

THE TOP 10 BUSINESS TECHNOLOGY MISTAKES

(And How IT Consultants Help Clients Avoid Them)

Small Business Focus

- **Businesses DO:**
 - Concentrate on learning/maintaining knowledge of their industry
 - Commit to client satisfaction
 - Operate their businesses (servicing plumbing needs, selling real estate, completing tax returns, seeing patients, etc.)
- **Businesses DON'T:**
 - Wish to become information technology experts
 - Track daily patch, fix, update and other hotfix news and bulletins
 - Invest time tracking security announcements
- **As a result, 10 common technology mistakes occur**

#1: Insufficient Technical Support

- Small businesses too often rely upon:
 - Warcraft gamers turned “gurus”
 - A staffer’s relative who’s a “geek” by desire
 - PC manufacturers’ toll free numbers
 - An electronics store employee learning the business
 - A technician performing service “on the side”

Support Recommendations:

- Small businesses should develop long-term relationships with professional IT consultants
- Professional IT consultants:
 - Resolve failures faster
 - Leverage skills and knowledge to service critical client technology needs
 - Determine appropriate hardware/software solutions
 - Deliver proven monitoring and preventive maintenance services
 - Reduce downtime
 - Cut costs

#2: Hardware/Software Issues

- Organizations often operate PCs too long
 - Cheap components and older systems are more likely to fail
 - Obsolete hardware is inefficient
- Inconsistent hardware and software:
 - Slows failure diagnosis and recovery
 - Complicates license tracking while increasing support burdens
 - Increases the likelihood of incompatibilities

Hardware/Software Recommendations

- Small businesses can overcome common hardware/software issues by:
 - Retiring equipment at proper lifecycles
 - Standardizing hardware components
 - Standardizing software applications
 - Maximizing technology investments

#3: Insufficient Power Protection

- A single electrical event can destroy expensive components and corrupt critical data
- Even small but consistent electrical events damage systems
- Resulting data recovery, repairs and downtime are expensive

Power Recommendations

- Steps small businesses can take to help themselves:
 - Deploy high-quality battery backups on all critical PCs
 - Ensure all servers are connected to dependable uninterruptible power supplies
 - Confirm IT staff properly install and configure communications cables and software
 - Leverage network protections
 - Use only high-quality surge suppressors on other PCs
 - Regularly replace surge suppressors and UPS batteries
 - Avoid using simple power strips

#4: Illegal Software

- Estimates suggest 22% of North American software is unlicensed
- Licensing terms prove confusing
- Manufacturers are cracking down on violators
- Organizations don't "own" software
- Pirated and improperly licensed software slows recovery

Licensing Recommendations

- There are no shortcuts to running legitimate operations
- Manufacturers are increasingly implementing product activation features
- Carefully document and track all license purchases
- Only purchase software from reputable partners
- Carefully read all license agreements

#5: Insufficient Training

- Estimates suggest office workers understand less than 20% of available software features
- Inefficiencies (and errors) result
- Limited skills mean tasks needlessly require more time

Training Recommendations

- IT consultants can prepare and deliver simple lunch-and-learn presentations
- Businesses can partner with local training centers
 - Customized training programs can target specific needs
 - Prepackaged training modules teach fundamentals
- Self-paced manuals and computer-based training aids assist employees training off site or after hours
- Training requirements should be tied to performance review objectives

#6: Security Failures

- Businesses often fail to take security concerns seriously
- Malicious programs work nonstop to:
 - Steal and/or delete proprietary, sensitive and/or client and customer data
 - Render systems unusable
 - Enable hackers to control PCs remotely
- Security breaches often result in bad press, lost sales and forfeited customer trust

Security Recommendations

- Several steps assist small businesses in correcting security failures:
 - Implement and enforce password policies
 - Regularly install security updates
 - Deploy business-class firewalls
 - Disable guest accounts
 - Implement Internet and email policies
 - Prohibit file sharing programs
 - Deploy proven security software
 - Perform regular security audits

#7: Poor Backup Strategies

- Data losses can prove irrecoverable
 - There is a 50% chance an organization will go out of business immediately when critical data is lost
 - Odds of business failure increase to 90% within two years
 - Data losses cost an average of 19 days' productivity
- Data recovery from damaged drives is incredibly expensive and time consuming
- Businesses sometimes back up the wrong data
- Gartner estimates only half of all tape backups restore successfully

Backup Recommendations

- Technology professionals assist small businesses by helping:
 - Identify critical data
 - Determine backup schedules
 - Regularly restore backup sets
 - Update backup routines when required
 - Secure backups

#8: Virus Exposure

- Viruses pose serious threats
 - Improperly protected systems have become infected within eight seconds of being connected to the Internet
- Viruses are expensive
 - Estimates place the average cost per incident at \$2,500-\$99,000 or more
 - Downtime and data recovery slows business operations
- Virus threats are increasing, yet many businesses have no protection or outdated software

#9: Spyware Exposure

- Spyware programs pose a significant threat to small businesses
- Whereas viruses often aim to corrupt or remotely control systems, spyware typically monitors a user's behavior, attempts to obtain sensitive information or displays unwanted advertising
 - System performance frequently suffers
 - User productivity plummets
- CompTIA found infection rates exceeding 25%

Virus/Spyware Recommendations

- No anti-virus and anti-spyware strategy is perfect
- Technology professionals typically recommend:
 - Installing reputable antivirus and antispyware programs
 - Installing a second antispyware program in high-risk environments
 - Updating security programs regularly
 - Ensuring security programs don't expire
 - Performing regular automated scans
 - Regularly review security software log files
- Businesses should avoid deploying "free" products

#10: Unsolicited Email

- Most every user and business is familiar with unsolicited email
- Half of all email is likely spam
- Businesses waste time and resources processing and storing spam
 - Unsolicited email's business costs are believed to exceed \$20.5 billion annually

Spam Recommendations

- The best spam defense is multifaceted:
 - Implement server- or network-based filters, when required
 - Follow best practices when sharing an email address:
 - Don't publish email addresses on Web sites
 - Avoid chain, get-rich-quick and similar email solicitations
 - Leverage email application filters
 - Read all terms and privacy policies when sharing an address
 - Consider creating a free standalone email account when signing up for newsletters, creating user accounts on Web sites and fulfilling similar tasks

Thanks For Your Time

- Are there any questions?
- For more information, contact your IT department or consultant