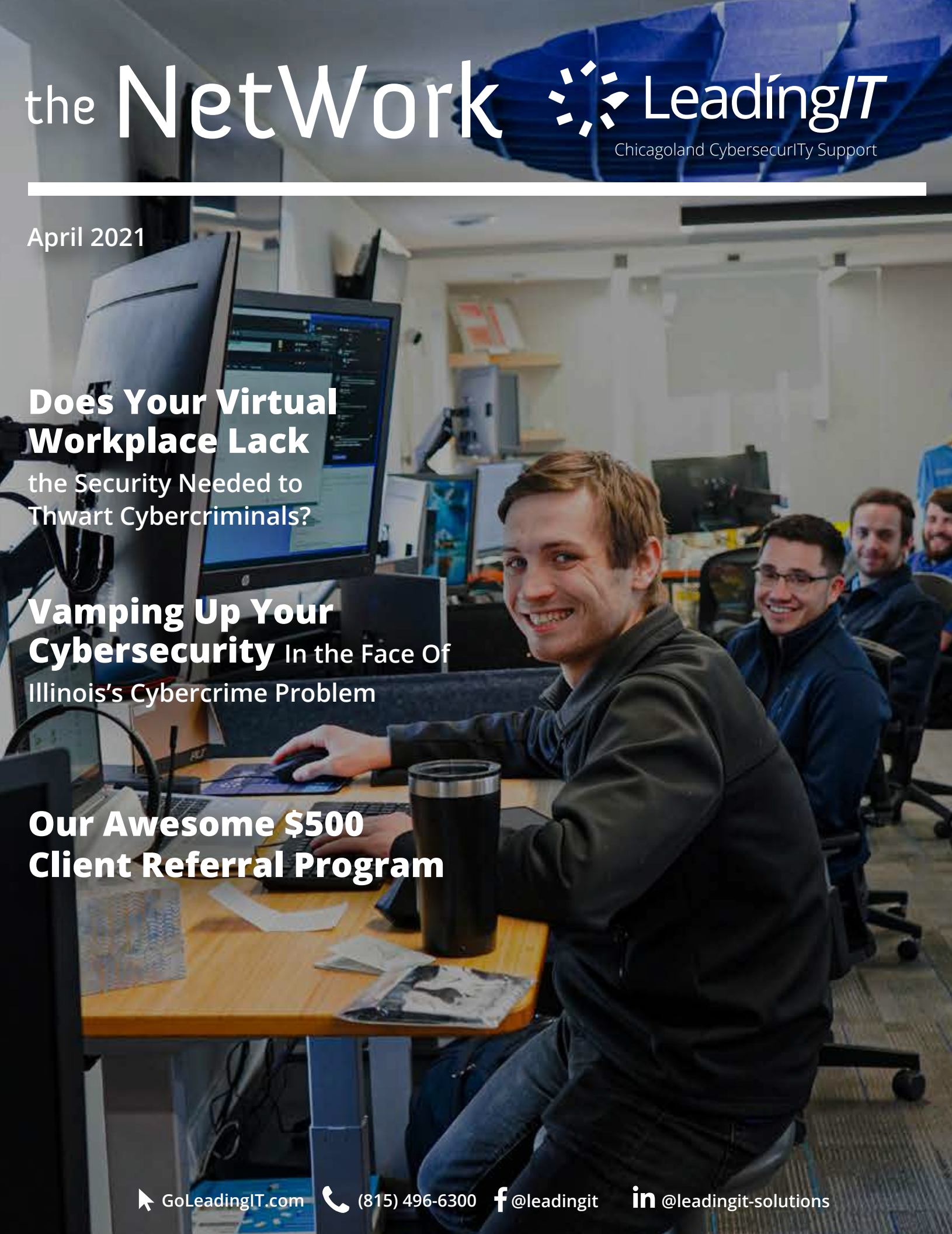
the NetWork

LeadingIT
Chicagoland CybersecurITy Support

April 2021



Does Your Virtual Workplace Lack
the Security Needed to Thwart Cybercriminals?

Vamping Up Your Cybersecurity In the Face Of Illinois's Cybercrime Problem

Our Awesome $500 Client Referral Program

Does Your Virtual Workspace Lack the Security Needed to Thwart Cybercriminals?

The past year has been full of unexpected situations — from a global pandemic that required the majority of Americans to work from home to a tidal shift in the way we do business. It's not surprising that cybercriminals have stepped into the gap that is often left when staff members shift their operations offsite or to less-than-perfectly-secure home-based office locations.

Top Cybersecurity Risks Facing Your Business

Many businesses have chosen to continue allowing remote work for some or all of their employees. The cost savings to both the staff member and to the organization can be significant, with everything from operating to transportation costs being slashed. Unfortunately, this also means that many companies have employees working on their personal PCs or mobile devices, with limited support or control from a centralized IT operation. This is causing some challenges for IT departments that are struggling to keep up with the growing demand for immediate access to sensitive corporate systems and information.

1. Endpoint Security Gaps

"Organizations of all kinds are facing an uptick in email-based threats, endpoint-security gaps and other problems as a result of the sudden switch to a fully remote workforce," says William Altman, Senior Analyst at the Global Cyber Center of NYC, operated by SOSA. Without adequate oversight, IoT devices within the organization can quickly become out of control.

2. Lack of Secure Home WiFi

Personal WiFi isn't necessarily built to have the same levels of protection as a corporate solution, with limited monitoring capabilities and only automated notifications of a potential breach or security hazard. Companies are struggling to help individuals shore up the protection for their personal connections with a wide range of solutions from network connection keys to multi-factor authentication.

3. Improper Password Protocol

Password requirements and business rules around how often passwords should be changed can quickly go by the wayside when you're faced with an army of virtual workers. Everything from mobile devices to connection portals needs to have a more stringent level of security added, or you risk falling victim to costly brute force or phishing attacks.

4. Lagging Security and Risk Management Spending

While CIO.com's 2020 State of the CIO survey showed that 34% of CIOs saw security as a major area for spending their IT budgets in the future, there are still many gaps to be filled for mid-size businesses. A commitment to spend a certain amount on cybersecurity doesn't provide the near-term protection needed to secure your organization. While companies are investigating best-practices individually, hackers are rapidly gaining ground on foiling the most common forms of security protection.

The complications introduced by a full or partially remote workforce are often more than internal IT support teams can handle, leading companies to look for options for outsourcing their IT infrastructure and operations.

Vamping Up Your Cybersecurity In The Face Of Illinois's Cybercrime Problem

When you hear about hackers, cyberattacks and cybercrime, it's easy to fall into the dangerous mindset of thinking it couldn't possibly happen to your organization. However, according to a study by Clario, 1 in 5 people have been a victim of cybercrime. In fact, the same study pointed out that Illinois has the highest number of cybercrime victims per 1000 people, totaling 14. 6 people out of 1000. People perpetuating cybercrime show no signs of slowing down, which means protecting your Chicagoland organization from potential threats takes priority.

The Costly Consequences of Security Breaches

It's a Matter of Trust

When your organization experiences a cyberattack, whether from phishing, malware, ransomware or other forms of cybercrime, you risk losing customers, vendors, and employees. Research conducted by RSA in 2019 found that 64% of Americans would blame the company, not the hacker, for the loss of personal data. A breach of trust caused by compromised security has lasting effects on an organization's reputation. The responsibility falls not just on the leader, but on the employees, too. Training employees in cybersecurity can better protect your organization and increase trust among your clients and coworkers. If the whole team has an understanding of what cybercrime looks like and the security measures you've put in place to prevent it, everyone feels more confident.

Playing the Financial Long Game

Upgrading your cybersecurity systems to match advancing technology will save you money in the long run. At the end of the day, you want to focus on achieving your goals and growing your organization.

Cyberattacks stall your progress and, just like athletes have to heal from an injury, your organization has to heal from security violations. The downtime after a data breach can put your work on hold for days, which could cost you clients and cause worry among your employees about job security. Ransomware attacks demand their victims pay a steep price, and as Forbes points out, this includes factors like "hardware replacement and repair costs, lost revenues, and, in some incidents, damage to the victim's brand." In this case, improving your securi**ty** measures saves you from potential losses.

First Steps to Fortifying Your Technology

First Things First: Start by Reviewing the Basics

There are many ways your organization can take a proactive stance on cybersecurity solutions. Features like two-factor authentication provide stronger protection than a regular password. Even this simple security measure reinforces the defenses around confidential data, since the second step required in two-factor authentication can stop potential hackers from accessing accounts. Flexible work schedules and remote working present your organization with the perfect opportunity to invest in a virtual private network (VPN) and secure cloud system. These will enable your employees to work effectively through the office network even if they're at home or finishing a project at odd hours. You should also consider what backups and data recovery plans your organization has in place. As an essential element to cybersecurity, they mitigate the dangers of data breach downtime and needing to pay a ransom to recover stolen data.

We Are Growing!

Please help us in welcoming Jacob Patterson (left) and Justin Gackowski (right) to the LeadingIT staff. Both are Level 1 techs and will be happy to assist you at the LeadingIT Help Desk.

Class Computing Has Joined LeadingIT

We are excited to announce the acquisition of CLASS Computing, a managed services provider (MSP) based in downtown Chicago, serving fire districts, park districts, non profits and businesses around Chicago.
Please join us in welcoming their team to ours!

Now Together With

classcomputing | LeadingIT

Our Awesome $500 Client Referral Program

Here is how the program works:

1. You send us your referral's contact information.
2. When they sign up, we send you a **$500 AMEX gift card**.
3. Easy.

https://www.goleadingit.com/refer/

REFERRAL PROGRAM
POWERED BY LeadingIT

WE ARE CELEBRATING!

Anniversaries
Eddie Dwyer - April 15, 2019

Birthdays
Spencer Weith - April 11th
Josh Laemont - April 28th

Read Our Blog For More
https://www.goleadingit.com/blog