the NetWork

LeadingIT
Chicagoland CybersecurITy Support

May 2022

Employee Training: Cultivate a Culture of Cybersecurity Awareness

Vulnerability Scan: Identify and Prioritize Unknown Cyber Threats

Protect Your Business' Data From Cyber Risk

LeadingIT in the Community

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

Employee Training: Cultivate a Culture of Cybersecurity Awareness

Typically, executives may imagine deploying sophisticated intrusion detection, and prevention technologies as the ultimate recourse to malware and supply chain attacks. Employee cyber awareness training is still the most effective strategy. Cybinit estimates that 95% of cyberattacks originate from human error. That means that a cyber-informed staff can catch 90% of data breaches.

Here's the thing—your employees are the most vital defense line against cyber attackers and inarguably also the weakest link. So, as you invest in those complex data security and technologies, you should always ask yourself: How well can my staff understand and use these technologies? Otherwise, you might deploy expensive, sophisticated systems and remain vulnerable.

Peter

Employee Cybersecurity Mistakes You Can Mitigate Through Training

According to PurpleSec, over 90% of data breaches rely on social engineering. These are cyberattack vectors that dupe users into revealing critical data. Some of the typical employee negligences include:

• Password-related errors: Several organizations don't have password expiration and complexity protocols. For instance, a 2019 study by the National Center for Cyber Security shows that "1234" is still the most popular password worldwide. When employees use such easy-to-crack basic passcodes, they expose your systems to unauthorized access.

• Misdelivery: According to Verizon's 2018 Breach Report, misdelivery is the fifth most common cause of data breaches on corporate systems. The bad guys can use this tactic to trick users into exposing their logins or for direct financial gain. For example, the internet was recently abuzz with news about Barbara Corcoran, the bookkeeper who unknowingly sorted a malicious invoice and paid over $400,000 to a fake account. Training employees how to spot these tricks can prevent accidental wire transfers or ACH payments that result in huge monetary loss.

• Skill-based negligences: These slips may occur when employees perform routine activities. They can be because of ignorance or tricks from cyber actors. A perfect example is the opening of malicious links, which 78% of American employees still do despite understanding the underlying threat.

Cybersecurity Awareness Training Topics for Your Employees

A thorough staff cyber awareness training program should prepare your staff for intrusion detection and prevention. Some areas you can focus on include:

- **Threat identification:** Train your staff on monitoring the system and how to spot abnormal activities that may show underlying dangers. The earlier your employees can identify threats, the faster you'll thwart them, resulting in less destruction and downtime.
- **Common cyber tricks:** The bad guys continually advance their tactics to target emerging vulnerabilities. Occasional training can train your staff on these tricks and how to avoid them.
- **Fast-response protocols:** The IT support team's job is to develop a fast-response protocol. But what good is it if your employees can't follow it? The cyber awareness training program should also include coaching the staff on how to act during a breach.

Cyber awareness training shouldn't be a onetime thing; you should occasionally retrain your staff to keep them current with emerging threats. Launching simulated attacks occasionally might also help measure readiness levels and identify areas that need more training.

Pictured on the cover: Steven

Vulnerability Scan: Identify and Prioritize Unknown Cyber Threats

A rule of thumb in cybersecurity is that everybody is a potential target. You're not safe, regardless of your organization's size or industry. And that's why vulnerability scans are crucial—they can help you gauge your cybersecurity posture, trace your digital footprint, and identify areas that need adjustments.

When you're sick, you may rush to the doctor. But you don't have to wait until bed-ridden to visit a hospital. Sometimes, you go to the doctor for routine checkups to ensure everything is okay. Similarly, you don't wait for your car to break down before taking it to a mechanic. Regular garage visits for routine maintenance can increase the car's lifespan. Why should cybersecurity be any different?

How Safe Is Your Chicagoland Business From Cyberattacks?

Whenever we advise businesses to conduct vulnerability scans, they may think we are trying to market them a product. And when we tell them that the audit is free and requires zero commitment, some say, "nobody wants to hack us" or "we are fine." Some even say, "we are too small to be a target; we have nothing that the bad guys would want."

According to the 2019 Varonis Data Risk Report, only 5% of corporate folders have proper protection. The bad news is that almost 70% of business executives feel that their cybersecurity risks are increasing in volume and severity. So, before you say you're safe, look at the trends and statistics.

What Should Comprehensive Vulnerability Scans Assess?

A vulnerability scan isn't a witch-hunt on your IT support services provider. It's an honest, comprehensive IT infrastructure review to spot systemic vulnerabilities that expose you to hacks and breaches. Some areas may cover:

- Physical security: The scan can focus on role-based access controls, disc encryption, and biometric data. Which measures do you have to safeguard your files from physical compromise?
- Operational security: Which cybersecurity policies and protocols do you have to guide day-to-day operations. The scan might also look at their responsiveness.
- Data security: How do you protect your files and credentials during collection, transit, and storage?
- System security: What are your protocols for monitoring and managing systems access and enforcing privileged access?
- Network security: The scan focuses on the security controls, network visibility, Security Operation Centers (SOCs), antivirus configurations, and similar techniques to shield your environment from unauthorized access.
- Dark web monitoring: A vulnerability scan can also review the dark web to check if your files or credentials are up for sale.

> "95% of cyberattacks originate from human error."

Introducing Our Confidential, Painless CyberSCORE Vulnerability Scan

Why pay for a vulnerability scan when we offer it for free? LeadingIT's CyberSCORE vulnerability scan is a confidential, zero-obligation service available for all Chicagoland businesses. How does it work?

1. First, we will spend about half an hour having a non-technical conversation about your opinion on your organization's IT security.
2. Next, we will conduct a non-invasive investigation of your backups, network, and security protocols to gauge your posture. You don't have to inform your current IT company of the audit, or we can involve them. We often advise clients to keep it confidential because even the bad guys don't announce when they're coming.
3. We will then spend another hour with you to explain our discoveries.
4. If we identify any glitches, we will develop a Security Action Plan for you for free. You can choose to work with us to implement it or retain your current team.

Protect Your Business' Data From Cyber Risk

If you're managing data, you must invest in cybersecurity—there are no two ways about it. Here are seven practical cybersecurity strategies you can implement:

1. Use strong passwords with 2FA: Statistics show that 8 out of 10 data breaches are due to weak passwords. Do not assume that your employees will always create strong passwords. Passwords should be strong, complex, and lengthy. The latest recommendations suggest creating passwords with minimum a length of 12 characters using uppercase, lowercase, numerals and symbols. Implement password expiration and complexity protocols in all access levels. Only then can you be confident that your systems always have reliable passwords.

2. Create reliable backups: Ransomware is inarguably one of the most rampant cyberattack vectors. Typically, the bad guys encrypt your data and pressure you into paying a ransom. Most businesses pay ransom to avert downtime and business interruptions. However, if you have easy-to-retrieve backups of your crucial files, you can sustain normal operations without giving in to ransom demands. We recommend sending backups to remote servers at least thrice a day.

3. Conduct regular cyber awareness training: A cyber-conscious workforce is better than even the most sophisticated intrusion detection and prevention systems. Cybinit estimates that 9 out of 10 cyber-attacks succeed because of employee negligence. Educating your staff on identifying and thwarting breach attempts can help lower your risk levels.

4. Update and patch your systems on time: Cybersecurity is dynamic. Actors keep devising new tricks, and software developers respond by eliminating vulnerabilities. Each software update comes with advanced security features. Installing these updates and patches ensures you have the safest versions of apps and software.

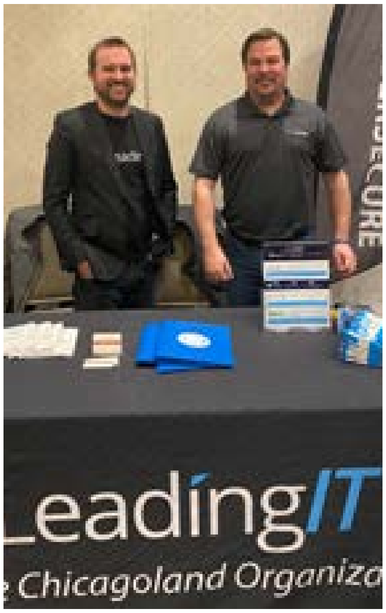
5. Monitor your network 24/7: You never know when the bad guys will strike. Sometimes, they can lie dormant in your systems to identify more vulnerabilities before launching an onslaught. Monitoring your network round-the-clock can help you identify and eliminate threats early enough before they get more severe.

Continue reading: goleadingit.com/blog

LeadingIT in the Community

We recently had the pleasure of sharing the latest information surrounding IT and cybersecurity at the Northern Illinois Alliance of Fire Protection Districts Annual Conference, Calumet Area Industrial Commission, and at the IFIA Fire & Life Safety Conference. We'd like to thank these organizations for allowing us to share our knowledge with their groups and to attend these events.

Stephen and Dale at events including CAIC, and NIAFPD



WE ARE CELEBRATING

Birthdays

Laura Piekos - May 21st

LeadingIT

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

Check out our blog at goleadingit.com/blog