
SME ONE
Building Resilient IT Systems:
A Guide for Small Business Owners
www.smeone.co.uk
GEEK ~~not~~ GEEK

Introduction

Have you ever considered how crucial your technical systems are to the success of your business? It might not be a top priority for most business owners until the day those systems go down. Your technology systems form the foundation of your business and are essential for driving success. Implementing the right systems can support your business and propel it forward.

Understanding IT Resilience

IT resilience refers to your company's ability to withstand and recover from disruptions, whether technical, human, or cybercriminal. It encompasses both preventive measures to avoid outages and strategies for rapid recovery when outages occur. Here’s how to enhance your IT resilience.

Steps to Enhance IT Resilience

Step 1: Conduct a Risk Assessment

Asset Identification and Classification

- Create a comprehensive inventory of all valuable assets, including hardware, software, and data.
- Rate each asset based on its sensitivity and importance.

Threat Identification

- Identify potential threats to your assets, such as system failures, natural disasters, human errors, and cyber-attacks.
- Rate the likelihood and potential impact of each threat.

Vulnerability Assessment

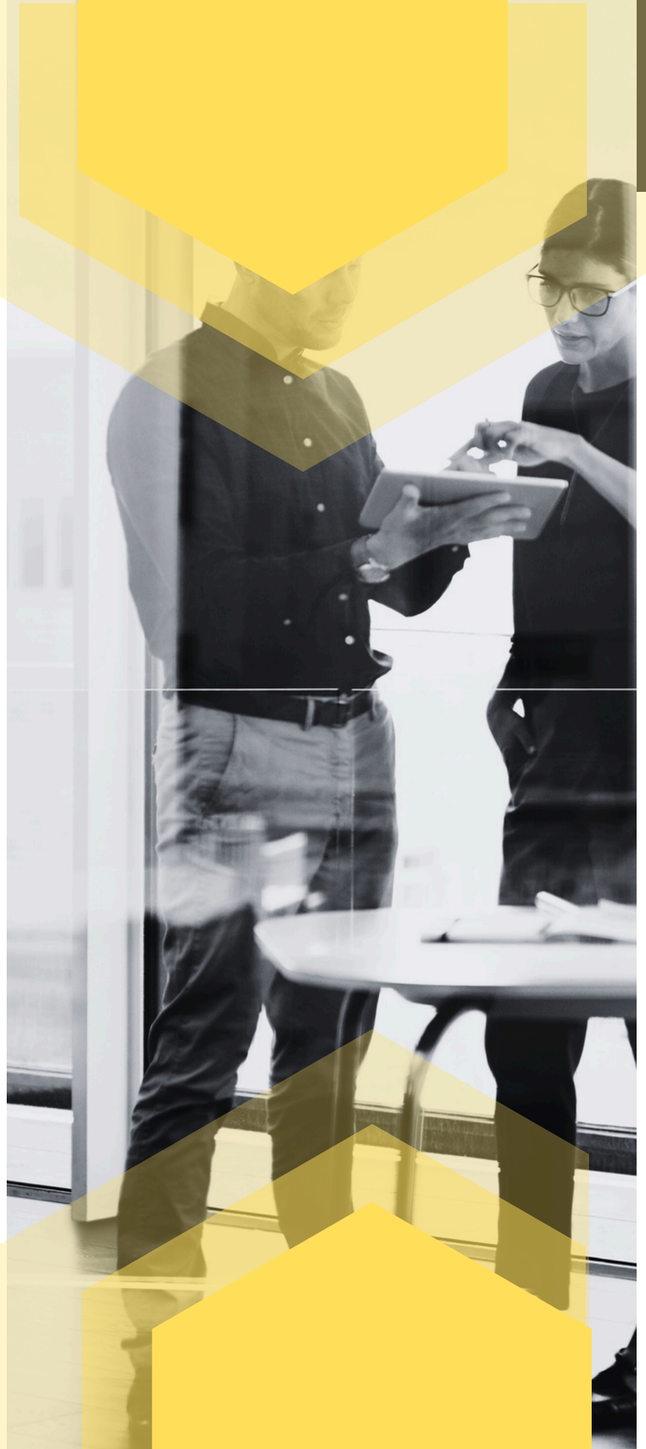
- Determine weaknesses that could be exploited by threats.
- Use automated vulnerability scanning tools.
- Assess current security measures and identify gaps.

Impact Analysis

- Understand the potential consequences of system outages and security breaches.
- Analyze the impact on business operations, financial losses, downtime, legal consequences, and reputational damage.

Risk Scoring

- Calculate risk levels using the formula: Risk = Asset Value x Threat Likelihood x Vulnerability.
- Prioritize risks based on their potential impact by assigning risk scores (high, moderate, low) and identify critical areas that require immediate attention.



Step 2: Take a Pro-Active Approach

Adopt Cloud Solutions

- Cloud solutions often come with built-in resiliency features such as geographic redundancy, load balancing, redundant systems, 24/7 monitoring, proactive maintenance, security, and compliance measures.
- Be thorough in investigating what is included in your cloud provider's offerings.

Plan for the Worst

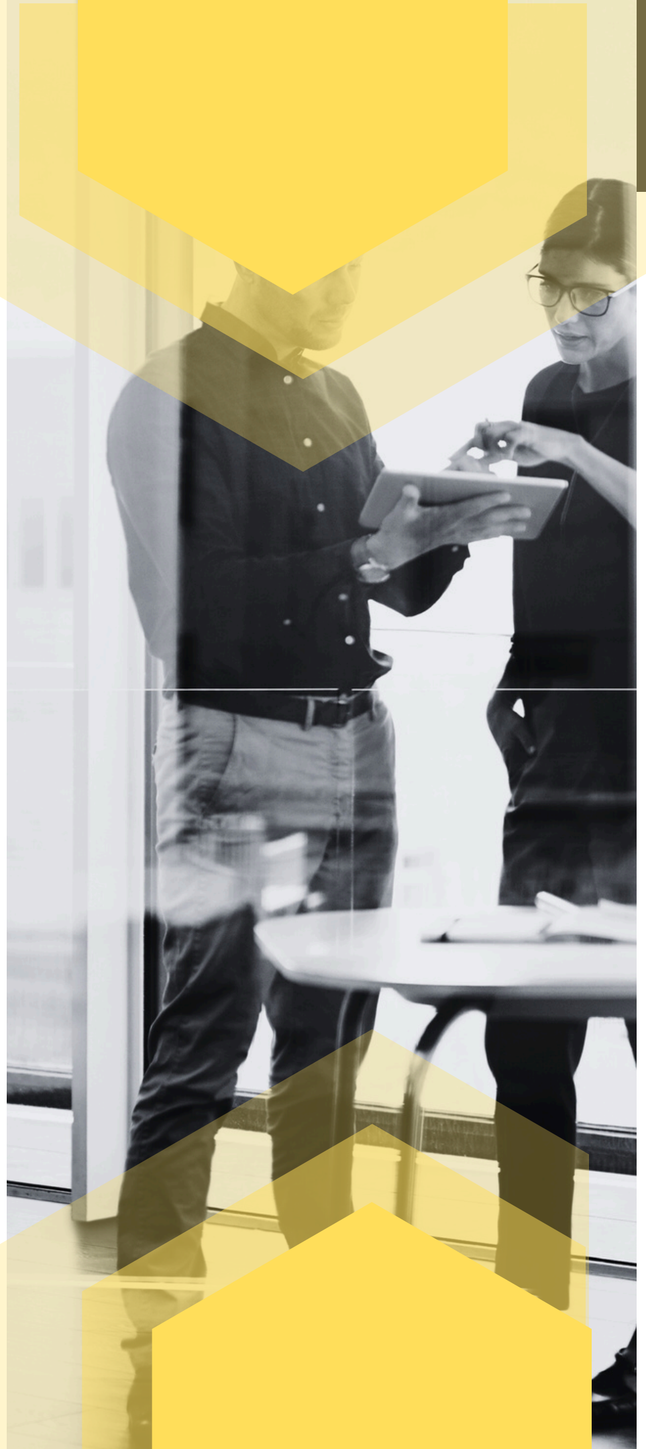
- Implement regular data backups (remembering that backups and disaster recovery are not the same thing).
- Use the 3-2-1 rule for backups: 3 copies of your data, 2 different locations, 1 off-site.
- Regularly test backup restorations to ensure data can be recovered when needed.

Pro-Active Network and System Monitoring

- **Implement continuous 24/7 monitoring to catch issues before they escalate.**
- **Set up alerts and notifications to IT staff for potential problems.**

Daily Operational Excellence

- Conduct system health checks, monitor performance, and review system logs.
- Verify backup status and perform test restores.
- Ensure security measures are up to date.
- Apply critical security patches and updates.
- Regularly review and adjust user access levels.
- Monitor network bandwidth and the status of network devices.
- Adhere to company policies and compliance requirements.
- Manage hardware assets and software licenses.



Step 2: Take a Pro-Active Approach

Enhance Cybersecurity Measures

- Install and maintain firewalls and anti-malware software.
- Keep all systems and software updated with the latest security patches.
- Train employees on cybersecurity best practices.
- Use a global user management system like Active Directory.

Invest in Uninterruptible Power Supplies (UPS)

- Ensure critical systems like servers and networking equipment have backup power sources.

Leverage IT Support Services

- Decide between hiring an in-house IT team or outsourcing IT functions based on your business needs.
- Weigh the pros and cons of each option to make an informed decision.

Step 3: Redundancy and Failover

Backup

- Back up everything you budget allows for
- Follow the 3-2-1 backup rule
- Automate your backups
- Perform regular backup tests

Disaster Recovery Options

- Choose target locations for your disaster recovery environment, ensuring geographic separation.
- Options include duplicating hardware or replicating environments in the cloud.

Disaster Recovery Solutions

- Evaluate your needs based on acceptable downtime and budget.
- Options range from simple backup and restore to complex active-active configurations.
- Consider the following solutions:
  - Backup and Restore: Cost-effective but with long recovery times.
  - Pilot Light: Minimal environment always running in the cloud, ready to scale up.
  - Warm Standby: Scaled-down version of the production environment running in standby mode.
  - Hot Standby (Active-Passive): Fully functional replica of the production environment maintained offline.
  - Active-Active (Multi-Site): Two or more fully operational environments running simultaneously for continuous availability.

Conclusion

Planning for IT resilience involves a combination of risk assessment, proactive maintenance, robust security measures, and redundancy planning. By following these steps, you can ensure your business remains operational during disruptions, thereby safeguarding your success and growth.

Thank You

Phone: 0333 335 5676
Website: www.smeone.co.uk
Email: buzzbox@smeone.co.uk

SME ONE