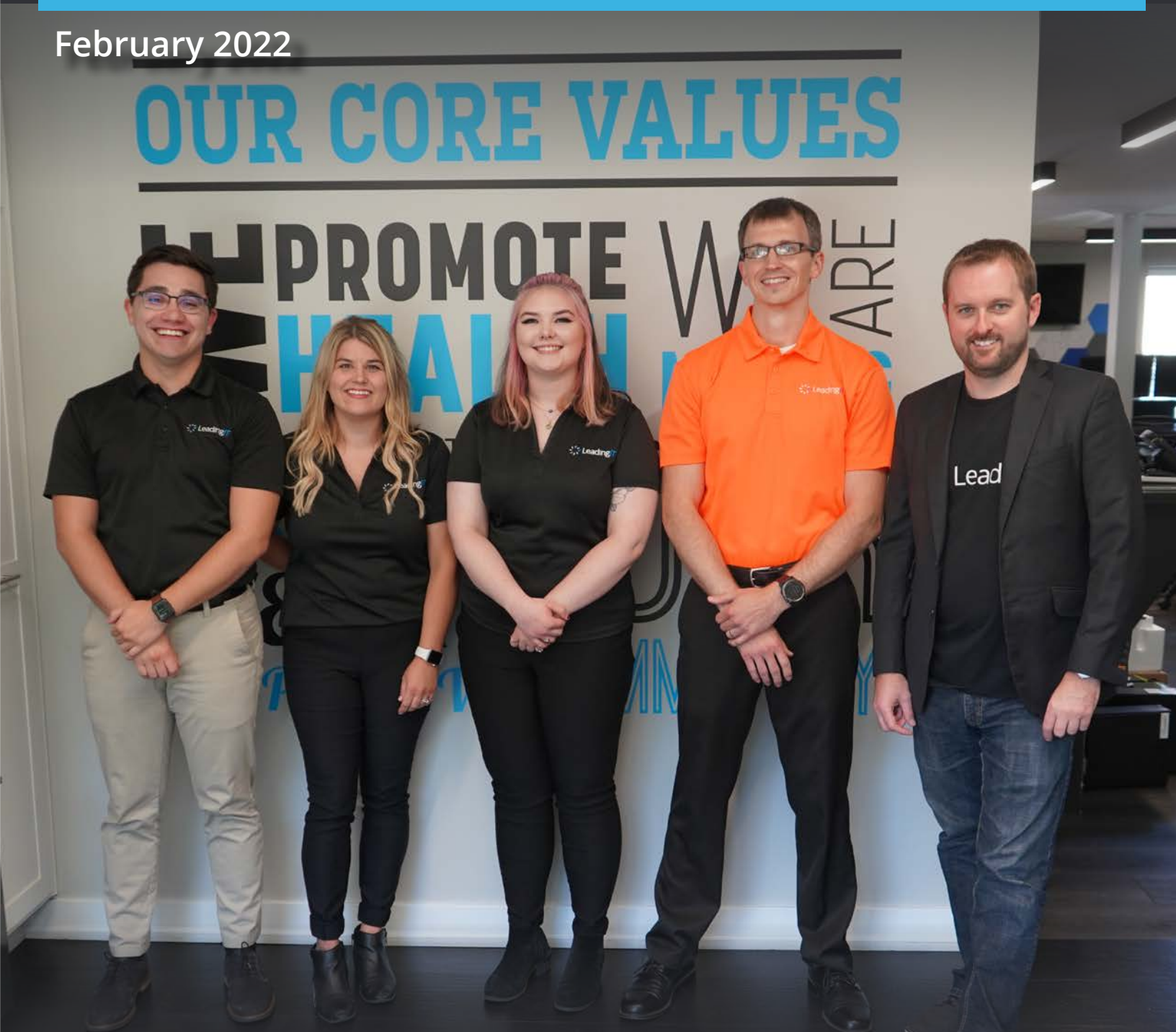
the NetWork

LeadingIT

Chicagoland CybersecurITy Support

February 2022



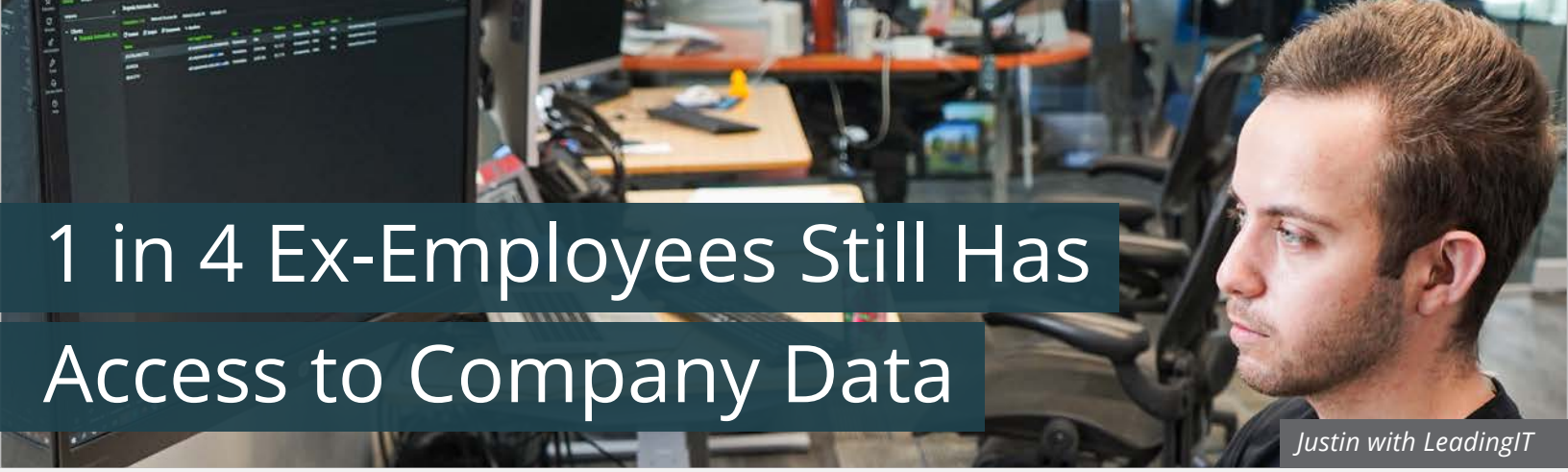
Budgeting for Ransomware Protection: Essential in 2022

1 in 4 Ex-Employees Still Has Access to Company Data

Only 46% Of SMBs Have Password Management in Place

We love our clients!

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



1 in 4 Ex-Employees Still Has Access to Company Data

Justin with LeadingIT

According to a recent study by Beyond Identity, approximately 25% of employees can still access their past workplaces accounts and emails. What's even more worrying from the report is that over 41% of these employees admitted to sharing their former workplace logins. So, as you're strategizing to safeguard your systems from hackers, what are you doing to avert the threats from former employees?

How Many Former Employees Can Still Access Your Data?

The simple answer is — more than you may imagine. Based on the Beyond Identity research, one in every four former employees can still access emails and accounts from their former workplaces. A similar study by Identity and Internet Access Management (IAM) provider, OneLogin, suggests that this figure could be as high as 50%.

The OneLogin study gives a clearer picture of the number of former employees who can still access past workplace apps, emails, and accounts. According to the survey results:

- 70% of companies take approximately one hour to de-provision one employee from all the corporate application accounts
- 50% of former employees' accounts remain active for longer than a day after leaving the workplaces
- 48% of organizations are aware that former employees can still access corporate applications
- 32% of organizations said that it takes over seven days to fully de-provision a former employee
- 20% of former employees' accounts stay active for up to a month after leaving the workplace
- 25% of employees do not know how long former employee accounts remain active after leaving their workplaces

The bottom line is that most companies do not take the de-provisioning of former employees' applications and accounts seriously. Out of the 500 US-based IT decision-makers who responded to the OneLogin survey, over 100 admitted that failure to terminate network access by former employees contributed to data breaches at their companies.

Why Should You Terminate Former Employee Access Privileges Immediately?

Most of the employees who leave your company may not even be thinking of logging back into your network, but you can't miss a few rogue individuals. While these individuals may not be that many, you cannot overlook the threat they pose:

- ***Data loss:*** When you lay off employees, some of them may not take the termination of their contracts kindly. The disgruntled ex-employees may look for ways to take revenge by deleting or compromising your organization's critical files. A perfect example is the former IT administrator at Lucchese, who shut down the boot manufacturing company's servers and deleted crucial files when he lost his job.
- ***Data breach:*** According to a recent study by the Ponemon Institute, over 50% of employees have stolen data from former employers. Out of these, 40% said they intended to use the stolen information in their new workplaces.
- ***Wasted spend:*** Former employees using your G Suite, Office, and other work environment licenses may increase your service bills. Worse still, the service providers may continue billing you for unused accounts that you haven't terminated.
- ***Breach of confidentiality:*** The present-day business environment is data-driven. You rely on data to make almost every critical business decision. Therefore, it's common for companies to poach employees from rival organizations to access confidential information.

Continue reading: goleadingit.com/blog

Pictured on the cover: *Peter, Laura, Mallory, Dave, Stephen*

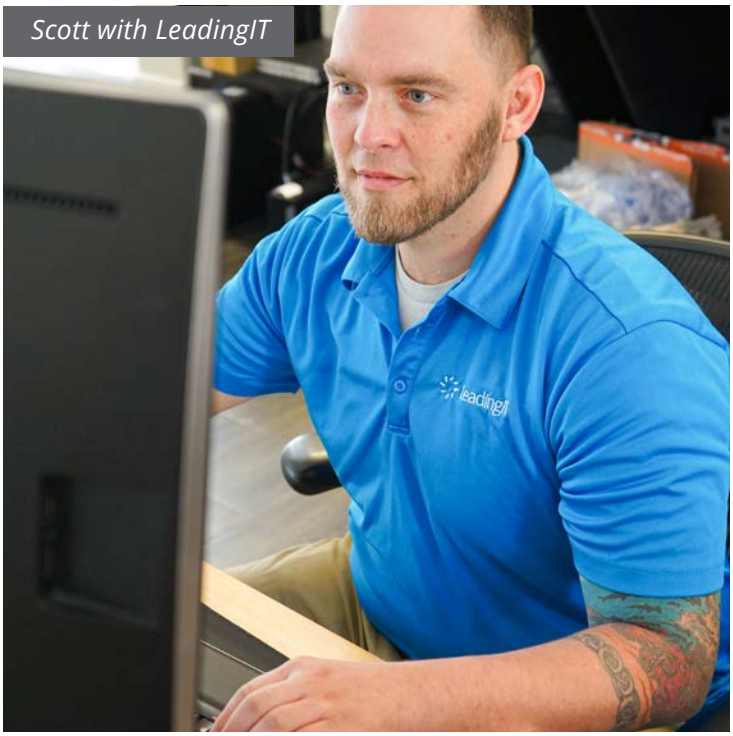
Budgeting for Ransomware Protection: **A Business Essential in 2022**

According to Cybersecurity Ventures, businesses record a new ransomware attack every 11 seconds. With Symantec estimating that the U.S. accounts for up to 18.2% of global ransomware incidences, there is enough reason for your Chicagoland business to be concerned. So, how well is your organization prepared to shield its systems from ransomware? Does your CFO have a budget for ransomware prevention? In this article, we discuss what ransomware is, explore reasons you should be concerned about, and explain why you need a ransomware prevention budget.

What is Ransomware?

Ransomware is a cyberattack vector involving cyber actors introducing malicious software (malware) into your network to encrypt your data or computer systems. The encryption blocks access to your files until you pay ransom to the cyberattackers.

So, how do the bad guys introduce malware into your systems? According to CSO Online, cyberattackers deliver 94% of malware through emails. Typically, you will receive an email purportedly from trusted sources. The email contains a malicious link, file, or image and a message that prompts you to open them. When you click on these attachments, they redirect you to a page that mines your credentials or automatically introduces malware into the organization's network. Approximately 48% of these malicious attachments are Office files, making them challenging to identify.



Scott with LeadingIT

Why Should You Care?

Ransomware has been around for a very long time. So, why should you care now more than ever? Here's why:

Ransomware Cases Are Continually Increasing

While almost all cyberattack vectors increased in 2021, ransomware received the most attention. From the Colonial Pipeline to Brenntag to Acer, JBS Foods, Quanta, NBA, and Kaseya, the list of businesses that suffered ransomware attacks this year is endless.

Ransomware Is Expensive

Initially, ransomware attacks were pretty simple — hackers would encrypt personal gadgets and demand a few dollars for decryption. Over the years, it has evolved into one of the most lethal and costliest cyberattack vectors.

Budgeting for Ransomware Protection Is No Longer Optional For Businesses

On the surface, investing in cybersecurity may seem costly. Why spend thousands of dollars annually on safeguarding your business against a threat that you're not even sure will befall you?

It's a no-brainer that most small and medium-sized businesses opt for random IT Guys who they call when necessary. This option always seems better than outsourcing IT support until you become a victim of a ransomware attack and your fears become a reality.

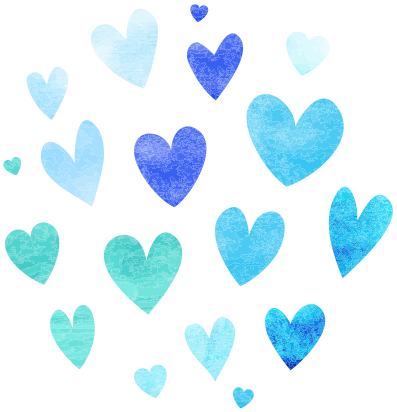
Here's the thing—technology can empower your organization to do more, perform better, and run faster. However, without the best IT support, it exposes you to the risk of ransomware attacks, which can bring your business to its knees overnight. That's why with cybersecurity and ransomware prevention, there's no option but to have the best support available. ***So, why should your Chicagoland business have a ransomware prevention budget?***

- Everyone is a potential target
- It's less costly to invest in ransomware prevention
- Investing in ransomware prevention enhances your cybersecurity posture

WE ARE CELEBRATING

Birthdays

Jason Frederick Jimenez
February 9th



We love our clients!

Show us some love by sending us some great referrals!
We'd love to sweeten the deal by rewarding you for the referral.
Visit **goleadingit.com/refer** for more details.

REFERRAL PROGRAM
POWERED BY LeadingIT

LeadingIT

We Protect Your Chicagoland Organization From Ongoing CybersecurITy Threats.

Check out our blog at goleadingit.com/blog

Only 46% Of SMBs Have Password Management in Place

Your passwords are the primary line of defense in safeguarding your sensitive data from unauthorized access.

They act as barriers between the bad guys and the organization's systems. According to the 10th edition of Verizon's Data Breach Investigation Report, over 80% of hacking-related breaches begin with compromising passwords. That shows you how integral password management is in the fight against cybercrime.

Ironically, less than half of small and medium-sized businesses already have password management in place. Last Pass' 2021 study on the state of SMB password management shows that only 46% of SMBs globally have invested in password management. The research also shows that 51% of business executives consider passwords the most crucial identity and access management solution.

Most SMBs understand the vitality of password management but haven't invested in it. Why is that so? What is password management, and why is it crucial? What are the password management best practices?

What is Password Management?

Password management can refer to using sustainable practices to create, store, and maintain passwords throughout their life cycles. It involves developing organization-wide policies and deploying a Password Management System to ensure that users always have strong and complex passwords. The goal is to safeguard your logins from unauthorized access and compromise.

Password management is crucial now, more than ever, because of the central role that data has taken in the day-to-day operations of businesses. In this information age, organizations rely on data to plan policies, plan and track growth, measure performances, design marketing strategies, and make crucial business decisions. How well you collect, store, and use data can give you a competitive edge or disadvantage your business.

The bad guys know this pretty well and will stop at nothing to compromise your files and stall your operations. With the increased integration of technology into business processes and adoption of the work-from-home model, your data is more vulnerable to unauthorized access than ever. Today, employees access corporate systems from several less-secured environments miles away. You expose your data to more risks as you broaden your network and increase your assets.

Continue reading: goleadingit.com/blog