Business System Solutions

Caretakers of Your Productivity
since 1995

THE BSS ADVISOR

Monthly Newsletter

September 2024

7 Biggest Small Business Cybersecurity Misconceptions

Photo by Pixabay/kirill_makes_pics

Business System Solutions is your IT Service Partner who provides peace of mind through guidance, education, and responsive support. We are the Caretakers of Your Productivity.

With Offices in:
North Central Indiana
(765) 742-3440

Middle Tennessee
(615) 819-0600

West Michigan
(616) 776-0400

info@bssconsulting.com

"Trust in the Lord with all your hear; and lean not on your own understanding. In all your ways acknowledge him, and he will direct your paths"

Proverbs 3:5-6

Small businesses are the lifeblood of American prosperity. Almost half of all workers in the country work for a business with fewer than 500 employees – and that doesn't even account for the some 27 million small business owners who are their own sole employee.

Unfortunately, because small businesses are the drivers of our economy, they are also are the target for over half of reported cyberattacks, according to a recent FBI report. We get it – you're focused on customer acquisition, shipping, marketing, and getting the job done. But security needs to play a bigger role in your operation. If you and your employees adopt a handful of behaviors, you can vastly improve your cyber defenses and keep your company rolling.

To learn new behaviors, though, you will first need to "unlearn" some misconceptions. Here are the top eight small business cybersecurity misconceptions...and how your business can overcome them.

Misconception 1: I am Not a Target for Cybercriminals

Every business, regardless of its size, the type of data it handles, or the industry it operates in, is susceptible to cyberattacks. Opportunistic

(Continued on Next Page)

(Continued from page 1)

cybercriminals see small and medium-sized businesses as prime targets due to a perception that they will have weaker cybersecurity defenses.

To protect your small business, regularly conduct security audits to identify vulnerabilities, encourage employees to use strong, unique passwords, learn to identify phishing attempts, and keep your software up to date.

Misconception 2: Cybersecurity is only a Technology Issue

Technology is undoubtedly a crucial component, but it represents one of the three essential pillars of effective cybersecurity: The other two are people and processes. Most cyberattacks occur through social engineering, where a criminal infiltrates a system through your people and processes. Employees who click on malicious links, use weak passwords, or inadvertently share sensitive information can compromise the security of your entire business.

Implement comprehensive training programs and clear cybersecurity policies and guidelines. Make security a collective responsibility and a fundamental part of the organizational culture – your defenses become stronger and your people are a force multiplier for technology-based security measures. Well-defined processes, such as incident response plans and business continuity strategies, are indispensable in mitigating and recovering from cyber incidents. Physical security is also paramount – escort visitors, use cameras, separate areas with network equipment behind locked doors, and always use shred sensitive documents.

Misconception 3: Cybersecurity Requires a Huge Financial Investment

Undoubtedly, security for your organization will probably cost money, but the investment is worth it. There are numerous cost-effective solutions to suit companies of your size. Many cloud-based services offer robust security features (often at a fraction of the cost of maintaining internal infrastructure).

Consider outsourcing some or all your needs to reputable vendors – then you tap into their cybersecurity expertise without incurring the cost. Conduct a risk assessment to identify your most critical vulnerabilities; then prioritize spending on the areas that need the most attention. Measure the ROI for cybersecurity investments versus the potential cost of a security breach.

Misconception 4: Cybersecurity is a One-Time Project

More than a single project, cybersecurity is an ongoing and dynamic process that demands continual monitoring, adaptation, and enhancement. Cyber threats are ever evolving, and new vulnerabilities are discovered regularly. Similarly, solutions, regulations, and industry standards change to address emerging risks and challenges.

This constantly shifting landscape underscores the need for businesses to view cybersecurity as a continuous effort, such as regularly downloading the latest software updates. Establish a routine of security audits, reviews, and testing. Regular data backups and disaster recovery planning are ciritcal for business continuity in case of a breach – think in terms of “when,” not “if.”

Misconception 5: Cybersecurity is Only the IT Department’s Responsibility

Cybersecurity is a collective responsibility that extends to every member of an organization. Different roles and functions can contribute to cybersecurity, just as they can also inadvertently compromise it. Anyone

(Continued from page 2)

on staff can impact security through actions like using weak passwords. Create shared responsibility and accountability for all employees to establish clear roles and expectations. Communicate and consistently enforce robust cybersecurity policies and procedures and make regular cybersecurity training and awareness programs available to all staff.

Misconception 6: Cybersecurity Insurance Will Cover all Losses from a Cyberattack

In reality, the extent of coverage greatly depends on the specific policy and the nature of the claim. Cybersecurity insurance typically covers some losses, such as direct costs like data recovery and notification expenses, and possibly legal defense costs. However, it may not cover costs like business interruption, reputational damage, or the full scope of legal liability.

Terms, conditions, and exclusions of cybersecurity insurance policies can vary significantly between providers, so read the policy closely! Review available policies closely and select one that aligns with your risk profile. Work with an agent who specializes in cyber insurance policies.

Misconception 7: Cybersecurity Compliance Equals Cybersecurity Protection

Compliance requirements often establish minimum baselines, and these standards may not evolve quickly enough to keep pace with the ever-changing threat landscape. Moreover, compliance requirements can vary significantly across jurisdictions and industries, leading to gaps in security measures.

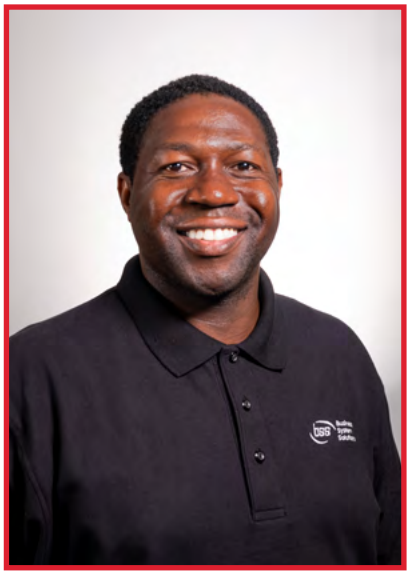
Implement security controls, conduct regular risk assessments, and stay informed about emerging threats. Don't think of compliance as the endpoint but as a step toward a wide-ranging and continuous security journey.

Your Small Business Deserves Protection

Dispelling these seven cybersecurity misconceptions is a first step toward forging a resilient cyber defense. Your small business is a prime target for cybercrime. It's not about the scale of your business, but the effectiveness of your cybersecurity measures that matters. Embrace a holistic approach that encompasses technology, people, and processes. Stay proactive and adaptive. Then you can rest assured as you navigate the digital world and protect the data under your control. Stay safe online and get down to business! □

See the full article at the National Cybersecurity Alliance: https://staysafeonline.org/resources/8-biggest-small-business-cybersecurity-misconceptions

Employee Highlight: Byron Glenn



Byron Glenn joined our Murfreesboro Tennessee office in October of last year as our Business Development Specialist but quickly took on the role of Sales and Marketing Manager. We are delighted by his dedication to forging connections in the community and being a champion of one of BSS' core values: Empathy.

Having earned his MBA and a Software Certification, he came to IT after a careers in real estate, non-profits, and government. In his spare time, he runs a non-profit advocacy company with his wife of 13 years. When not serving on the many boards in his community, he loves spending time with his family.

Byron dreams of providing tutoring and meals for every child, clean water for every community, and an end to conflicts around the world. We're grateful to have him representing BSS in the Tennessee community!

Business System Solutions

Return Address:
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544

The BSS ADVISOR

info@bssconsulting.com

North-Central Indiana Office
1211 Cumberland Avenue
West Lafayette, IN 47906
(765) 742-3440

Middle Tennessee Office
1026 West College Street
Murfreesboro, TN 37129
(615) 819-0600

West Michigan Office
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544
(616) 776-0400

Important announcement for Quickbooks Users

Quickbooks is phasing out its desktop product offerings and encouraging buisinesses to move to one of its online products.

After September 30, 2024, Quickbooks Desktop plans (Desktop Pro, Premier, or Mac versions 2021 and older) will no longer be offered for purchase. Quickbooks Enterprise will be the only desktop version that will still be offered and supported.

Quickbooks will still be supported and updates will continue for existing customers until your subscription is up for renewal.

However, **if your subscription expires or you choose to stay on an unsupported version, you will not be able to access technical services or have access to add-on services** including Desktop Payroll, Desktop Payments, and online bank feeds until you move your subscription to a different service.

If you are not ready to make the switch to Quickbooks Online, consider purchasing a Quickbooks Desktop Plus subscription before September 30, 2024. If you need guidance or more information, reach out to your BSS Account Manager for more information.