the NetWork

LeadingIT

Chicagoland CybersecurITy Support

August 2023

The Human Factor: Educating Employees on Cybersecurity Best Practices for SMBs

The Advantages of Prioritizing Secure Hardware in Your Business

How Cyber Resiliency Is Crucial for Business Continuity

LeadingIT Community News

GoLeadingIT.com 815-893-2525 @goleadingit

The Human Factor:

Educating Employees on Cybersecurity Best Practices for SMBs

Security experts have long known that employees are often unaware of the risks they pose to small and medium-sized businesses (SMBs), and many don't understand how to avoid cyber threats. As a result, they may inadvertently open up an organization's critical data to hackers who could use it for malicious purposes. In fact, IBM research shows that human error is behind more than 90% of all cyberattacks.

That's why it's critical to educate employees on cybersecurity best practices. But where do you start? ***Invest in Cybersecurity Awareness Training Programs***

In the fast-paced world of cybersecurity, there's no such thing as too much training. As we stated, the threat landscape is constantly changing, and the only way to stay ahead of these threats is by continually educating employees on the most up-to-date best practices. Plus, training programs are an affordable investment compared to the potential financial and reputational damages that can result from a successful cyber attack.

Here are a few ideas for employee training:

- Phishing Awareness Training
- Password Management Best Practices
- Make Employee Education Relevant to Their Position
- Reinforce Training and Best Practices
- Build a Security-Aware Culture

The human factor is crucial in cybersecurity for SMBs, so never underestimate the power of informed employees. By embracing a top-down approach, investing in cybersecurity awareness training, tailoring education to each employee's role, and reinforcing best practices, organizations can nurture a security-aware culture. This, in turn, helps to minimize the overall risk of cyberattacks. At the end of the day, a well-informed and vigilant workforce is a company's strongest defense against the ever-changing world of cybercrime.

Jeremiah & Scott

Pictured on the cover: Dave, Keegan, Salvador, Scott

The Advantages of Prioritizing Secure Hardware in Your Business

As technology proliferates and cyber threats continue to rise, investing in secure hardware is no longer a luxury—it's essential. Not only does it safeguard sensitive information, but it can also bring numerous financial and long-term benefits that businesses should be eager to capitalize on.

What is Secure Hardware?

First, let's understand what secure hardware is. Essentially, it encompasses any physical device with built-in security features, such as secure servers or encrypted hard drives, that protect you from cyber threats. These devices provide added layers of protection to keep your data safe from unauthorized access and malicious attacks. By investing in secure hardware, you can ensure that your valuable information is better secured against potential intruders.

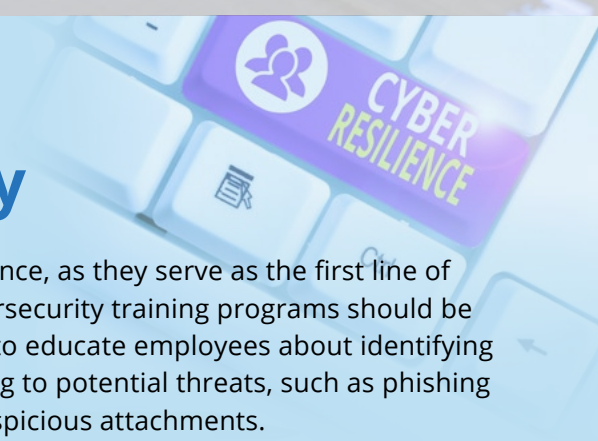
Financial Benefits of Secure Hardware Investments

Investing in secure hardware can be a beneficial decision for businesses of any size, as it helps to protect them from the ever-growing and costly threat of cybercrime.

According to Cybersecurity Ventures' report, these attacks are expected to cost an estimated $10.5 trillion annually by 2025. By investing in secure hardware now, companies can

Continue reading on page 4

How Cyber Resiliency Is Crucial for Business Continuity



In today's world, where cyber threats are pervasive and 70% of companies report being threatened by cyber attacks, understanding the link between cyber resilience and business continuity is vital. Cyber resilience refers to an organization's ability to maintain its operations during and after a cyber attack, minimizing the impact on business functions. It is essential to prioritize cyber resilience as cyber attacks like ransomware, data breaches, and phishing become increasingly common, posing risks to a company's reputation, finances, and operations.

To enhance cyber resilience, organizations should begin with a comprehensive risk assessment to identify potential threats and vulnerabilities. An incident response plan should be developed, outlining roles, communication protocols, and procedures for containing and recovering from cyber attacks. Regular testing and updating of the plan ensure its effectiveness against evolving threats.

Employee training and awareness play a crucial role in cyber resilience, as they serve as the first line of defense. Cybersecurity training programs should be implemented to educate employees about identifying and responding to potential threats, such as phishing emails and suspicious attachments.

Maintaining long-term cyber resilience requires ongoing improvement and adaptation. Staying informed about the latest cyber risks, updating technologies and processes, and collaborating with IT service providers for expertise and support are essential. Finally, fostering collaboration between IT and other departments within the organization is necessary for a comprehensive approach to cyber resilience.

Integrating cyber resilience into business continuity plans is crucial for protecting organizations from the harmful effects of cyber attacks. Prioritizing cyber resilience and implementing strategies like risk assessment, incident response planning, and employee training ensure long-term success and safeguard a company's reputation in the digital era.

LeadingIT Community News

We'd like to welcome Keegan back to the LeadingIT team! We look forward to witnessing the impact you will make in ensuring exceptional service delivery for our clients.

Secure Hardware continued...

significantly reduce the risk of being victimized by such malicious attacks and save themselves from paying out huge sums later on down the line.

Additionally, enhanced security measures implemented through secure hardware also have other financial benefits; reducing time spent dealing with security incidents or breaches often leads to lower operational costs over time.

Other Long-Term Advantages of Secure Hardware Investments

Beyond simply preventing data breaches, investing in secure hardware can yield long-term benefits that are impossible to ignore. For example, companies face hefty fines, tarnished reputations, and lost customers if they don't comply with strict data protection regulations — but those risks are mitigated by investing in safe solutions right away.

Not only does this investment show your commitment to protecting customer information, but it gives you an edge over competitors who haven't taken the same initiative. Recent McKinsey research has found that 53% of customers seek out and only buy from companies that are known for protecting consumer data.

In other words, your market standing will improve as customers recognize your dedication to safeguarding their sensitive details - this could lead to more revenue from increased consumer trust and confidence! Investing in secure hardware is a win-win for businesses looking to up their security game while reaping the rewards of elevated brand recognition.

Secure Hardware is a Business Must-Have

In short, there's no denying that investing in secure hardware isn't just smart — it's critical if any company hopes to stay ahead of its competitors and remain resilient against growing cyber threats. Although the big upfront expense can be daunting, the long-term advantages always outweigh the initial investment — making secure hardware an absolute must when devising any savvy business strategy.

LeadingIT

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

Continue reading on our blog at goleadingit.com/blog

WE ARE CELEBRATING!

Birthdays

Joseph Udy - August 6th
Stephen Taylor - August 11th
Maxwell Kulwiec - August 24th
Jose Ledesma - August 26th
Collin Saunders - August 26th
Mallory Hale - August 30th

Anniversaries

Jeremiah Bird - 8/24/2020
Garrett McCleary - 8/16/2021
Amie Koster - 8/18/2021
Salvador Navarro Vega - 8/1/2022
Katlyn Rogerson - 8/16/2022