Welcoming the Class Computing Team to LeadingIT!

We are excited to introduce our new team members joining us from CLASS Computing!

Please join us in welcoming them to LeadingIT!

Mike

Mark

Jose

Anthony

Dale

Looking to Improve Your Company's Online Digital Experience?

At LeadingIT we partner with LuccaAM for all our creative needs. Our mutual clients benefit from our partnership and often experience shorter turnaround times than through 3rd party vendors.

LuccaAM is a digital creative agency who can assist your company with:

- Web Design and Development
- Creative
- Social
- SEO
- Google Ads and Facebook Advertising
- Content Creation

Contact us to learn more!

(815) 880-8676
hello@LuccaAM.com

LUCCA AM

WE ARE CELEBRATING!

Anniversaries	Birthdays
Spencer Weith - June 23rd, 2020	Jeremiah Bird - June 15th

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

the NetWork

LeadingIT
Chicagoland CybersecurITy Support

June 2021

8 Most Common Cybersecurity Issues Organizations
in Chicagoland Face

Not All Backups
Are Created Equal

Welcoming the Class
Computing Team to LeadingIT!

Looking to Improve
Your Company's Online Digital Experience?

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

8 Most Common Cybersecurity Issues Organizations in Chicagoland Face

Cybercrime is on the rise. According to Statista, about 1,001 data breaches were reported in 2020, and about 155.8 million records were exposed. Although this is well known in the business environment, most businesses still practice poor cybersecurity habits. These habits are slowly becoming a norm in the office, especially since they make work a little manageable.

What Are the Most Common Issues Facing Almost Every Chicagoland Organization?

1. Thinking That You Can't Be a Target
Small businesses are just as vulnerable as large companies when it comes to cyberattacks. According to a report by Verizon, in 2019, 43% of reported cyberattacks targeted small businesses. The growing number of cyberattacks targeting small businesses is growing because cybercriminals have realized that SMBs are negligent in their security and don't have proper cybersecurity solutions. Some companies also tend to get overconfident once they've implemented all the security controls.

2. Treating Your Cybersecurity as a One-Time Project
Your cybersecurity isn't a one-time project. You can't just set it up and wait for it to work its magic. Cyberthreats are continually evolving, and cybercriminals are coming up with more advanced and sophisticated ways of accessing your sensitive data.
Your cybersecurity measures need to evolve just as much to ensure the safety of your data. Frequently revisit your cybersecurity policies, procedures, and controls and test them against new cyber threats to determine their efficiency.

3. Not Offering Employees Comprehensive Security Awareness Training
According to Cybint, 95% of cybersecurity breaches are caused by human error. Hackers usually infiltrate companies through their employees, which are the weakest link in the cyberattack cycle. Social engineering attacks are typically targeted at your employees and pose a significant cyber threat to your businesses. If your employees know how to identify these attacks, they can easily prevent them and save your company a lot of time and money in downtime and ransoms.
Training your employees on cybersecurity controls and measures is the first step to having comprehensive cybersecurity. Training of employees should also be continuous to reshape old habits and be at par with new cyber threats.

4. A Lack Luster Password Policy
Using short and easy-to-guess passwords and using them across multiple company devices for a long time puts your company at risk of cyberattacks. On the other hand, long and complex passwords may be challenging to remember forcing your employees to write them down somewhere or share them with friends and family members so they don't forget them. Such poor password management tactics make it easy for hackers to log in to your account and steal your data. Your passwords should contain letters, numbers, and special characters. They should also be updated regularly, and the same password shouldn't be used for all your devices.

5. Neglecting Multi-Factor Authentication
Employing multi-factor authentication adds an extra layer of protection in your login process and makes it difficult for hackers to get access to your accounts. You can use MFA together with strong passwords to restrict intruder access.

6. Using Outdated Software and Programs
Another mistake that businesses make is not updating the programs and software they use. Most companies tend to ignore update notifications or delay installation. Using outdated versions of programs is like luring a hacker.

Your computer's operating system and all the programs you use need to be updated regularly, not just the versions but also the databases. Keeping program databases up to date helps you protect your computer from the latest cyber threats. Updates of programs fix security loopholes that hackers might easily penetrate.

Make a policy of updating your software, operating system, and programs regularly and as early as new versions are released.

Not All Backups Are Created Equal

There are more than 31 different flavors of backup solutions, and probably every service provider will tell you that theirs is the best. So, how do you identify the perfect backup system for your organization? What would you do if your organization lost all its data? If you wake up one day and find all your databases, websites, and essential apps are inaccessible or wholly wiped out—it happens to the best of us. You're probably thinking, "I'll rely on the backup." However, backup is an extensive and generic term. It can mean duplicating a few critical files and storing them in an offsite location, making carbon copies of entire servers, copying files, and pasting them in separate onsite databases, among many others. That's why we insist that as a business owner or manager, you should deeply interrogate the features of a backup solution before trusting it. What are its rewards, pros, and cons?

Questions You Need To Ask Your IT Service Provider

1. Does the Backup System Have High Availability?
Imagine suffering a data loss and turning to your backup only to discover that its server was offline and your critical data is missing. Or finding out that the backup system has been regularly offline, and your scheduled backups haven't been taking place. Your backup provider should guarantee a high availability solution that stays online most of the time. We recommend a minimum availability of 99.95%.

2. How Reliable is the Backup Service's Disaster Recovery Plan?
You list the services of a backup provider in case anything happens to your onsite database. But what if it's the provider's servers that are compromised? Worse still, what if both your local servers and the backup system's servers go down at the same time? Before you enter into a contract with a backup provider, you should ensure that they have a reliable disaster recovery plan. For instance, a good provider will have multi-location data centers that run simultaneously. So, if one of the centers goes down, say due to a fire accident, they will immediately bring copies from one of the alternative locations online.

3. How Frequently Does the System Back Up Your Data?
If you're operating a busy e-commerce venture, for instance, you may need more frequent backups than the average business. The backup frequency usually depends on the amount of data you process. Some providers allow their clients to control the frequency and even timing of their backups. However, if the vendor regulates these factors, you should ensure that the backups are frequent enough not to lose any recent data in case of an incident. We recommend at least two backups a day if your organization is not that busy.

4. What's the Backup System's Storage Space Limit?
Most backup service providers charge clients based on the amount of storage space they've used. However, if the provider bills per user, they may limit the amount of data backed up from every workstation. Find out if there are storage limits, and if any, is it enough for your backup needs? While renting storage spaces is pretty inexpensive compared to buying personal servers, you may still want to look at individual providers' rates. Take the size of one backup and multiply it by the number of backups you need.

5. Is the Backup System's Storage Space Scalable?
As your organization grows, your backup storage requirements equally increase. Sometimes, the increase may be temporary due to occasional large-scale projects or peak seasons.
You need a backup solution that allows you to scale your storage space up or down on a need basis. This way, you avoid cases where you've paid for excess or too little space.

6. Is the Backup System Safe Enough?
As much as you put the necessary cybersecurity measures in place to safeguard your local databases, you must also ensure that the third-party backup provider you trust with your data does the same. Otherwise, bad cyber actors can use them as backdoors to access your sensitive information.
Ideally, they should have every security measure that you have and more. These include robust intrusion detection and prevention systems, proper data encryption (during storage and transfer), SSL, and several data centers, among many others. Also, they should have on-site security personnel and CCTV cameras monitoring their physical data centers 24/7.