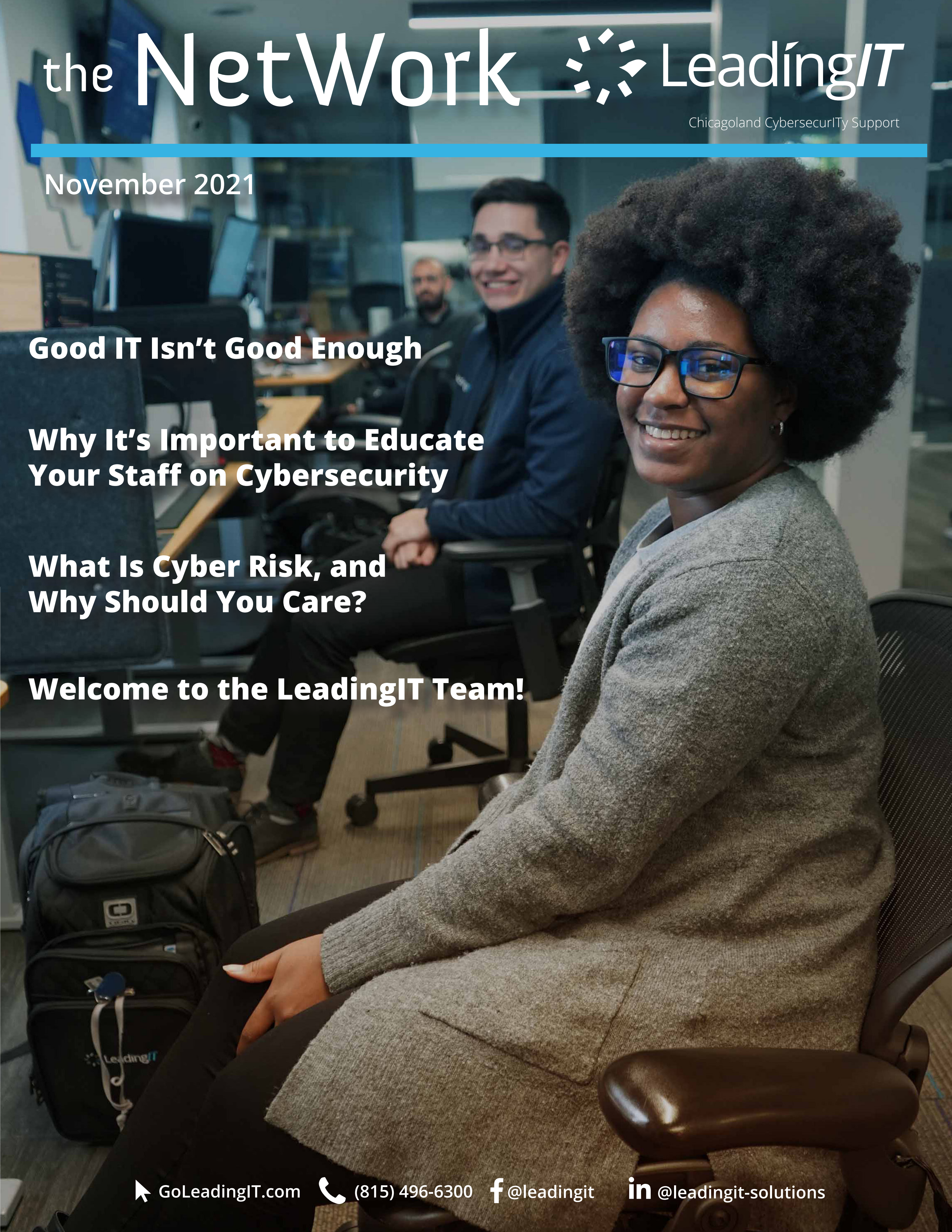

the NetWork

LeadingIT

Chicagoland CybersecurITy Support

November 2021

Good IT Isn't Good Enough

Why It's Important to Educate Your Staff on Cybersecurity

What Is Cyber Risk, and Why Should You Care?

Welcome to the LeadingIT Team!

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

Good IT Isn't Good Enough

Several business owners and managers seem to believe that their IT is good or good enough. Unfortunately, not once have we noticed alarmingly glaring glitches when we conduct preliminary scans on prospective clients' systems. So, how good is good enough?

Cybersecurity Is a Do or Die

For a long time, organizations primarily invested in cybersecurity to meet industry requirements. Others saw it as a way of marketing their businesses and boosting customer confidence in their offerings. While these reasons still hold ground, cybersecurity is no longer just a luxury—it's a do-or-die investment. Here's why:

- Ransomware is rising by the day: Over the years, ransomware has grown into one of the most lethal cyber attack vectors. With the average cost of ransomware attacks jumping to approximately $1.85 million, you wouldn't want to be a victim.
- Cyberattackers now focus on disrupting business operations: Initially, bad cyber actors targeted stealing data and blackmailing organizations to send ransoms, or they publicize the stolen information. However, going by the recent meat processing company, JBS, and other related supply chain attacks, they seem to shift their focus to interrupting business operations.
- Cyberattacks dent reputations: The adage goes—it takes several years to build a solid reputation and a single silly mistake to ruin it. The modern-day consumer is cautious about whom they trust with their data and even more skeptical about how you handle their information. If they think you cannot keep their credentials and personally identifiable information (PII) safe, such as when you experience a breach, they'll find alternatives.
- Cyberattacks are costly: According to Cybersecurity Magazine, organizations incur losses amounting to approximately $1 million for every cyberattack. By any standard, this is a huge financial setback.

What are we driving at? The cybersecurity issue is becoming more severe and is seemingly here to stay. The bad news is that everyone is a potential target and bad cyber actors keep advancing their tactics by the day. What may have been perfect yesterday may not work today. Therefore, assuming that your data security systems are always good enough might be your most significant risk. So, do you want to sit pretty and see how deep the rabbit hole goes? Or do you want to put in place proactive measures to enhance your security posture?

How to Keep Your Company's Networks Safe

1. Continuously train your staff on cybersecurity: Modern intrusion detection and prevention technologies are only as effective as your staff can use them. Therefore, you should occasionally teach your employees to identify emerging threats, first-response protocols, common tricks, information technology trends, and anything that will enhance their cyber awareness. You might also consider intermittently simulating attacks to test their preparedness levels and keep them agile.

2. Maintain reliable backups: With easy-to-retrieve and reliable backups of all your essential documents, however, you can sustain basic operations and bargain with the cyber actors when you're more collected.

3. Continually roll out new cybersecurity layers: The best way to keep threats out of your networks is using a multifaceted approach. While password complexity and expiration protocols may be an excellent way to start, the question is—what if the bad guys get hold of the passcode? And that's where multifactor authentication comes in; it adds an extra layer of security for additional protection.

Continue reading: goleadingit.com/blog.

Why It’s Important to Educate Your Staff on Cybersecurity

When bad cyber actors comprise a single gadget, say an employee’s work phone or tablet, they can access almost your entire network. It’s a no-brainer, therefore, that most cyberattacks begin with the end-users’ negligence. Your staff are your weakest link in the war against bad cyber actors, and ironically, also your first line of defense. Therefore,

Cyberattacks Are on the Rise as More Employees Work From Home

According to Global Workplace Analytics, 23-30% of all American workers will operate from home for at least two workdays in a week. The COVID-19 pandemic forced many organizations to adopt the work-from-home model without keenly evaluating their long-term cybersecurity ramifications. That has created some sort of hacker’s paradise:

- Employees are operating from less-protected home-office environments.
- Cyberattackers have a more expansive playground: With work environments scattered across various homes miles apart, hackers have more ground to practice their malice.
- Employees use unsafe devices to connect to corporate networks.

> **“Over 90% Of Cybersecurity Incidents Come From Staff Negligence.”**

Even with the most advanced threat intelligence technology and state-of-the-art security software automation, your systems are still vulnerable if your staff cannot identify and respond to threats efficiently. Bad cyber actors always look for the biggest score with the least effort, and it’s much easier to create a convincing spear-phishing email than to scout for zero-day vulnerabilities. That explains why most cyberattack vectors target employee negligence. Unfortunately, over 78% of workers understand the dangers of malignant links but still click on them, anyway.

A cyber-conscious workforce is better equipped to identify potential threats and thwart them before they get severe. With over 92% of successful data breaches and hacks resulting from staff laxity, a well-planned cyber awareness program can significantly make your systems safer.

Everybody Is a Potential Target

Some people believe that bad cyber actors mainly target IT support teams and executives with unabated access to corporate networks, but this is not true. Cyberattackers can use the most unexpected user as a backdoor to your entire system. Let’s take the recent “Shark Tank’s” host, Barbara Corcoran’s infamous phishing scam. Bad cyber actors duped her bookkeeper into paying over $400,000 into a fake Asian account. Who would have thought that they’d target the bookkeeper? Nobody.

Therefore, it’s essential to train all your staff, regardless of their roles or positions. Fortunately for Barbara, she recovered her money. But that’s not always the case. As you can see, cyber awareness training is an essential factor in the war against cyber-crime. We recommend making it a habit and not a one-time investment. That’s because bad cyber actors continually advance their tactics, and you need to keep your staff with the emerging threats.

What Is Cyber Risk, and Why Should You Care?

Technology has significantly revolutionized how we interact with one another and do business. It enables organizations to streamline operations through automation, create more targeted campaigns through AI, and derive more sales and profits. However, with all these gains comes one major challenge—cyber crime. According to Cybercrime Magazine, cyber crime will cost organizations up to $10.5 million globally in the next four years. By any standard, this will be a burden on the world's economy. Currently, one out of every five American small businesses has been a victim of either an attempted or actual cyberattack. Out of these, Vox estimates that 60% close shop within six months of the hacks or breaches. Again, this paints an oblique future for the war against cybercrime.

So, is it necessary for the public to know about the cyber risks they face? The answer is a resounding YES.

Negligence Is the Number One Reason for Cyberattacks

According to research by IBM, human error results in over 95% of cyberattacks. If you eliminate employee negligence, nine out of ten potential data breaches will not occur. Occasionally, train your users on threat detection, identification, and prevention. Teach them the different cyber attack vectors, how they manifest, and typical tricks bad cyber actors use. Your staff is your first defense line against cyberattacks, and ironically, the weakest one too. Let's take ransomware, for example—most ransomware attacks begin as phishing scams. Phishing is essentially cyber attackers using false identities to dupe your users into divulging critical credentials like logins. The actors target human negligence to gain entrance into your networks. So, the more informed and "cyber security-savvy" your staff is, the less your company's chances of falling prey to ransomware and other cyberattack vectors.

Continue reading: goleadingit.com/blog.

Welcome to the LeadingIT Team!

We are excited to introduce the newest additions to the LeadingIT staff. Amie joins us as a Level 1 technician and Garrett joins us as a Level 3 technician.

Amie

Garrett

LeadingIT

Serving the Chicagoland area with offices in Woodstock, IL and now in downtown Chicago.

Check out our blog at goleadingit.com/blog

WE ARE CELEBRATING!

Anniversaries

Peter Apostle - 11/25/2019

Laura Piekos - 11/26/2018

Birthdays

Dale Schwer - November 30th