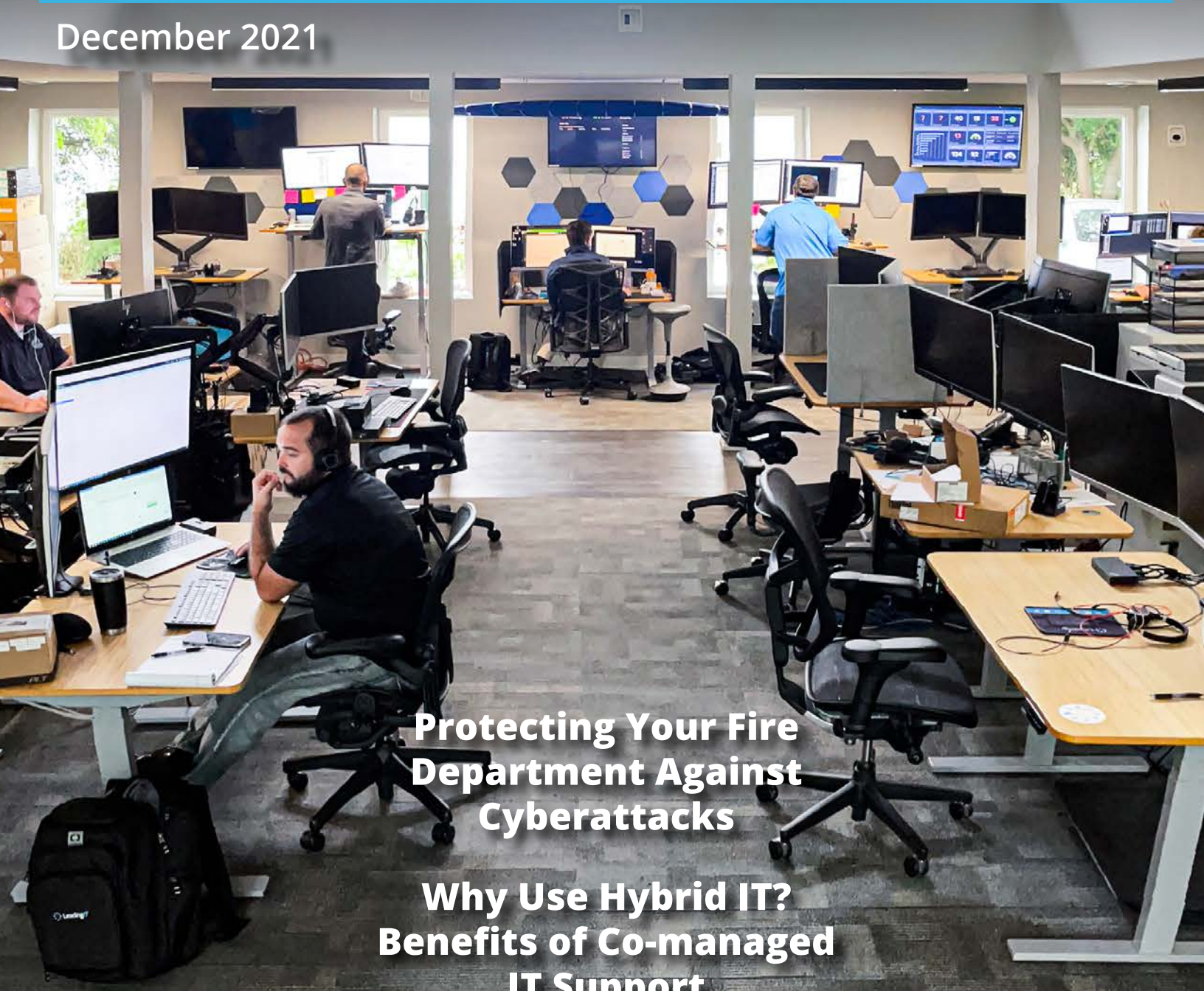
the NetWork LeadingIT

Chicagoland CybersecurITy Support

December 2021



Protecting Your Fire Department Against Cyberattacks

Why Use Hybrid IT? Benefits of Co-managed IT Support

Most Cyber Attacks Now Target Employee Negligence

Community News

GoLeadingIT.com (815) 496-6300 @leadingit-solutions

Protecting Your Fire Department Against Cyberattacks

Technological advancements have enhanced operational efficiency across almost all industries. Fire agencies are no exception—from better data recording and report generation to camera-assisted situation monitoring, improved safety, more accurate smoke detection, and quicker fire alert. We could almost say fire agencies are among the biggest beneficiaries of technology.

However, as you know, integrating technology into processes also comes with the threat of cyberattacks. And the risk has never been higher than it is today. According to recent research by the Clark School at the University of Maryland, cyberattackers launch onslaughts after every 39 seconds on average. Data from the 2019 Global State of Small & Medium-Sized Businesses Cybersecurity Report shows that over 76% of U.S. organizations dealt with attempted or successful cyberattacks in 2020. Within the first quarter of the same year, the FBI recorded an over 300% increase in its internet crimes desk reports. While we might partially blame this on the COVID-19 epidemic and the resulting situations, this has been the trend for pretty some time, even before the pandemic.

Everybody Is a Target

For a long time, cybercriminals only went after organizations in specific industries like banking and financing, healthcare, and government agencies. That's because they, presumably, provided an easier target and were more likely to pay ransoms.

Fast-forward to today—nobody is safe. Malicious cyber actors target all types of organizations, regardless of size or industry. Nothing best elaborates this than the recent surge in supply chain attacks in which cyber attackers go after hundreds, and sometimes thousands, of institutions simultaneously. So, is your fire agency safer than organizations in other industries? A few decades ago, the answer would be yes. But, today—no, nobody is safe. Therefore, you need to take data security as seriously as any other business and consider partnering with a reliable cybersecurity provider.

3 Common Forms of Cyberattacks on Fire Agencies

To understand why it's essential to have a cybersecurity partner, let's look at some of the data security risks that fire agencies like yours grapple with daily. Otherwise, it may not be sensible to prescribe a solution for a problem that you don't understand. Here are three of the most common types of cyberattacks on fire departments:

1. Ransomware

As the name suggests, it's a cyberattack vector in which the bad guys encrypt your files and deny you access and then demand ransom for decryption. It's one of the most lethal types of malware and costs businesses approximately $20 billion annually. A few years ago, Atlanta's municipal systems were part of a ransomware attack that caused widespread outages. Fire departments, and other essential service providers, had to halt temporarily, and the city spent over $2.7 million on emergency and recovery.

2. Phishing

Another widespread cybercrime to look out for is phishing. It involves cyber-attackers masquerading as known or legitimate entities to trick your users into divulging critical credentials. Typically, they'll email, text, or call you pretending to be your bank, insurance provider, credit card company, random person in distress, or any other individual you normally interact with and trust.

For fire agencies, they may masquerade as the federal government, mutual aid agencies, or non-profit organizations. Once they've won your trust, they ask you to verify your identity by giving them your username, password, or social security number. Beware—legitimate organizations do not ask for clients' personal information over the phone or online.

3. IoT Attacks

IoT (Internet of Things) are gadgets that can transmit data over networks but do not require human-to-computer or human-to-human contact. Perfect examples include fire alarms, thermal cameras, and smart sprinklers. The bad guys can hack these devices and use them to pry on you and see your sensitive information.

Continue reading: goleadingit.com/blog.

Why Use Hybrid IT?
Benefits of Co-managed IT Support

One of the oldest dilemmas in the IT world is whether in-house IT is better than outsourced IT support or vice versa. Traditionally, many business owners believe that there are only two alternatives—managing everything internally or outsourcing everything. The truth, however, is that you can use co-managed IT services to get the best of both worlds.

We're living in the information age, where technology is an integral component of almost every business process. Any slight glitch in your IT system can significantly set you behind your competitors. Today, every organization needs to ensure that its networks are up and running 24/7. That's why reliable IT management is crucial for modern-day businesses.

> **"Staff error plays a significant role in 95% of successful data breaches."**

In-house IT Management Vs. Outsourced IT Support

Both in-house IT management and outsourced IT support have their fair shares of advantages and limitations:

In-House IT Management

If you already have an internal IT team, you know how expensive it can be. In most organizations, especially those with in-house IT staff, IT is the most costly department. And reasonably so—you have to maintain salaried personnel, invest in the latest technologies, get the latest software updates, and continually upgrade your software in response to emerging threats. Glassdoor estimates that an IT leader takes home approximately $122,099 and an IT specialist $51,838 annually. That's without adding other benefits like holiday allowances, overtime, and insurance covers. By any standard, this can be a heavy financial burden on your business.

The trade-off is that you get an IT team that is fully dedicated to managing your networks. They take time to learn your systems to the detail and give your IT environment unwavering attention. Most business owners and leaders who opt for in-house IT may enjoy this advantage. Besides, because the IT department is part of your day-to-day activities, it understands your processes and identifies with your company's goals. Therefore, they can customize IT solutions to fit your unique IT support needs.

Outsourced IT Support

If you cannot afford to manage an in-house IT department, the alternative is outsourcing. Outsourcing enables your business to access a vast pool of deep benches of IT personnel at a fraction of the amount you'd have used to manage everything internally. The outsourced IT support team handles everything, from acquiring the latest technologies to hiring, training, and paying the IT specialists. All the hard work shifts to the service provider at a service bill per user or number of stations. Besides the financial benefit, this also creates more time for you to focus on other core business tasks.

What Are the Likely Downsides to Outsourcing IT Support?

While outsourcing grants you access to top-tier industry specialists, you may forgo the exclusivity benefit that comes with maintaining an in-house team. You may not directly involve the outsourced service provider in your daily operations.

Continue reading: goleadingit.com/blog.

Most Cyber Attacks Now Target Employee Negligence

The general opinion is that you need complex technologies and data security systems to prevent most cybersecurity threats like malware and supply chain attacks. While we may not entirely disagree, any data protection technology is only as effective as your staff can understand and use it. Your employees are your most crucial defense line in the war against cyber-crime, and ironically, the weakest link. Even with the best threat detection and anti-malware systems in place, your networks are only as safe as your staff is cyber-informed.

Employee Cyber Training Reduces Your Risk by Over 70%

As almost every organization is spending thousands of dollars on the most sophisticated data protection software and technologies, cyber actors are gradually redefining the nature of their attacks. Instead of directly targeting vulnerabilities in gateways and other security systems, they are now increasingly going after staff negligence. According to the 2021 IBM Cyber Security Intelligence Index Report, staff error plays a significant role in 95% of successful data breaches. In short, if you can eliminate human error, you can prevent over 90% of cyber incidents.

Types and Examples of Common Human Error

While cyber-attackers target thousands of human errors, we can categorize them into two types:

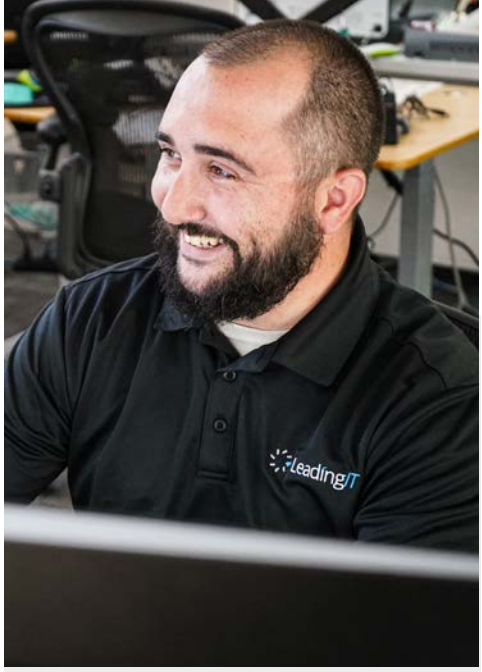
Skill-Based Error

These are lapses and slips that occur when employees are performing familiar activities. Typically, users know what to do but don't do so because of distractions, ignorance, memory lapse, not paying attention, or being overwhelmed. For instance, a recent study by FAU shows that an alarming 78% of Americans open suspicious links despite knowing the cyber risks that come with them.

Decision-Based Error

Here, the employee makes wrong decisions because of a lack of knowledge or misinformation on how to handle the circumstance. Sometimes, failure to take action also counts as a decision-based error. For instance, a user may fail to inform the IT support team of abnormal activity in their PCs and, because of their inaction, unknowingly buy more time for cyber actors to launch onslaughts on the entire network.

Continue reading: goleadingit.com/blog.



Community News

LeadingIT recently teamed up with Extra Life to raise money for the Children's Miracle Network Hospitals. Our team set goals and invited donors and sponsors to donate to the cause while playing marathon sessions of our favorite video games. LeadingIT's involvement in Extra Life supports our core value of community and the need to give back.

extra life™
Play Games. Heal Kids.

BENEFITING Children's Miracle Network Hospitals®

LeadingIT

We Protect Your Chicagoland Organization From Ongoing CybersecurITy Threats.

Check out our blog at goleadingit.com/blog

WE ARE CELEBRATING

Birthdays

Christa Gibbons - December 14th