SMALL BUSINESS BIG TARGET

BE RESILIENT

You might think, "My business is too small to be noticed by hackers." This misconception is exactly what cybercriminals exploit. Small businesses often lack robust cybersecurity measures, making them low-hanging fruit for attacks. The notion of Small Business, Big Target isn't just industry jargon—it's a call to action for businesses like yours to recognize and mitigate cyber risks.

Your interconnected digital systems offer unparalleled opportunities for growth but also expose your business to cybersecurity threats. Protecting your assets, maintaining business continuity, and safeguarding customer trust are no longer options—they are necessities.

PAIN POINTS

What makes your business attractive:

- Limited IT Resources: Small businesses often have minimal budgets for cybersecurity.
- Lack of Expertise: Without dedicated staff, recognizing and combating threats becomes challenging.
- Outdated Systems: Older hardware and software are more susceptible to attacks.
- Employee Negligence: Staff may not be trained to recognize phishing emails or suspicious links.

WITHSTAND. ADAPT. EVOLVE.

CYBER SOLUTIONS HUB
cybersolutionshub.com

WHY SHOULD YOU CARE

Cyber threats can cripple your operations, tarnish your reputation, and drain your finances. According to a report by Verizon, 43% of cyberattacks target small businesses. Yet, many small business owners underestimate the risks, believing that hackers only go after the "big fish." This false sense of security can lead to devastating consequences.

The High Cost of Ignorance

- Financial Losses: The average cost of a cyberattack on a small business is approximately $200,000.
- Reputational Damage: Customers lose trust when their data is compromised.
- Operational Downtime: Attacks can pause your business operations for days or even weeks.

TAKING THE NEXT STEP

- Conduct a Risk Assessment: Identify what data is most valuable and vulnerable.
- Implement Strong Password Policies: Use complex passwords and change them regularly.
- Invest in Security Software: Antivirus and anti-malware solutions are essential.
- Regular Updates and Patches: Keep all systems and software up to date.
- Employee Training: Educate your team about cyber threats and safe practices.

KEY STRATEGIES

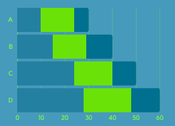
Foster a Resilient Company Culture
Promote a flexible, inclusive, and positive work environment. Encourage cross-functional training and ensure employees feel supported during this change. Employees who are adaptable and engaged are vital to your resilience.

Cybersecurity Preparedness
Invest in employee training, robust cybersecurity measures, and data backup systems to prevent data breaches and cyber-attacks.

Develop a Crisis Management Plan
Create contingency plans for various scenarios, assign roles, and communicate with employees and stakeholders effectively during these times. A proactive plan helps reduce panic and uncertainty during crises.

66% of SMB owners believe they are unlikely to be targeted by online criminals.

60% of SMB data breaches were due to negligent employees or contractors.



58% of consumers would avoid doing business with an organization that suffered a data breach.

60% of SMBs close within six months after experiencing a cyber-attack due to the financial strain.

BUILD AWARENESS

As a founder or executive, your attitude toward cybersecurity sets the tone. Demonstrate its importance by allocating resources and prioritizing initiatives.

IMPORTANT!
Cyber threats evolve rapidly. Regularly review and update your cybersecurity measures to adapt to new challenges.

BEST PRACTICES

- Educate Employees Regularly: Keep your team informed about the latest threats.
- Secure Wi-Fi Networks: Use strong encryption methods for all wireless networks.
- Implement Multi-Factor Authentication (MFA): Add an extra layer of security beyond passwords.
- Monitor Network Activity: Regularly review logs for suspicious activities.
- Establish Cybersecurity Policies: Formalize rules and procedures.
- Use Virtual Private Networks (VPNs): Secure remote connections.
- Limit Physical Access: Protect hardware from unauthorized personnel.
- Dispose of Data Properly: Shred physical documents and securely erase digital data.
- Prepare for Insider Threats: Not all threats come from outside; monitor internal activities.
- Engage Cybersecurity Professionals: Consider hiring experts or consultants.