the NetWork

LeadingIT

Chicagoland CybersecurITy Support

September 2022

Would Your Organization Survive A Cyber Attack?

The Importance Of Least Privilege To Your Security

The Benefits Of Cybersecurity

LeadingIT Employee Spotlight

GoLeadingIT.com 815-893-2525 @goleadingit

LeadingIT team

Would Your Organization Survive A Cyber Attack?

THE COSTS OF A CYBER ATTACK

From Target in 2013 to MGM Hotels in 2021, large-scale cyberattacks on major corporate companies always make the headlines. Unfortunately, many attacks on small to medium-sized businesses (SMBs) don't make the news, but that doesn't mean they aren't at risk. SMBs account for 43% of all data breaches, and 61% of SMBs reported at least one cyberattack in the last year. However, small business does not imply small costs. A data breach may cost a small business anything from $120,000 to $1.24 million.

Companies Aren't Prepared

It stands to say that cyber attacks are a threat to any business, from Amazon to a small online business. Unfortunately, many small to medium-sized companies aren't prepared to deal with a cyber attack. In fact, a 2020 study revealed that 43% of SMBs don't have any cybersecurity solutions in place.

If this describes you, then it's likely that your business may not survive a cyber attack. According to CyberCatch, 75% of SMBs would be forced to close shop in the case of a ransomware attack. The damages of cyber attacks are significant.

Financial Damage

As stated earlier, the costs associated with a cyber attack are expensive, even for a small business. Studies have shown that 83% of small and medium-sized businesses are unprepared financially to recover from a cyber attack.

However, it's not only the monetary amount that may sink a corporation; it's the disturbance to operations. CISCO reported that 40% of small businesses hit by a major cyberattack had at least 8 hours of outage. Downtime is a primary cost of a security breach.

Reputation Damage

Customers are selective of the companies they work with because of the growing threat of security breaches. If your company experiences a data breach, it could impact its reputation and customer willingness to do business with you.

In addition, the reputational ramifications of a data breach may last longer than the short-term consequences, harming your bottom line when consumers don't trust you.

Legal Damage

Companies might face severe legal consequences after a breach if customers are affected. The fines and settlements imposed on companies can quickly add up.

After an attack, Home Depot paid credit card issuers and banks $134.5 million. Home Depot paid hack victims $19.5 million in 2016, including credit monitoring. In 2017, the business agreed to pay $25 million to affected banking institutions.

Investment Is The Key To Preventing Attacks

The danger of a cyber attack is ever-present, and it's important to know how prepared your organization is should one occur. Investing in cybersecurity solutions and ransomware protection is the best prevention to ensure the survival of your organization.

Pictured on the cover: Justin, Steven and Jeremiah

The Importance Of Least Privilege To Your Security

In the digital world, cyber threats are prevalent and can have a devastating impact on businesses. As technology continues to evolve, so do bad actors' methods to access sensitive company data. Now is the time to upgrade outdated security systems and implement practices that protect your company from the inside.

A 2019 Centrify survey revealed that 74% of IT decision-makers whose companies had data breaches said hackers exploited privileged credentials. Companies can protect themselves from this cyber threat by implementing the principle of least privilege.

What Is The Principle Of Least Privilege?

The least privilege principle reduces risk and increases your system's security by limiting the privileges or access rights granted to users. With this cyber security model, users should be granted only the minimum privileges necessary to complete their tasks. In other words, it gives users only the permissions they need to perform their job and no more.

Many businesses may feel protected enough by their other cybersecurity solutions. However, surveys and testing have revealed that in 93% of cases, an external attacker could infiltrate a company's network perimeter, and access due to credential compromise accounts for 71% of these cases. This aligns with Forrester's prediction that 80% of security breaches result from compromised privileged credentials. For this reason, along with a few other benefits, implementing least privilege principles is essential for protecting your company.

Benefits Of The Principle Of Least Privilege

Reduces Liability

Issues might arise when someone accesses data, applications, or a network without permission. More open doors bring more liabilities and concerns, whether a curious employee or a bad actor. The least privilege access strategy reduces bad actors' attack surface. Fewer doors mean less possibility of an incident.

Increases Ransomware Protection

Ransomware is a common and expensive threat. Since January 1, 2016, there have been over 4,000 ransomware attacks daily. By strictly restricting who has access to important systems, you limit the chance of ransomware and other malware attacks because the user or their operating system will not be able to install them.

Continue reading on page 4

The Benefits Of Cybersecurity

Today's digital world is filled with risks. As businesses become more reliant on cloud services and Internet of Things (IoT) devices, potential internal and external cyber threats, such as ransomware, misused credentials, and data breaches, also increase. However, you can reduce this risk by implementing cybersecurity solutions.

An article published by Forbes in 2021 states that Silicon Valley startups are no longer the only companies that need to worry about cybersecurity. Every business owner must grasp cybersecurity basics and implement a strategy to protect against threats. A strong cybersecurity strategy can help you create value and drive business success.

A few important benefits of implementing cybersecurity solutions:

- Peace of Mind
- Compliance with Regulations
- Improved productivity
- Protecting your company's reputation

The Benefits Outweigh The Risks

Implementing a comprehensive cybersecurity plan and investing in cybersecurity companies will cost some money upfront. But you'll save money in the long run by preventing cyber attacks, ransomware, and business closure from occurring.

LeadingIT Employee Spotlight:

Mallory
Office Manager

What has working at LeadingIT been like?

A very positive change of pace. I came from a work environment that worked you to the bone, physically and mentally drained you, not allowing any time for oneself. Not to mention the lack of employee recognition and compensation. LeadingIT has shown me that a healthy and positive work environment is possible, alongside employee recognition and respect.

In your time at LeadingIT, what has been your favorite project?

I thoroughly enjoy assisting marketing with projects and cleaning up the prospect database. Knowing that we are making it as clean, organized, and accurate makes me feel very accomplished.

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

Go for it. The company is growing fast, and new positions are being created more frequently. If you are looking for somewhere to grow, learn, and expand with, I feel LeadingIT is a perfect place to start.

Which benefits are your favorite and why?

The set schedule and PTO for sure. Having a set schedule has allowed me to have more time for myself, family/friends/my significant other, as well as the ability to plan out vacations without any worry.

What was your childhood dream job?

An Astronomer. I have always been interested in space and astrology since I was little. It is the first "big" dream job I thought of.

Looking for a career change? Check out our open positions at goleadingit.com/careers.

The Benefits Of Cybersecurity continued...

Improves Data Classification

The least privilege principle requires network managers to maintain detailed access logs. Auditing, categorizing, and arranging data is necessary to implement the least privilege principle. IT support services can use this information to track the origin of a cyber attack. Network admins can identify the compromised asset, see who has access to it, and investigate it. In addition, keeping this data structured and audited helps companies fulfill HIPAA and HITECH regulations.

Least Privilege Access Prevents Catastrophes

Best practices for cybersecurity and data protection go beyond perimeter defense. Hackers can use privileged accounts to access sensitive data. The least privilege model locks doors if a bad actor enters an organization's network.

If a business doesn't follow this approach, compromised data, stolen information, or a ransomware attacks become real possibilities. Conversely, companies that learn, adapt, and use least privilege access principles are better protected from cyber threats.

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

Eric Elsbury - September 22nd
Amie Koster - September 22nd

Anniversaries

Katelynn Ware - 9/28/2021