UNDERSTANDING CYBER RISKS

PROTECT YOUR BUSINESS TODAY

MIKE O'DONNELL | SAFE COMPUTING | 2026

Email: info@safe-computing.net
Website: https://safe-computing.net

RISKS FOR SMALL BUSINESSES

Small businesses face significant information technology risks that can jeopardize their operations, financial stability, and reputation. Despite their smaller size, these businesses are increasingly reliant on digital systems and technologies to manage critical aspects of their operations, including customer data, financial transactions, and internal communications.

WHAT ARE THE RISKS?

The consequences of a cybersecurity attack on a small business can be severe and multifaceted, including:

- Financial Loss: Cyberattacks can lead to direct financial losses from theft of funds or ransom payments, as well as indirect costs such as legal fees, regulatory fines, and increased insurance premiums.
- Operational Disruption: Ransomware or other attacks can cripple business operations, leading to downtime, loss of productivity, and missed opportunities.
- Reputation Damage: A breach can erode customer trust and damage the business's reputation, leading to the loss of customers and difficulty in acquiring new ones.
- Data Loss: Sensitive information, including customer data, financial records, and intellectual property, when compromised, can lead to severe legal and operational repercussions.
- Legal and Regulatory Consequences: Businesses may face legal action from affected customers and regulatory penalties for failing to protect sensitive data.

- Recovery Costs: Restoring systems, data, and trust can be expensive and time-consuming, requiring significant investment in cybersecurity measures and public relations efforts.
- Customer Attrition: Customers may leave for competitors who are perceived to have better security practices.
- Loss of Competitive Advantage: Intellectual property theft can result in loss of competitive advantage and market position.

By understanding these potential consequences, small businesses can better appreciate the importance of investing in robust cybersecurity measures to safeguard their operations and future.

Safe Computing
Web: https://safe-computing.net
Email: info@safe-computing.net

WHAT ARE THE SPECIFIC RISKS?

Cyber threat actors utilize a wide array of tools that create risks for your business.

- Phishing attempts try to trick individuals into revealing sensitive information by posing as a trustworthy entity, often via email.
- Malware is malicious software designed to damage, disrupt, or gain unauthorized access to computer systems. Viruses, worms and trojans are types of malwares that can attack your business.
- Ransomware encrypts data and demands a ransom for its release.
- Spyware is Software that secretly monitors and collects user activity and information without consent.
- Rootkits are software tools that enable an attacker to gain undetectable privileged access to a computer.
- Adware is software that automatically displays or downloads unsolicited advertising material. Adware is often bundled with other software and can slow down systems or lead to malware infections.
- Denial of Service (DoS) Attack are Attempts to make a machine or network resource unavailable by overwhelming it with traffic.

- Man-in-the-Middle (MitM) Attacks intercept and alter communications between two parties without their knowledge. This allows the attacker to eavesdrop, steal data and even hijack your computing session.
- Zero-Day Exploits are attacks that exploit previously unknown vulnerabilities in software. There is high potential for damage as there is no immediate defense.
- Insider Threats are risks posed by individuals within the organization, either maliciously or accidentally
- Social Engineering manipulates or tricks individuals into divulging confidential information.

There are mature and efficient processes and tools to prevent or recover from these risks. Studies show that approximately 90% of cybersecurity issues are the result of human error. Cybersecurity awareness training is one of the least expensive and most effective ways to prevent issues.

Safe Computing
Web: https://safe-computing.net
Email: info@safe-computing.net

HOW TO PROTECT YOUR BUSINESS

Protecting your small business from cybersecurity threats is crucial. Here are practical steps you can take:

- Train Employees: Educate your team to recognize phishing emails, how to use strong passwords, and following best internet practices.
- Be Wary of Phishing Scams: Do not click on links or download attachments from unknown or suspicious emails. Always verify the source before sharing personal information.
- Use Strong Passwords and Multi-Factor Authentication (MFA): Implement MFA and encourage the use of complex passwords using a password vault product.
- Keep Software Updated: Ensure that your operating system, software, and apps are up to date with the latest security patches.
- Secure Your Networks: Use firewalls, encrypt your internet connection, and ensure your Wi-Fi network is secure and hidden.
- Implement Security Policies: Establish strong IT and security governance policies.
- Use Antivirus Software: Install and regularly update antivirus software on all business devices.
- Secure Remote Work: If employees work remotely, use Virtual Private Networks (VPNs), and ensure endpoint security measures are in place.

- Create an Incidence Response Plan: Be prepared for how to respond in the case of a cyber-attack.
- Manage Your Accounts: Employ the principal of least privilege and access control lists to limit data access that required for an employee's duties.
- Monitor Your Accounts: Regularly check your financial and online accounts for any suspicious activity.
- Stay Informed: Keep up with the latest cybersecurity threats and best practices.
- Consult Experts: If possible, hire a cybersecurity consultant or Chief Information Security Officer (CISO) to develop a comprehensive security program.

Implementing these measures can significantly reduce your risk of falling victim to cyber threats.

Safe Computing
Web: https://safe-computing.net
Email: info@safe-computing.net

SAFE COMPUTING

IS HERE TO HELP

Small companies are busy running their business. Allocating resources to care for cyber safety may be perceived as unnecessary, too expensive or time consuming. It does not have to be.

Safe Computing tailors' services in accordance with the CIS 8.1 Framework, leveraging those controls that make sense for your business size and specific needs. Whether your company has one computer with three employees or hundreds of employees and a data center, Safe Computing is ready to meet your requirements.

- Inventory control
- Data Protection
- Account Management and Controls
- Malware Defenses
- Data Protection and Recovery
- Infrastructure Monitoring
- Disaster Planning and Recovery
- Vulnerability Management
- Audit Log Management
- Email and Web Browser Protections
- Virtual Private Networks
- Incident Response Management
- Incident Recovery
- Technology Solutions

To schedule a free, one-hour consultation, please contact us via email or phone:

Mike O'Donnell
Phone: 512-228-0411
Email: mike@safe-computing.net

UNDERSTANDING CYBER RISKS
PROTECT YOUR BUSINESS TODAY

Safe Computing
Web: https://safe-computing.net
Email: info@safe-computing.net