the NetWork

LeadingIT

Chicagoland CybersecurITy Support

August 2024

An SMB's Ten Step Guide to Cybersecurity Strategies

Data Breaches and Data Privacy: Keeping Your Information Safe in an Increasingly Connected World

Making The Most of Your Tech Budget Through Goal Prioritization

What's Causing the Wave of Healthcare Cyberattacks?

LeadingIT Core Values Victor of the Month

GoLeadingIT.com 815-788-6041 @goleadingit

An SMB's Ten Step Guide to Cybersecurity Strategies

To keep your business's operations running smoothly, you want to ensure you are on top of cybersecurity. Hackers, phishers, and data breachers alike are hungry to exploit businesses' most sensitive information through gaining electronic access to their data. With 94% of SMBs reporting at least one cyberattack in 2024 already, it is time to make sure you're prepared to fight off the threat of cyberattacks.

These ten suggestions will help you understand what should be prioritized when managing your cybersecurity strategies.

01

Establish Organizational Security

Organizational security is the planned list of steps used to prevent a cyberattack, as well as the steps taken after an attack. Every business requires some sort of unique protection; think of security measures you already have in place, what practices you participate in that may put you at risk, and what common threats your industry faces while making your plan.

02

Communicate Quickly and Clearly

Unfortunately, cyberattacks are a matter of "when" rather than "if". That means establishing secure communication channels for employees to use during an attack is a crucial part of planning your strategy.

Brevity is the soul of wit. Be concise when giving information regarding the attack to your employees and IT support. Refer to your organizational security plan to help guide you through this predicament.

03

Update Your Software

In May of 2017, the WannaCry ransomware attack devastated the computers of around 230,000 companies globally. Hospitals in the UK, several government bodies across India, and other prominent institutions fell victim to the attack. How did this cryptoworm successfully target such a wide range of facilities? By exploiting their outdated software.

Software providers are constantly updating their systems. Old versions of software are abandoned to shift focus on the latest rendition. Ensuring your hardware can support the latest software updates is one of the easiest steps you can take to secure cyber protection for your business.

Pictured on the cover: Matthew and Kyle

04

Stay Up to Date on News and Trends

We know, keeping up with news of any kind these days is a grueling task. But brushing up on what's happening in the world of cybersecurity (and beyond!) will help guide what decisions you make to strengthen your business's cybersecurity.

Sites like The Hacker News report a vast range of stories related to cybersecurity. Scroll through their top stories and keep an eye out for keywords relevant to you. This includes names of companies you purchase hardware and software from and words like 'business', 'resume', and 'job'.

05

Provide Employee Cybersecurity Training

This really can't be stressed enough. Requiring cybersecurity awareness training will give your employees the skills needed to detect phishing attempts and other cybersecurity threats. If this isn't already part of your onboarding process, then there's no better time than the present to instate it.

06

Document the Incident

When your business falls victim to a cyberattack, you should document what happened. It is recommended that organizations file a report stating the details of the attack to the FBI.

Some SMB owners worry that filing a report will draw customers away from their business. But not being honest with your clients will ultimately do more harm than good for your business. Not only that, but having a record of the incident will help when seeking legal counsel regarding the incident.

Continue reading on page 7

Making The Most of Your Tech Budget Through Goal Prioritization

Staying on top of the latest tech trends is a surefire way to keep your SMB on clients' radars. It comes as no surprise then that 66% of businesses plan to increase their IT spending in 2024.

The hardest part of planning a tech budget is knowing where to start. Fortunately, by looking at where your business's priorities and size are, you can establish where your business's tech spending should go.

Trends and Projections

It is projected that the majority of IT spending in 2024 will go towards software and hardware. Following that is IT labor and costs associated with hosting/cloud-based services.

A 2020 survey revealed that 75% of small business owners viewed keeping up with technological advancements as important to their company's success. But don't feel alone if the prospect of investing in the latest and greatest tech intimidates you. The same survey reported 46% of respondents were troubled by the cost of entry with new tech, with 40% worried about new technical training costs.

One Size (Does Not) Fit All

How should these troubling costs be managed, then? What's most important to consider when tackling your technology budget is the size of your business.

Business sizes are often divided into four categories based on the number of employees: small business, midsize business, small enterprise, and large enterprise. Larger businesses tend to be more developed. Doesn't it make sense, then, that a small to midsized business would have different tech needs than a large enterprise?

Startups usually focus on building a customer base through marketing while midsized companies are more concerned with topping their competitors. Technology needs should reflect these goals accordingly.

Technology Should Grow with You

Understanding common trends and determining your business's current goals should give you a better grasp on how to prioritize your tech budget. And since technology is an investment, you want to ensure your money is being put towards the best options available to you.

Any hardware, software, or services you purchase should keep up with the ever-growing standards of both your industry and the tech industry at large. Communicating with your IT service provider can help you meet this standard.

Whether they work in house, are a service provider you've hired, or a combination of both, your IT support service providers have an intimate understanding of your company's technology needs and can provide insight regarding pricing and priorities you may have not previously considered. They will be able to guide you through what tech options will not only grow but help advance your business's mission.

Following trends, considering your business's size, and consulting your IT support system are all great ways to optimize your tech budget. They all help you set goals that prioritize where your money should go in consideration of where your company currently is and how you want it to grow.

Data Breaches and Data Privacy:

Keeping Your Information Safe in an Increasingly Connected World

Cybercriminals view your company's confidential data as a goldmine. Employee SSNs, medical records, and bank statements are just a few examples of information stolen and then sold to unauthorized individuals during a data breach. Stolen information can also be used to initiate a campaign of extortion against you and your company. The costs of time, money, and image resulting from a data breach weigh heavily on affected companies.

A 2023 Identity Theft Resource Center impact report states that there's been an overall increase in cyberattacks against small businesses, with 73% of SMB owners or leaders reporting a data breach that year. Of those respondents, 85% stated they were prepared to properly respond to a cyberattack.

There are precautions you can take to prevent a data breach from happening, ensuring the protection of the data you are trusted with to keep business operations running smoothly.

Provide Employee Cybersecurity Training

95% of traceable cybersecurity issues are a result of human error. Cybercriminals will try to take advantage of those unable to detect common digital schemes, posing as a higherup in your company urgently requesting log in information from unsuspecting employees.

Cybersecurity training should be a requirement for any SMB. Basic takeaways applicable to any industry include but are not limited to:

- Best practices for creating and protecting passwords
- What correspondence with the company's IT provider looks like
- How to detect phishing attempts

Backup Your Data

Gone are the days of organizing filing cabinets– virtually every modern business uses some kind of cloud service. But using a cloud without backing up its data on a regular basis is a risky move that data breachers will absolutely extort.

A data backup involves copying your data from its primary location into a secondary location. This may be another cloud or some kind of external hard drive.

Power outages, system overloads, and ransomware alike can compromise your main cloud. Human error also does its fair share of damage – we all know the panic that an accidental mis-click can bring. Backing up your data gives you peace of mind that all your business's sensitive information will stay intact through any scenario.

Continue reading on page 7

What's Causing the Wave of Healthcare Cyberattacks?

Healthcare institutions are hypervigilant when it comes to protecting their digital data—at least, they should be. Patients trust their providers to keep their information confidential. This includes both their personal information and their medical records.

Several industries fall under the healthcare umbrella: pharmaceuticals, hospitals, insurance, and diagnostics are just a few examples. Within each of these are unique technologies, ranging from patient portal applications to gigantic MRI machines. In many cases, these industries' technologies are interconnected with each other through a wireless connection.

Though these systems are needed to keep up with the ever-evolving advancements in modern medicine, they are also particularly vulnerable to a cyberattack. Cybercriminals have multiple angles of attack to gain unauthorized access to any healthcare institution's private data, whether it be through wireless tethering or through a unique software system.

Patients, healthcare workers, healthcare investors—really, anyone who has seen a doctor—all depend on healthcare institutions to keep their private data safe. So why is it, then, that we are seeing a surge in healthcare organizations falling victim to cyberattacks?

Headlining the news recently is the ransomware attack initiated against Change Healthcare, a technology provider specializing in payment management and health information exchange systems. It is owned by UnitedHealth, a health insurance provider. Change made the controversial decision to pay the ransomware gang attacking them the $22 million in bitcoin demanded, setting a dangerous precedent.

Cybercriminals are now under the impression that, if they cause enough damage, they can get large sums of money from healthcare institutions they attack. Healthcare organizations allocate an average of 7% of their budgets cybersecurity—with this wave of cyberattacks, it's time for that number to go up.

Because Change manages the billing of insurance claims, healthcare industries throughout the country (most notably hospitals and pharmacies) were unable to receive the funds necessary to cover provided services. This prevented them from adequately managing their practices, as they lacked the resources needed to pay their workers and keep everyday functions running normally. As a result, many patients lost access to life saving care.

Cyberattacks initiated against health institutions are literally deadly. It is even more frustrating, then, that the breach in Change Healthcare's system was the direct result of the company not implementing two-factor-authentication within their internal systems.

Perhaps one of the easiest and most effective cybersecurity measures someone can take, two-factor authentication (2FA) security systems require a minimum of two distinct forms of identification to access an account. This typically looks like a password paired with something else—usually a code sent to the phone number associated with the account.

Not implementing easy security measures such as 2FA is typically the result of a company using legacy systems, which is a fancy way of saying outdated software. These systems often cannot support modern IT solutions, and if they can, then the cost and inconvenience of implementing them are exorbitant. The reason a company may use a legacy system is because of the frustrating process of migrating their software over to a newer server. This issue is a double-edged sword, as the longer you wait to update a system, the more difficult it will be to migrate.

Healthcare institutions are often guilty of using legacy systems, though it sometimes is not by choice. As mentioned before, healthcare technologies are diverse and constantly evolving. Upgrading to the latest and greatest system is not always financially possible. Mismanaged resources also may prevent healthcare institutions from implementing the necessary upgrades they need.

While UnitedHealth claimed to be in the process of updating Change's outdated legacy systems, it is obvious that the process needed to occur quicker than it did. When health care industries lag behind on their cybersecurity measures, lives are put at risk, putting both patient health and institutional credibility on the line.

An SMB's Ten Step Guide to Cybersecurity Strategies continued from pg 3...

07

Know Who Knows What

It's easier than ever to let technology remember things we would recall ourselves just 20 years ago. When was the last time you wrote down a password instead of asking your browser to save it for you? Can you even say what your cell number is without checking your phone's contacts?

Features like these are convenient, but they also hold onto information cybercriminals are eager to get their hands on. You want to know who has access to your private data, what they know about it, and what they can do to prevent cybercriminals from gaining access to it.

08

Ensure You Have Access to Backups

Server backups are a great way to ensure your data stays safe during any kind of disaster recovery. Whether a hacker gained access to your primary server or a natural disaster compromised it, putting copies of files on a secondary server means operations can continue even during the worst-case scenario.

09

Limit Employee Permissions

Provide employees only with the resources they need to do their job, period. As the number of people with permitted access to your data rises, so does the risk of unwelcome visitors sneaking their way in.

You should also monitor technology you provide your employees with, such as work issued smart phones and laptops. Create guidelines for how the devices should be used by any employee trusted with them.

10

Lock Your Wi-Fi

Please password protect your wi-fi networks, we're begging you. Think of your wi-fi network as a back door; leaving it unlocked makes it easier for intruders to break in, taking whatever they want without being detected. By protecting your wi-fi access with a strong password, you are keeping the metaphorical back door locked up and inaccessible to hackers.

Data Breaches and Data Privacy: continued from pg 5...

Know How Your IT Provider Is Using Your Data

This is why reading the fine print is important. While it is expected that your IT service provider should collect some of your business's data, problems arise if they push the boundaries of what that data should be used for.

Make sure you know how your provider – prospective or current – manages your data, especially upon termination of your contract with them. Do they delete it from their servers entirely? If they do keep it, then what is their reason for doing so?

If a prospective IT service provider gets defensive over or avoids questions regarding their use of your data, take the sign and look for an alternate provider.

Today's world requires us to constantly be connected to each other through technology. Taking steps to protect your SMB's classified information not only keeps you, your employees, and your clients safe, but also reflects well on how your company is perceived. Folks who want the best for themselves do the same to whoever they provide goods and services for.

LeadingIT Core Values Victor of the Month

Vanessa Canete - Level 2 Technician

We're excited to announce Vanessa as this month's Values Victor, celebrated for her Positive/ Fun Mindset! At LeadingIT, Vanessa exemplifies what it means to maintain a positive outlook and a focus on solutions. Her approach to challenges is always constructive, steering clear of negativity and looking for effective resolutions. Vanessa's spirited attitude and infectious enthusiasm remind us daily that 'how we view is how we do.' Her ability to uplift the team while driving forward with optimism makes every project not just a task, but a joyful journey. Congratulations, Vanessa, for inspiring us all to keep spirits high and solutions in sight!

LEADINGIT VALUES:

- We Are Driven
- We Chase Excellence
- We Are Humbly Confident
- We Are Accountable
- We Have A Positive/Fun Mindset

Continue reading on our blog at goleadingit.com/blog

LeadingIT

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

LeadingIT

$1000 REFERRAL PROGRAM

WE LOVE REFERRALS!

Do you know an organization that needs fast + friendly IT and cybersecurity support?

If they sign up, you'll receive $1000!

LEARN MORE

GOLEADINGIT.COM/REFER

815-788-6041

WE ARE CELEBRATING!

Birthdays

Stephen Taylor - August 11th
Heather Hoffman - August 12th
Maxwell Kulwiec - August 24th
Jose Ledesma - August 26th
Mallory Rocha - August 30th

Anniversaries

Garrett McCleary - 8/16/2021
Michael Tarasiewicz - 8/14/2023
Jacob Abernathy - 8/15/2023