The NetWork

IN THIS EDITION:

- AI SOCIAL ENGINEERING HAS ARRIVED: HERE'S HOW OUR 24/7 IT SUPPORT IS PREPARED

- WHAT DO INFORMATION TECHNOLOGY PROFESSIONALS DO?

- MANAGED SERVICES VS OUTSOURCING IT: UNDERSTANDING THE KEY DIFFERENCES

AI Social Engineering has Arrived: Here's How Our 24/7 IT Support Is Prepared

AI–generated voices and synthetic videos aren't future threats, they're active tools criminals use to impersonate executives, vendors, and trusted partners.

According to the Wall Street Journal, a UK energy firm lost $243,000 to a cloned voice impersonating their CEO. CNN reports a 2024 deepfake video conference in Hong Kong led to a $25.6 million transfer. The FBI's 2024 Internet Crime Report shows cyber-enabled crime resulted in $16.6 billion in losses in 2024, a 33% increase from 2023.

Organizations must treat identity-based attacks as top operational risks requiring 24/7 IT support and continuous monitoring.

What the threat looks like:
Attackers deploy three primary tactics

Voice cloning uses AI to mimic executives requesting urgent wire transfers. According to the American Bar Association, these attacks resulted in over $200 million in losses during Q1 2025 alone.

Deep-fake video meetings present fake videos of multiple executives simultaneously. The Hong Kong case showed how convincing these can be.

Automated spear-phishing leverages AI to craft highly personalized messages that bypass traditional security awareness. The FBI warns cybercriminals now use sophisticated AI tools that adapt to each target's communication style.

1) Social engineering awareness training

LeadingIT runs recurring, role-based training for every client user group. Building social engineering awareness across your organization creates the first line of defense.

Training includes recognition of AI-style anomalies, verification discipline (multi-channel confirmation for sensitive requests), stress drills with simulated impersonation scenarios, and phishing tests with AI-style messages for AI spoofing prevention.

CBS News reports that cybersecurity experts recommend out-of-band safe words for sensitive requests—we apply this principle at work.

Training cadence: quarterly refreshers, biannual tabletop exercises, and immediate post-incident reviews.

2) Procedural controls

Technology alone won't stop determined attackers. Essential controls include:
Multi-channel verification for fund transfers, credential changes, or vendor approvals; authenticated approval chains requiring two verified approvers for high-risk actions; pre-shared authentication tokens for sensitive workflows; and change-control gates requiring ticketed approvals with time-delayed enactment.

These controls align with ENISA's multilayer framework for AI cybersecurity.

3) 24/7 network IT Security Monitoring

LeadingIT combines human training with around-the-clock monitoring to spot anomalies early. Unlike many IT security companies offering only business-hours support, our 24/7 IT support ensures threats are detected at any hour.

Our monitoring includes identity telemetry tracking suspicious sign-ins, voice/video provenance checks examining metadata inconsistencies, SIEM correlation triggering automated playbooks, and automated runbooks executing containment steps.

Network IT security monitoring analyzes traffic patterns continuously to identify AI-driven social engineering attempts in progress.


4) Rapid incident response

If impersonation is suspected, our team executes immediate protocols: contain the action, apply multi-channel validation, preserve all media and logs, notify legal/compliance, and run a post-mortem.
When it comes to AI impersonation, immediate response often determines whether an attack succeeds or fails.

What Chicagoland businesses can do today

Protect your organization by: requiring two independent verification channels for payments and privileged access; using pre-shared verification tokens for high-risk approvals; treating any unusual request as unverified until confirmed; ensuring backups and immutable copies exist; and partnering with IT security companies providing 24/7 monitoring.
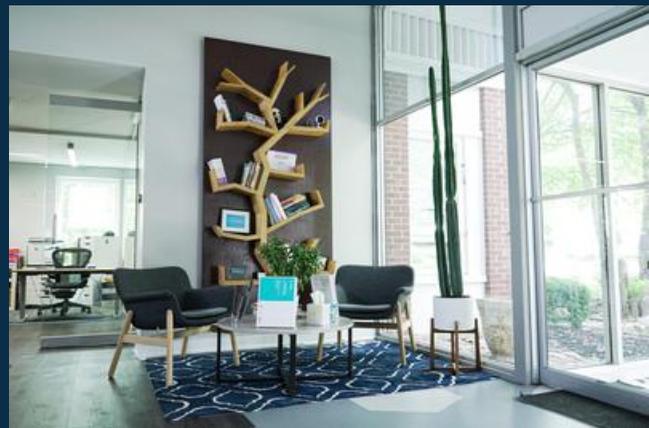
LeadingIT Protects your Chicago Business

AI impersonation is real and evolving. LeadingIT treats identity-based social engineering as a continuous program: trained people, enforced procedures, and layered detection through 24/7 IT support.

Our approach combines social engineering awareness training with network IT security monitoring for comprehensive protection.

What Do Information Technology Professionals Do?

Information technology professionals design, develop, implement, and maintain computer systems, software applications, and network infrastructure. They solve technical problems, protect data from cyber threats, and ensure organizations operate efficiently. Understanding what IT professionals do helps businesses recognize the value these experts provide.

According to the Bureau of Labor Statistics, computer and information technology occupations are projected to add 317,700 openings each year through 2034, with a median annual wage of $105,990. The field offers diverse career paths spanning software development, cybersecurity, network administration, and systems analysis.

Core Responsibilities of Information Technology Professionals

Information technology professionals handle critical tasks that keep organizations running. Common responsibilities include:

- Analyzing technical problems and identifying solutions
- Implementing security measures to protect sensitive data
- Managing hardware and software systems across the organization
- Providing technical support to users and stakeholders

These core tasks appear in virtually every IT role, though specific responsibilities vary by position and industry. Grasping what the IT staff actually do begins with recognizing these foundational responsibilities.

Software Development and Programming

Software developers write, test, and maintain code that powers applications and systems. They build everything from mobile apps to enterprise software and update applications to improve performance. When people ask: "What do IT professionals do?" Software development is often the first role that comes to mind.

According to the Bureau of Labor Statistics, employment of software developers is projected to grow 15% from 2024 to 2034, reflecting continued demand for digital solutions.

Cybersecurity and Data Protection

Information security analysts protect organizations from cyber threats. Key responsibilities include:

- Implementing security measures and monitoring for suspicious activity
- Designing defense strategies to prevent data breaches
- Conducting vulnerability assessments to identify weak points
- Responding to security incidents and unauthorized access attempts

This critical security work represents a major part of what information technology professionals do in today's threat landscape.

Employment of information security analysts is projected to grow 29% from 2024 to 2034, according to the Bureau of Labor Statistics. Many businesses partner with managed IT services to ensure access to cybersecurity professionals who defend against evolving threats.

Systems Analysis and Network Management

Computer systems analysts evaluate technology infrastructure and recommend improvements. They analyze business requirements and design solutions aligned with organizational goals. Network administrators build and maintain communication systems, ensuring networks run smoothly and troubleshooting issues as technology evolves.

IT Support and Management

IT support specialists provide help desk services, troubleshooting hardware issues and assisting with software installations. Computer and information systems managers oversee IT departments, coordinating projects and managing teams. These roles represent another key aspect of what information technology professionals do, requiring both technical knowledge and leadership skills.

The Value IT Professionals Bring to Organizations

Information technology professionals fill diverse roles across every industry. Whether writing code, protecting networks, or managing IT infrastructure, these professionals keep organizations running in an increasingly digital world.

Businesses that partner with a chicago managed services provider gain access to experienced IT professionals who handle everything from cybersecurity to system maintenance. Understanding what information technology professionals do helps organizations recognize the value these experts bring to business operations.

Managed Services vs Outsourcing IT: Understanding the Key Differences

Both managed services and IT outsourcing involve partnering with external providers, and these terms are frequently used interchangeably in the industry. However, IT industry consensus identifies meaningful differences between these service models.

According to Grand View Research, the global managed services market reached $335.37 billion in 2024 and continues growing at 14.1% annually. For Chicagoland businesses managing complex technology environments, understanding the distinctions between managed services vs outsourcing IT helps you evaluate providers and choose the right model.

What is IT Outsourcing?

IT outsourcing involves hiring an external provider to handle specific technology tasks or projects. When evaluating outsourcing IT vs managed services, businesses discover that outsourcing focuses on narrowly defined work with clear start and end points.

Common IT outsourcing examples include:
- Tier 1 help desk support for routine user requests
- Software development projects or application upgrades
- Network infrastructure installation
- Temporary data center management

Organizations often outsource IT support services to handle routine technical requests without maintaining full-time staff.
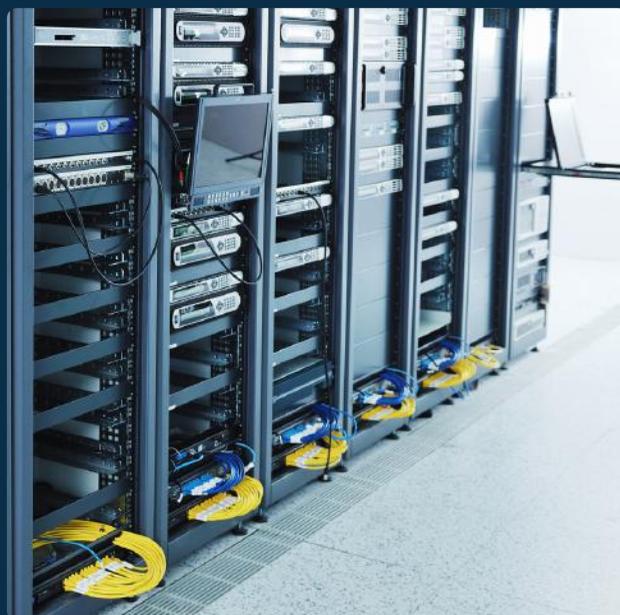
What are Managed IT Services?

Managed IT services provide comprehensive, ongoing technological support and management. Rather than addressing individual tasks, managed services providers deliver end-to-end operational support for your entire IT infrastructure.

Key managed services components include:
- 24/7 proactive system monitoring and maintenance
- Comprehensive cybersecurity protection
- Regular software updates and patch management
- Strategic IT planning aligned with business goals

This model creates strategic partnerships where providers take responsibility for your technology's health and performance, shifting focus from fixing problems to preventing issues.

Key Differences: Managed IT Services vs IT Outsourcing

While many IT providers use these terms interchangeably, the IT industry has established key distinctions. Understanding managed services vs outsourcing IT helps businesses evaluate what they're actually getting.

Here are five key areas where these models typically differ:

Scope: IT outsourcing addresses specific tasks or projects, while managed services cover comprehensive infrastructure support.

Relationship: Outsourcing creates transactional vendor relationships. Managed services establish strategic partnerships where providers function as team extensions.

Support Model: Outsourcing operates reactively. Managed services work proactively, monitoring systems continuously and addressing issues before downtime occurs.

Pricing: Outsourcing typically uses project-based or hourly billing. Managed services offer predictable monthly fees.

Strategic Focus: Outsourcing handles immediate requirements. Managed services prioritize long-term IT health and alignment with business objectives.

With 75% of organizations struggling to find qualified IT professionals according to ManpowerGroup's 2024 report, many Chicagoland businesses rely on external expertise to maintain robust technology operations.

Choosing the Right IT Support Model
When evaluating MSP vs outsourced IT, consider your organization's IT complexity, growth plans, security requirements, and budget. Chicagoland SMBs with complex environments often benefit from managed services for comprehensive, proactive support, while IT outsourcing works well for specific projects or supplementing existing teams.

Since IT providers may use these terms differently, focus on the actual services offered, whether support is reactive or proactive, project-based or ongoing, transactional or strategic, rather than relying on labels alone.

At LeadingIT, our Workplace Complete package provides comprehensive managed IT services designed for Chicago-area businesses.

$1000 REFERRAL PROGRAM

Do you know an organization that needs unlimited IT and cybersecurity support with an unbeatable guarantee?

You'll earn **$50** for every referral. If they sign up, you'll receive **$1000!**

815-788-6041   GOLEADINGIT.COM/REFER

SCAN TO LEARN MORE

WHAT'S NEW AT LEADINGIT

We're excited to share a few team updates as LeadingIT continues to grow and invest in our people.

Congratulations to Dustin, who has stepped into a new role as **Security Analyst**. Dustin's journey with LeadingIT is one we're especially proud of, growing from a Level 1 to Level 2 engineer (all while completing his degree) and now focusing his skills on strengthening our cybersecurity efforts.

We're also thrilled to welcome **Nick** to the team as our newest Level 3 Technician. Nick brings several years of upper-level network experience and will be a great asset to our L3 team as we continue solving complex challenges for our clients.

Finally a warm welcome to **Tina**, our new **vCIO**! Tina brings over 10 years of experience helping businesses grow by providing dependable support and strategic insight. Her thoughtful, people-first approach is a great fit for LeadingIT, and we're excited about the impact she'll make for our clients and across the organization.

Leading IT

Read more at GoLeadingIT.com/blog