIPAA regulations by securing their electronic medical records (EMR) and enforcing stringent security protocols.

**Cost Savings**: By outsourcing their IT needs, Zenith was able to avoid the cost of hiring an in-house team, while benefiting from top-tier technology and support.

### Key Results:

**Increased Operational Efficiency**: With minimized disruptions, patient care was never compromised.

**HIPAA Compliance**: Patient data is now fully protected, and Zenith avoids the risk of fines for non-compliance.

**Reduced Costs**: Outsourcing IT saved significant operational costs, enabling Zenith to reinvest those savings back into patient care.

In the **healthcare industry**, IT efficiency and security are crucial. By partnering with i.t.NOW, Zenith Family Health Center improved its IT infrastructure, achieved compliance, and ensured data protection, providing peace of mind for both staff and patients.

# TRENDING IT NEWS

## RANSOMWARE ATTACKS SURGE 30% IN 2024

Cyberattacks, especially ransomware, are targeting more businesses, with attacks up 30% compared to last year. These attacks can paralyze your operations by locking up critical data and demanding a ransom for its return.

**Why It Matters**: If your systems are not properly secured, you risk severe downtime, data loss, and financial costs. Strengthen your defenses to avoid becoming a target.
[Read more.]

## UTAH'S NEW DATA PRIVACY LAW FOR 2024

Starting this year, Utah businesses face stricter regulations around the handling and protection of customer data. The new law requires stronger data security protocols, and businesses found non-compliant could face fines.

**Why It Matters**: Non-compliance can result in severe penalties. Now is the time to review your IT security policies and ensure they align with the new regulations.

[Learn More]

## WINDOWS 10 END OF LIFE – OCTOBER 14, 2025

Microsoft has announced that Windows 10 will reach its End of Life in 2025, meaning there will be no more updates or security patches.

**Why It Matters**: Without critical updates, your systems will be vulnerable to cyber threats, and you could face compliance challenges

Now is the time to plan your transition to Windows 11 or consider upgrading your equipment.

[Download Your Special Upgrade Offer Here]


## Why it matters:

Cybersecurity isn't just a tech issue—it's a business imperative. This checklist helps ensure you're taking the necessary steps to secure your business from costly data breaches.

# Cybersecurity Checklist

### Is Your Business Safe?

Our Cybersecurity Checklist will help you evaluate your current defenses and ensure your business is prepared for modern cyber threats. Download it to identify potential vulnerabilities and strengthen your cybersecurity posture.

**Download Here**

## Don't Let This Be You!


# NETWORK SEGMENTATION TO LIMIT DATA BREACHES

ENHANCE YOUR SECURITY POSTURE

In today's evolving cybersecurity landscape, traditional defense mechanisms alone aren't enough to fully protect your business. One of the most effective strategies to enhance your security posture is through network segmentation. This method divides your network into smaller, isolated segments, each with its own access controls and security measures, limiting the ability of cybercriminals to move freely within your network if a breach occurs.

**What is Network Segmentation?**

Network segmentation involves breaking a larger network into smaller sections or segments that are governed by specific rules and access policies. These segments could be divided by department, data sensitivity, or device type. By doing so, you create isolated zones within your network, making it harder for attackers to move laterally if they gain access to one segment.

Imagine your company's network as a building with multiple rooms.

In an unsegmented network, once an attacker breaks into the building, they can access all rooms freely. In a segmented network, each room is locked separately, limiting the attacker to only the room they entered, protecting the rest of the building.

**How Network Segmentation Reduces Breach Impact**

Segmentation significantly minimizes the impact of a breach. If a hacker penetrates a non-critical segment, they are prevented

from moving to critical areas such as databases or financial systems, thanks to the additional controls in place. This prevents the entire network from being compromised.

For instance, if a breach occurs through a user's device on the guest Wi-Fi network, segmentation ensures that the core business systems remain secure. This is crucial for preventing widespread malware infections, data theft, or ransomware attacks.

**Benefits of Network Segmentation**

**1. Enhanced Security**

By isolating sensitive areas, network segmentation provides multiple layers of defense, reducing the likelihood of a breach escalating throughout your entire network. Attackers are forced to penetrate additional layers of security, making it harder for them to reach critical data.

**2. Improved Regulatory Compliance**

Industries such as healthcare, finance, and retail are subject to strict regulatory requirements like HIPAA, PCI DSS, and GDPR. Network segmentation helps achieve compliance by ensuring that sensitive data is stored in isolated, secure segments, accessible only to authorized personnel.

**4. Better Network Performance**

Network segmentation can also boost performance by reducing unnecessary traffic. Isolating traffic-heavy processes into different segments ensures that critical systems, like financial databases, are not bogged down by unrelated network activity.

**4. Increased Control and Monitoring**

With segmented networks, it's easier to monitor traffic and detect anomalies. Segments can be individually monitored, and security breaches are more easily identified and isolated, preventing them from spreading.

**5. Improved Incident Response**

Should an attack occur, segmented networks allow for quicker identification of the compromised area, improving the speed and precision of incident response. This prevents breaches from spreading and allows for more targeted containment.

**Implementing Network Segmentation in Your Business**

Start by assessing your current network infrastructure and identifying the most critical areas that need isolation. Next, define security policies for each segment, enforce them with firewalls, and monitor activity to ensure compliance. Regularly review the segmentation plan to ensure it remains effective as your business grows.

**Read more about IT Security for Small Business**

For more details on network segmentation and other critical security practices, check out i.t.NOW's comprehensive guide to IT security for small businesses.

This guide covers various strategies, including how network segmentation fits into an overall cybersecurity strategy, helping small businesses protect their data from increasingly sophisticated cyber threats.

Network segmentation is a must for businesses seeking to minimize their risk of cyberattacks. By dividing your network into smaller sections, you make it harder for attackers to move freely if they gain access. This extra layer of protection not only strengthens your security but also ensures compliance with industry regulations.


# PREVENTING CYBERSECURITY BREACHES IN 2024

## ON-ON DEMAND WEBINAR

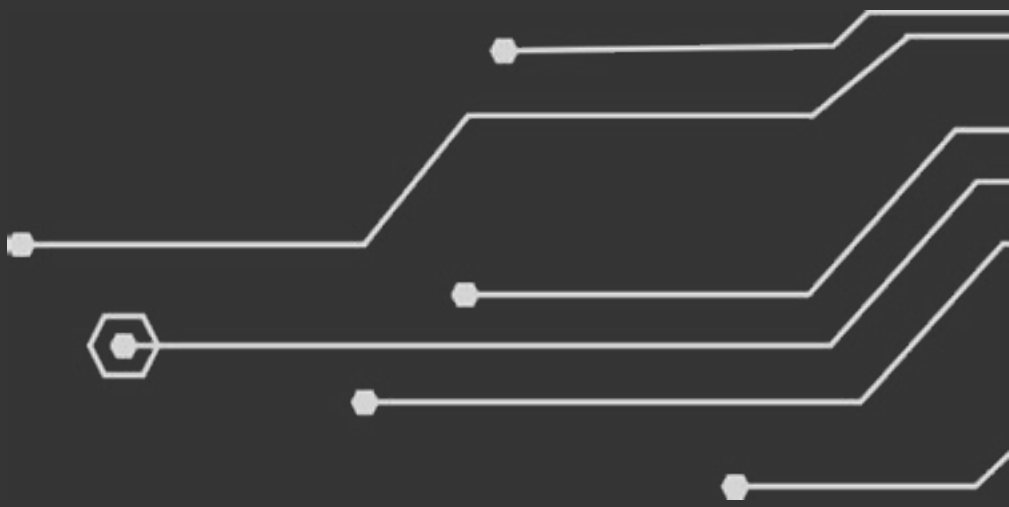
Watch our on-demand webinar and learn how to stay ahead of cybersecurity breaches. In this webinar, our cybersecurity experts will walk you through practical steps for identifying vulnerabilities and fortifying your defenses. Whether you're working with remote teams or managing an on-premise system, this webinar will provide actionable insights for keeping your business secure. **Watch It Now.**

**Why It Matters:**

Cyber threats are evolving every day, and staying informed is essential for protecting your business. This webinar will equip you with the knowledge to take immediate action.

**Book an Appointment with Mike Herrington, VP of Sales & Marketing**

Whether you're planning a transition to Windows 11 or need to strengthen your cybersecurity, i.t.NOW is here to help. Schedule a call with Mike Herrington, VP of Sales & Marketing, to explore how we can protect your business. **Schedule an appointment here**



(801) 562-8778
Sales: (801) 859-2171

help@itnow.net

2436 W 700 S
Pleasant Grove, UT 8406