Cybersecurity Awareness Month

the NetWork

LeadingIT

Chicagoland CybersecurITy Support

October 2023

- A BIG Thanks To Our Clients!
- Navigating Cybersecurity Awareness Month: Your Guide to Securing Your Organization
- Ethical Hacking: How White Hat Hackers Help Strengthen Cyber Defenses
- 5 Reasons to Replace Your Computer Every 3 Years
- The Importance of Emergency Response Plan Testing

GoLeadingIT.com 815-893-2525 @goleadingit

A BIG Thanks To Our Clients!

We're thrilled to announce that LeadingIT has once again secured a spot on the renowned Inc. 5000 list!

Earning the impressive rank of No. 3283 in the 2023 edition, this achievement reflects our dedication, hard work, and the outstanding partnerships we've fostered along the way.

With an astounding three-year revenue growth of 155 percent, we're honored to be part of the dynamic landscape of independent and entrepreneurial businesses driving our economy forward.

We extend our heartfelt gratitude to our incredible team and valued clients who have been instrumental in this journey. Here's to continued growth, innovation, and making strides together!

Jeremiah, Scott and Salvador

5 Reasons to Replace Your Computer Every 3 Years

With each passing year, new advancements in hardware and software are introduced, promising enhanced performance, improved security, and more efficient workflows. Consequently, there is a growing emphasis on the importance of upgrading your computer every three years to keep up with the changing technology landscape and ensure optimal performance.

1. Performance and Speed

This allows for faster processing times as well as smoother multitasking capabilities so that software applications run without a hitch.

This also means higher productivity; J. Gold Associates reported that computers older than five or more years decreased respondents' productivity by 29.45%.

2. Compatibility and Support

As developers roll out updates, new features, operating system updates, and security patches that are designed to work best with newer computers – using an outdated device could lead to a less-than-satisfactory experience.

Continue reading on page 6

Pictured on the cover: Collin, Dave, Pedro, Salvador, Laura, Scott, Stephen, Keegan, Matt, Jeremiah, and James

Navigating Cybersecurity Awareness Month: Your Guide to Securing Your Organization

October marks Cybersecurity Awareness Month - the perfect time for companies to review their cyber defenses and ensure they're protected against the growing digital threats out there. With data breaches and ransomware attacks rising, focusing on security is more critical than ever. Partnering with a managed service provider (MSP) can help reinforce your organization's protection from these malicious actors - but how? In this article, we'll explore all the ways an MSP can bolster your cybersecurity efforts for maximum safety.

The Current Threat Landscape

The current digital security arena is constantly shifting and complex, with bad actors using more advanced tricks and tactics all the time. Cyber threats are also becoming more frequent and costly - according to IBM, the average data breach now costs $4.45 million.

Ransomware hits remain a huge worry, with threat groups demanding massive sums to unscramble important data. Phishing and social engineering attacks have gotten more convincing and personalized, making it hard for people to spot genuine communications from malicious ones. Also, supply chain hacks have surged in prominence, with cybercriminals sneaking into the systems of trusted suppliers to compromise their customers.

Despite all this, 62% of SMBs lack the in-house skills to handle cybersecurity - and this is where working with an MSP can help.

Outsourcing Security: The Benefits

Outsourcing your security to an MSP isn't just about access to a specialized team - it's about having the peace of mind that you're getting superior protection. An MSP brings more than just sophisticated tech and threat awareness; they provide comprehensive coverage with minimal internal resources so you don't have to worry about managing complex systems or defending against cyber threats yourself.

Investing in an MSP means safeguarding your organization with industry-leading expertise and up-to-date info, allowing for better defense without breaking the bank.

Let's explore some key benefits of partnering with an MSP to secure your organization:

24/7 Monitoring and Management

MSPs monitor networks and devices around the clock to quickly catch potential vulnerabilities and threats. This means they can respond right away to contain the damage from cyberattacks. They act as an extension of your IT team, handling your security infrastructure, maintenance, and support 24/7.

With nonstop oversight of your systems and data, MSPs can spot unusual activity that may signal an impending attack. These experts know what to look for and can rapidly investigate and tackle emerging threats. This constant vigilance allows MSPs to stop attacks before they spiral into expensive data breaches.

Backup and Disaster Recovery

Data is the lifeblood of any organization, so having a comprehensive cybersecurity strategy that includes backup and disaster recovery measures is absolutely essential. MSPs provide both to safeguard your systems and information.

Backup involves regularly copying and archiving mission-critical information. If a breach or outage occurs, backups allow you to restore systems and files without data loss. MSPs can set up automatic on-site and cloud backups to run continuously or on a schedule. Cloud backups give geographic redundancy,

Continue reading on page 7

Ethical Hacking:

How White Hat Hackers Help Strengthen Cyber Defenses

Hackers have long been portrayed as the bad guys in the media, labeled as mischievous cyber-criminals who wreak havoc and steal data. But that's not always the case; ethical hacking is a form of digital security testing that actually helps to protect from malicious hackers by finding vulnerabilities before they can be exploited.

Ethical hackers - or 'white hatters' as they're often known - play an essential role in reinforcing cyber defenses and protecting organizations from digital attacks. In 2022, HackerOne's ethical hacker initiatives uncovered more than 65,000 software vulnerabilities - a 21% increase on 2021 figures - plus over 120,000 customer vulnerabilities.

What is Ethical Hacking?

Ethical hacking is a crucial practice in the cybersecurity field that involves white-hat hackers protecting organizations from malicious attacks. By using the same techniques and tools as attackers, ethical hackers are able to identify weaknesses in IT infrastructure and provide solutions before criminals can exploit them. This type of security testing allows businesses to close up any potential gaps or vulnerabilities, ultimately creating stronger defenses against cybercrime.

In essence, ethical hacking gives companies an opportunity to prepare for threats before they become a reality - something all business owners should strive for if they want their data safe from harm's way. It's important to realize that although "hacking" often has negative connotations associated with it, this form of digital investigation offers organizations invaluable insight into how secure their systems really are - providing peace of mind when it comes to online protection.

How Ethical Hacking Helps

There are several key ways that ethical hackers help improve cybersecurity:

Penetration Testing

Ethical hackers conduct controlled "penetration" tests on systems by attempting real-world attack scenarios. This helps detect potential weaknesses and ensure security for organizations.

Vulnerability Assessments

Ethical hackers systematically scan networks and applications to discover misconfigurations, unpatched software, and other weaknesses. This provides a clearer picture of an organization's security posture.

Process Improvement

Ethical hacking assessments often reveal bigger-picture issues in security processes and procedures. Organizations can use the findings to strengthen policies, employee training, and incident response plans.

Social Engineering Assessments

Because people are often the weakest link in security, ethical hackers test things like phishing susceptibility and physical access controls. This identifies areas where employee education could help.

Continue reading on page 7

The Importance of Emergency Response Plan Testing

Having an emergency response plan is absolutely crucial for any organization. These plans play a role in ensuring that when IT-related crises occur they can be swiftly and efficiently addressed. However, creating the plan itself is the starting point. It is equally important to test the plan and ensure its ability to handle any IT-related crisis. Unfortunately, many organizations often neglect this step.

According to a study conducted by the Ponemon Institute, only 25% of businesses consistently incorporate an incident response plan into their operations with a mere 14% testing these plans more than once annually. What's more alarming is that a staggering 66% of organizations identify a lack of planning as the primary obstacle preventing them from being resilient against cyberattacks.

Here are a few advantages of testing your emergency plan:

Identifies Potential Gaps

Identifying potential gaps in communication, decision-making processes, and resource allocation can help organizations stay ahead of the curve.

Prepares Employees

Practice drills make it easier for employees to know their roles during an emergency situation – reducing stress and boosting efficiency.

Refines Procedures

By testing procedures under real-world conditions, companies are able to fine-tune plans so they remain adaptable and effective when needed most.

The Importance of Updating an Emergency Response Plan

Regularly updating and reviewing your emergency response plan is an essential part of maintaining a cyber-resilient organization. Not only does it keep the plan up-to-date with the current IT environment, but can potentially reduce the impact of any incidents.

According to IBM's 2021 Cyber Resilient Organization Report, 38% of organizations seen improved resiliency by updating their plans regularly.

Here are just a few benefits of updating your emergency plan:

Adapts to Emerging Threats

Updating your emergency plan ensures that you have up-to-date procedures ready to handle whatever new kinds of attacks may come up.

Addresses Changes to IT infrastructure

As an organization adopts new technologies or updates its existing IT infrastructure, the emergency response plan must also be adjusted to reflect these changes.

Accounts for Employee Changes

Employee roles and responsibilities can change over time - updating the plan ensures that the right individuals are assigned the appropriate tasks.

Be Proactive, Be Resilient

A well-crafted emergency response plan's effectiveness hinges on regular testing and updates. Testing can help you recognize any weak points in the system as well as get your team familiarized with how to put the plan into action. Plus, keeping up-to-date with changes such as new security threats or technologies will ensure that your organization remains secure and prepared for anything.

Don't get caught off guard by an IT emergency - be proactive, stay informed, and remain resilient. By dedicating yourself to constantly testing and updating your response plans, you're not only safeguarding your organization's digital assets but also positioning yourself for a more resilient future.

5 Reasons to Upgrade Your Computer Every 3 Years continued from pg 2...

3. Enhanced Security

At a certain point, computers reach their end-of-life or end-of-support, meaning they no longer receive updates and may be vulnerable to security risks. If you're still using an older computer that isn't equipped with the latest security features, then your data is at serious risk of being compromised or stolen.

4. Cost-Effectiveness

Investing in a new computer every three years can prove more cost-effective than relying on an older machine. According to a study from Techaisle and Microsoft, computers that are more than four years old are 2.7 times more likely to need repairs, and computers at this age cost around $2,736 USD to maintain.

5. Competitive Edge

Newer computers provide powerful features and capabilities that can give you an advantage. Whether you're a creative professional needing top-of-the-line graphic processing for complex projects or a business owner looking to maximize multitasking potential, upgrading your tech ensures you won't be left behind by outdated hardware limitations.

Make the Smart Investment

You won't stay competitive in today's digital landscape if you don't keep current. While the upfront investment of replacing your computer every three years might seem significant, the long-term advantages in terms of productivity, cost-effectiveness, and security make it a strategic decision that pays off in more ways than one.

Ethical Hacking continued from pg 3...

Compliance Testing

Ethical hackers can check for adherence to security standards and regulations like PCI-DSS, HIPAA, and GDPR. Audits help avoid costly fines and damage to an organization's reputation.

Attack Simulation

"Red team" exercises simulate realistic attacks to test incident response plans and readiness. Gaining practice against mock threats improves an organization's resiliency.

Control Validation

Ethical hacking verifies that implemented security controls are functioning as intended. Tests reveal when protections are improperly configured or fail to block attacks.

Proactive Cybersecurity: Leveraging Ethical Hacking

Overall, proactive ethical hacking delivers huge benefits for bolstering cyber resilience and decreasing an organization's exposure. Although no system is completely hack-proof, ethical hacking pinpoints vulnerable areas that need to be addressed. Companies that routinely perform ethical hacking tests can find and fix flaws in their defenses. With persistent evaluations and implementation of suggested controls, businesses can build more robust cybersecurity and be better equipped to withstand real attacks.

Navigating Cybersecurity Awareness Month continued from pg 3...

so backups are not impacted if your office has a fire, flood, or other disaster.

Disaster recovery means planning and preparation to quickly respond to unplanned downtime. Having documented policies and procedures to restore systems, regain access, and coordinate teams will enable faster recovery. MSPs can create and handle your disaster recovery plan based on your operations, systems, and goals. Their breach response experience gives practical insight into effective recovery processes.

Ransomware Protection

Ransomware attacks have been rampant with no sign of slowing down - increasing by 37% from April 2022 to April 2023. MSPs offer multi-layered ransomware protection including email and spam filtering, endpoint detection and response, patch management, access controls, and data encryption.

By locking down vulnerabilities, monitoring networks, and keeping systems current, MSPs proactively prevent ransomware infiltration. If an attack succeeds, MSPs are skilled at swiftly isolating infected devices, restoring encrypted data from backups, and activating recovery plans to restore productivity. Their methodology defends your organization while minimizing downtime and avoiding ransom payments.

Partner with an MSP and Secure Your Organization

As technology continues to evolve, so do the risks associated with it. Artificial Intelligence (AI) and the Internet of Things (IoT) have opened up new entry points for potential cyber attacks - making it more important than ever for companies to be diligent

in their cybersecurity efforts. To stay one step ahead of these threats, organizations should prioritize investments in security solutions.

For a cost-effective way to access enterprise-level protection against modern cyber threats, consider partnering with an MSP like LeadingIT during this Cybersecurity Awareness Month. Our team is well equipped with the expertise needed to strengthen your organization's security posture by transitioning from a reactive approach towards proactivity; focusing on early detection and mitigation of malicious activities before they become a problem.

Fore-tifying Partnerships!

We were thrilled to tee off our sponsorship at the Calumet Area Industrial Commission (CAIC) golf outing. As a proud hole sponsor, we had a ball connecting with industry leaders and enjoying a friendly game of Jenga with the attendees. Here's to building stronger connections on and off the course!

Pictured above: vCIO team, Dale and Mike

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

Garrett McCleary - October 5th
Dustin Looper - October 10th
John Funk - October 26th
Gregory Radon - October 30th

Anniversaries

Devin Lindelof - 10/5/2020