LeadingIT

October 2025

Y AWARENESS MONTH – CYBER SECURITY AWARENESS MONTH – CYBER SECURITY AWARE

The NetWork

Understanding the Core 4 Steps to Stay Safe Online

Staying safe online is not just a concern for large enterprises. For small and mid-sized businesses across Chicago, a single cyberattack can disrupt operations, damage reputation, and cause lasting financial harm.

During Cybersecurity Awareness Month, the National Cybersecurity Alliance highlights the “Core 4” steps that every organization and individual should follow to improve online safety. Here’s how Chicagoland businesses can put these best practices into action.

Step 1: Use Strong Passwords and a Password Manager

Weak or reused passwords remain one of the top entry points for hackers. Every account should have a unique password that includes a mix of letters, numbers, and special characters. Password managers make this process easier by securely storing and auto-filling credentials. Businesses should also enforce company-wide password policies and train staff on secure practices. IT support services can help implement password management tools that protect employees and clients.

Step 2: Turn on Multi-Factor Authentication

Passwords alone are not enough. Multi-factor authentication (MFA) adds an extra layer of security by requiring a second step, such as a code sent to a phone or a biometric check. According to Microsoft, MFA can block over 99% of automated cyberattacks. For Chicago SMBs, enabling MFA across email, financial accounts, and cloud services should be non-negotiable.

Step 3: Update Software Regularly

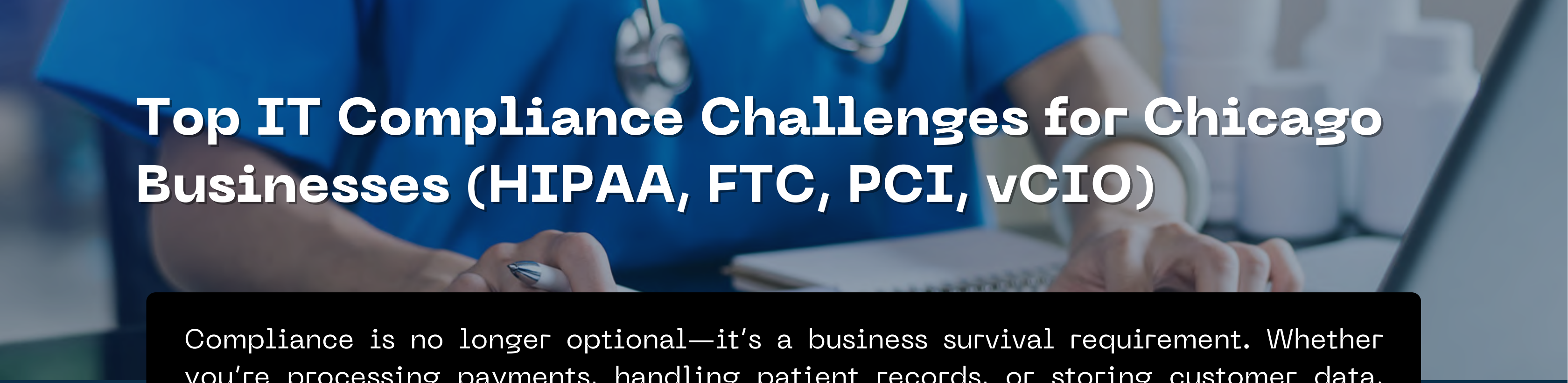
Hackers often exploit outdated software with known vulnerabilities. Regular updates and patches protect against these risks. Businesses should create a patch management policy and consider automated tools that ensure systems, applications, and devices are always current. Our Workplace Complete package includes proactive monitoring and updates so businesses never fall behind on critical patches.

Step 4: Recognize and Report Phishing

Phishing remains one of the most common attack methods. Employees should learn how to spot suspicious emails and messages that attempt to steal credentials or trick them into clicking malicious links. Encourage staff to verify senders, avoid opening unexpected attachments, and report phishing attempts immediately. Ongoing cybersecurity training keeps these skills sharp.

Putting the Core 4 Into Action

These four simple steps can drastically reduce the risk of cyber incidents for Chicagoland businesses. By focusing on passwords, MFA, updates, and phishing awareness, organizations empower their teams to become active participants in security.



Top IT Compliance Challenges for Chicago Businesses (HIPAA, FTC, PCI, vCIO)

> Compliance is no longer optional—it's a business survival requirement. Whether you're processing payments, handling patient records, or storing customer data, Chicago businesses face strict regulations that can't be ignored.

According to IBM's Cost of a Data Breach Report, the average compliance-related data breach costs over $4.45 million in 2024. Noncompliance fines from regulators like the FTC or PCI Council can add thousands more, not to mention reputational damage.

For small to mid-sized businesses in Chicagoland, navigating the maze of IT compliance is overwhelming. That's where strategic IT support and vCIO services come in. By aligning your technology with HIPAA, FTC, and PCI requirements, you can reduce risk, avoid fines, and protect your reputation.

HIPAA Compliance: Protecting Patient & Client Data

Healthcare organizations and businesses that handle medical information are under the watchful eye of HIPAA (Health Insurance Portability and Accountability Act).

The challenge? HIPAA is complex and constantly evolving. Common IT pain points include:

- Encrypting electronic health records (EHRs) at rest and in transit
- Securing email communication with patients and partners
- Restricting access to sensitive data with role-based permissions
- Conducting required security risk assessments annually
- Implementing reliable backup and disaster recovery plans

Failing to meet HIPAA requirements can result in penalties up to $50,000 per violation. Chicago providers, clinics, and even small nonprofits working with patient data must take compliance seriously.

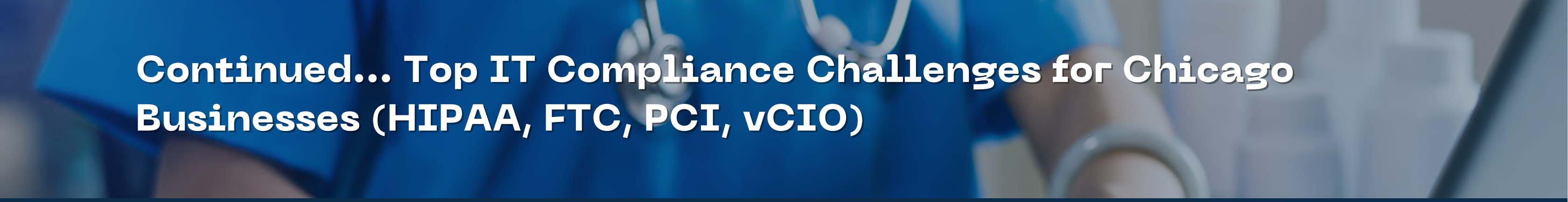
FTC Safeguards Rule: Protecting Consumer Information

The Federal Trade Commission's Safeguards Rule, updated in 2023, expands beyond financial institutions to cover a wide range of businesses that collect consumer data—think accountants, law firms, and even car dealerships.

Key compliance hurdles include:

- Creating a written information security program (WISP)
- Appointing a “qualified individual” to oversee compliance
- Encrypting customer data across all systems
- Conducting vulnerability testing and penetration testing
- Vendor risk management for third-party providers

The FTC now aggressively enforces these rules, and noncompliance can lead to lawsuits, reputational loss, and fines. For Chicago SMBs, having a vCIO to monitor and update compliance practices is no longer optional—it's essential.



Continued... Top IT Compliance Challenges for Chicago Businesses (HIPAA, FTC, PCI, vCIO)

PCI DSS Compliance: Securing Payment Data

If your business processes credit or debit cards, PCI DSS (Payment Card Industry Data Security Standard) compliance is mandatory.

Chicago retailers, nonprofits, and service providers face these common compliance challenges:

- Installing and maintaining secure firewalls and antivirus protection
- Restricting access to cardholder data to only those who need it
- Maintaining detailed logs of all access to systems processing payments
- Encrypting cardholder data during transmission and storage
- Conducting quarterly vulnerability scans and annual penetration tests

Noncompliance can result in fines up to $500,000 per incident and even the loss of your ability to process card payments. For businesses, that's a showstopper.

The Role of a vCIO in Compliance Success

Most SMBs in Chicago don't have the internal bandwidth to manage compliance alone. That's where a vCIO (Virtual Chief Information Officer) adds measurable value.

A vCIO can:

- Assess your current compliance posture through a IT Risk Assessment
- Build a compliance roadmap tailored to HIPAA, FTC, or PCI needs
- Oversee policy development and employee training
- Manage vendor relationships to reduce third-party risk
- Ensure continuous monitoring, reporting, and documentation

With a vCIO on your side, compliance moves from a stressful burden to a strategic advantage.

Why Chicago Businesses Can't Afford to Wait

Regulatory scrutiny is intensifying. Whether it's healthcare data, financial information, or consumer transactions, the stakes are higher than ever.

Chicago businesses that fail to comply risk:

- Hefty regulatory fines
- Loss of customer trust
- Lawsuits and legal action
- Permanent brand damage

By investing in proactive IT compliance support, you can avoid these risks, streamline operations, and focus on growth—not regulatory headaches.

IT Budgeting: Balancing Essentials and Innovation for Chicagoland SMBs

Smart IT budgeting is no longer just about keeping the lights on. For small and mid-sized businesses in Chicago, it is about balancing essential services with forward-looking innovation.

According to Gartner, global IT spending continues to rise as organizations invest in both cybersecurity and digital transformation. Yet many Chicagoland SMBs still struggle with how much to allocate for core services versus new technologies.

Done right, IT budgeting helps protect your business from unexpected risks while positioning you for growth. Done poorly, it can leave you exposed to compliance fines, cyberattacks, or outdated tools that slow you down.

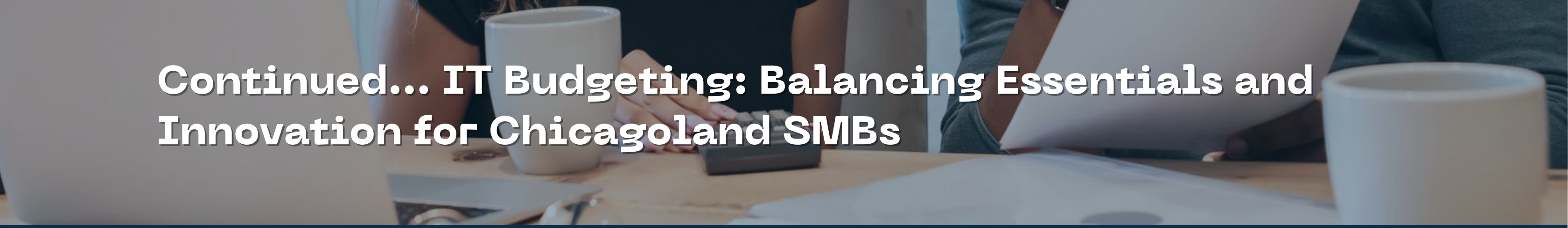
Here are the most important areas Chicago businesses should consider when building a strong IT budget.

Covering the Essentials: Non-Negotiable IT Investments

Every business needs a foundation of secure, reliable technology. These essentials should take priority in any IT budget:

- Cybersecurity: Firewalls, endpoint protection, multi-factor authentication, and employee training protect against today’s top cyber threats.
- Backup and Disaster Recovery: A tested disaster recovery plan ensures data can be restored quickly after an outage, attack, or human error.
- Compliance Requirements: Industries handling health, financial, or consumer data must align with HIPAA, PCI, and FTC standards. Noncompliance can cost thousands in fines.
- Reliable IT Support: Proactive IT support services prevent downtime and help employees stay productive.

These essentials may not feel exciting, but they are the backbone of every business. Without them, innovation is impossible.



Continued... IT Budgeting: Balancing Essentials and Innovation for Chicagoland SMBs

Planning for Innovation: Technology That Drives Growth

Once essentials are covered, SMBs should invest in innovation that fuels competitiveness. Forward-thinking IT budgets often include:

- Cloud Services: Flexible storage and collaboration tools that scale with your business.
- Artificial Intelligence and Automation: Tools like Microsoft Copilot and workflow automation that reduce manual tasks and free staff for higher-value work.
- Modern Communication Systems: VoIP and unified communications that support hybrid teams and improve client experience.
- Data Analytics Tools: Platforms that turn data into actionable insights for smarter decision-making.

Innovation does not have to be expensive. With a thoughtful plan, SMBs can adopt new technology in phases while continuing to support day-to-day operations.

Building Flexibility Into the Budget

Technology evolves quickly, and so do business needs. A strong IT budget should leave room for flexibility. Chicago SMBs can achieve this by:

- Setting aside a contingency fund for unexpected needs or emerging tools
- Working with a vCIO to create a roadmap that balances today’s essentials with tomorrow’s innovations
- Reviewing and adjusting IT spending quarterly instead of only once per year

This approach helps ensure your business is never caught unprepared.

Why IT Budgeting Matters for Chicago SMBs

Chicago’s competitive business environment requires more than reactive IT. Budgets that cover only the bare minimum leave companies vulnerable to cyber threats, compliance issues, and technology obsolescence.

On the other hand, over-investing in every new trend without a plan drains resources and distracts from core goals. The real advantage comes from finding the right balance: covering essentials while strategically funding innovation.

Cybersecurity Awareness Training: Building a Culture of Security in Chicagoland Organizations

Cybersecurity is no longer just the responsibility of the IT department. Every employee—from the front desk to the C-suite—plays a critical role in keeping data secure. For organizations across Chicagoland, cybersecurity awareness training is one of the most effective ways to reduce risk.

According to Verizon's Data Breach Investigations Report, 74% of breaches involve the human element, whether through phishing, weak passwords, or misused credentials. That means technology alone is not enough, your people are the first line of defense.
Here's how Chicago businesses can build a culture of cybersecurity that lasts.

Why Awareness Training Matters

Without training, employees may not recognize phishing emails, may reuse weak passwords, or may accidentally share sensitive data with the wrong person. Even one mistake can lead to significant losses.

Cybersecurity services like firewalls and monitoring tools are essential, but they cannot replace human judgment. Training gives employees the confidence to make smart decisions every day.

Best Practices for Employee Cybersecurity Training

- Make it ongoing, not one-time: Cyber threats evolve constantly. Chicago businesses should provide training at least quarterly, with refreshers after major incidents or updates.
- Use real-world simulations: Phishing simulations and mock incidents help employees recognize and respond to threats in a safe environment.
- Reinforce lessons regularly: Posters, newsletters, and team meetings keep cybersecurity top of mind between formal trainings.
- Tailor training to roles: Finance teams may need extra focus on wire transfer fraud, while healthcare staff must prioritize HIPAA compliance.
- Track progress: Use metrics to measure improvement, such as reduction in phishing click-through rates.

Creating a Security-First Culture

Cybersecurity awareness works best when it is embedded into company culture. Leaders set the tone by following security best practices themselves, while managers reinforce expectations daily. Working with a vCIO can help your organization create a cybersecurity training roadmap and align it with compliance requirements like HIPAA, PCI, or FTC Safeguards.

When employees understand that cybersecurity is everyone's job, risks are reduced and resilience improves.

DRIVEN – CHASES EXCELLENCE – HUMBLY CONFIDENT – ACCOUNTABLE – STAYS POSITIVE

LeadingIT Core Values Victor of the Month

Congratulations to **Jeremiah**, our Values Victor for this month! Jeremiah was recognized by his peers for Chasing Excellence.

JB brings his best to every challenge, striving for improvement, and delivering outstanding support to our clients and team every single day.

We're proud to celebrate Jeremiah for living out one of LeadingIT's core values and setting the bar high for excellence across the company.

LeadingIT

We Help Chicagoland Organizations Eliminate Concerns Over IT and Cybersecurity Where the Unsolvable is Solved with Unlimited Support, and an Unbeatable Guarantee.

WE ARE CELEBRATING!

BIRTHDAYS

DUSTIN LOOPER	10/10
KYLE FUNK	10/26

ANNIVERSARIES

MATTHEW PEPPIN	1 YEAR