the NetWork

LeadingIT

Chicagoland CybersecurITy Support

August 2022

- Email Cybersecurity Should Be Your Company's Top Priority
- Are You Eligible For Cyber Insurance?
- 4 Cybersecurity Challenges Faced By CEOs Today
- LeadingIT Employee Spotlight

GoLeadingIT.com ☎ 815-893-2525 in @leadingit-solutions

Email Cybersecurity Should Be Your Company's Top Priority

Although it brings a myriad of benefits, email systems can be quite risky if they don't have a reliable cybersecurity plan. This might seem like common knowledge to some, but the fact remains that up to 50% of small businesses do not have a cybersecurity plan for 2022, with many citing cost as a major player in their decision.

Your company's email system is a prime target for a data breach. Hackers and scam artists target email systems because they provide an easy way to deceive unsuspecting victims. Contrary to popular belief, the commonly used cloud-based email systems, such as Gmail, simply do not provide enough built-in security to protect businesses from threats.

Email remains one of the most common and necessary ways to communicate in the business world. It provides organizations with an efficient, instant way to communicate with colleagues, customers, and vendors. So, having an effective email security protocol is essential to a company's success.

3 Major Risks of Having No Email Security Protocol

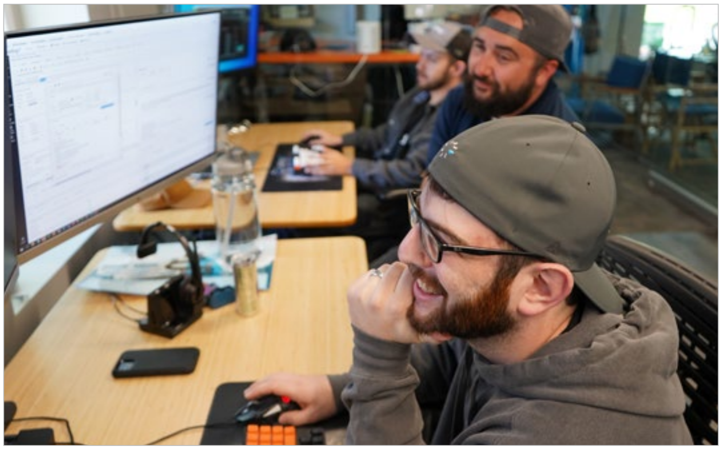
Attackers are commonly looking to gain some sort of control over servers, which gives them access to sensitive information and files. Without a proper security protocol, your email system can be vulnerable to a multitude of risks.

Malware

Criminals like to use malicious software (malware) to attack servers. This includes anything from putting in viruses to introducing spyware to a company's system. If their efforts are successful, hackers can gain unlimited control over a company's servers. Once they do, they can do a variety of things such as altering permissions and viewing sensitive information.

Spam and phishing

Spam typically involves the act of sending unsolicited emails to disturb systems and subsequently introduce malware into those systems. Phishing is like spam, but it takes things one step further. The scammers try to trick unsuspecting victims into believing they're someone else. If they can, they attempt to intercept sensitive information from the individual or introduce malware in a more sophisticated way.



Steven and Collin

Identity theft

Identity theft is a common result of a phishing attack. Scammers start by getting information like emails and passwords and then use them to intercept as much information as possible. This can result in the scammer using the information to act like the victim in future attacks on other organizations.

Let's mitigate those risks!

While many attacks are easy to identify, there are still quite a few that are sophisticated enough to trick an unsuspecting business. For this reason, it's imperative to hire a trusted cybersecurity-focused provider to help mitigate risks.

Don't be one of the 60% of small to mid-sized businesses that shut down within 6 months of a data breach. A reliable cybersecurity professional can help by providing the support and expertise you need, including:

- Regular staff training exercises on cybersecurity
- MFA (multi-factor authentication)
- Server backups
- Continuous system monitoring

All these services work in unison to provide businesses with the utmost level of email security so they can focus more on work and less on criminals trying to hack their systems. Many times, it's the lack of education from staff members that contributes to a successful hacking attempt.

Pictured on the cover: Collin and Nathan

Are You Eligible For Cyber Insurance?

Cyber insurance is a growing segment in the insurance market, but adoption is still low. According to a survey by the Insurance Information Institute, less than half (40%) of small businesses report having cyber liability coverage. Even within larger companies, the adoption rate of cyber insurance remains low because many business owners are either unaware of its existence or are intimidated by the cost and complexity of procuring it.

Buying cyber insurance isn't like buying a vehicle, home, or business liability coverage from an agent. Cyber rates are based on projected and previous losses and claims, the prospect's risk profile, and other risk-related factors. To learn more about cyber security eligibility requirements, read on.

Why Do You Need Cyber Insurance?

When hackers make off with your customer's personal data, it's bad news for your company and customers. In the aftermath of a cyber attack, businesses are left to pick up the pieces and figure out how best to move forward. Some lose customers. On the other hand, 60% of small companies go out of business within six months following a data breach or cyber attack.

That's where cyber insurance comes into play. Cyber insurance can help you recover after an attack by covering some or all of the costs associated with cleaning up after a breach. In addition, insurance may cover lost productivity and customers.

So, How Do I Get Insured?

Your cybersecurity system will need to go through a similar examination as you would if applying for life or health insurance. To protect their own interests and assets, cyber insurers require that organizations follow a set of standards and best practices before issuing a policy.

Marsh McLennan Agency (MMA), which services global clients, reports 12 security controls considered essential, but five considered the most critical for coverage

- Multi-factor authentication: A layered approach to data and application security where a user must show two or more credentials to log in.
- Endpoint detection: A system that continuously monitors end-user devices for ransomware and malware.
- Reliable backups: Backups that are secure, encrypted, and tested.
- Privileged access management: An information security method that protects special user IDs.
- Email filtering and web security: A system that filters harmful emails or websites.

Investing In Your IT Solutions Is Key.

The good news is that your investment in cyber security solutions and IT services will increase your eligibility. Also, your business will be better protected if it meets cyber insurance company criteria.

4 Cybersecurity Challenges Faced By CEOs Today

A 2021 Insider Data Breach Survey found that 94% of organizations have experienced some variation of an insider data breach. Having the proper cybersecurity protocols in place is important for every business in today's digitized world. If you're a CEO, it's likely that you've experienced a serious data breach or know of someone who has.

The main culprit? Human error. But, despite knowing this, most leaders remain more concerned about intentional, malicious behavior instead of things like employee carelessness or ignoring security rules.

While malicious behavior (both internally and externally) is part of the issue, there are definitely other factors to consider. On that note, there are four primary cybersecurity challenges faced by CEOs today.

1) Lack of Employee Education

As previously mentioned, human error is the primary cause of data breaches. Why does this happen? Simply put, most employees are under-educated in the cybersecurity space. Breaches are often caused by an unsuspecting employee downloading a malicious file, which introduces malware into their company's network.

Cybersecurity training is important for organization to implement because it teaches employees how to recognize and protect against cyber-attacks.

2) Ransomware

It's imperative for business leaders to have an effective solution for dealing with ransomware. The harsh reality is that most businesses cannot survive a serious ransomware attack, and business leaders' responses to such attacks generally make matters worse instead of better.

Continue reading on page 4

LeadingIT Employee Spotlight:

Peter

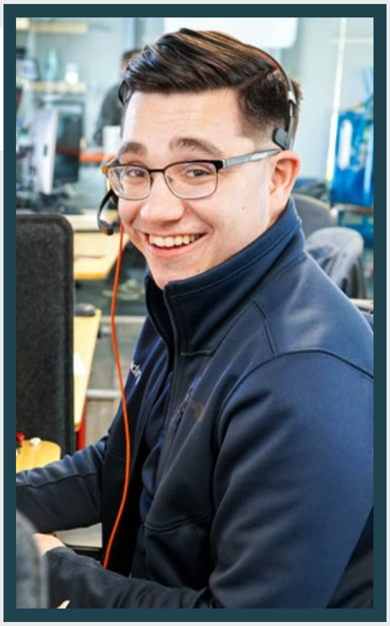
Level 1 Manager

- ***What drew you to LeadingIT originally?***

I was working part time as an intern as internal IT at a data company in Chicago and I was looking for my first real IT job that would bring me to the next level. LeadingIT was close to home, looked professional, and while I knew nothing about the sector, I was very excited to have the opportunity to interview. It felt like a good fit for me prior to joining, but the real draw came from the work I was doing, the knowledge I was gaining, and the people I was working with.

What has working at LeadingIT been like?

I have learned what feels like a decade of experience condensed into 2 ½ years because of the diversity in our client base and the hours and hours of training with coworkers.



If you could switch positions with anyone at LeadingIT who would it be and why?

If I had to absolutely choose to swap, I'd swap with a Level 3 technician. I enjoy project work and would like to show more of that side of myself.

What would you say to someone considering a career with LeadingIT?

The focus that we put on developing our employees should catch your attention and for good reason. If you value a flexible and understanding environment, look no further. Learn everything you can and never stop asking questions.

Which benefits are your favorite?

Certifications being paid for.

What was your childhood dream job?

I wanted to design rollercoasters, even though I was and still am afraid of heights. I also considered helicopter pilot when I got older but again, afraid of heights.

Cybersecurity Challenges continued...

3) Cyber Insurance

Too many companies fall into one of the following categories: they have inadequate cyber insurance, or they didn't know such a policy ever existed. Most companies assume that their existing property damage or related policy covers cybersecurity issues. The reality is that most organizations end up realizing they are responsible for an entire loss from a cyber incursion only after it's too late.

4) Budgeting

The pandemic has forced companies to revisit their budgets and make major cuts just to remain afloat. This has led to many citing budgeting concerns as a reason why they cannot maintain adequate cybersecurity protections. Fortunately, there are affordable options out there that could very well make all the difference in protecting a business from a major attack.

LeadingIT

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

Check out our blog at goleadingit.com/blog

WE ARE CELEBRATING

Birthdays

Stephen Taylor - August 11th
Justin Gackowski - August 14th
Jose Ledesma - August 26th
Collin Saunders - August 26th
Mallory Hale - August 30th

Anniversaries

Jeremiah Bird - 8/24/2020
Amie Koster - 8/18/2021
Garrett McCleary - 8/16/2021