7 AVOIDABLE MISTAKES MOST IT MANAGERS MAKE

TECH LEADER GUIDE

The Swenson Group

People · Passion · Purpose

While small to midsized businesses (SMB) don't have the luxury of IT resources that large enterprises can afford, they still face many of the same challenges.

Regardless of size, all businesses depend on technologies to operate efficiently. Company data resides on networked computers and employee productivity depends on having access to that data at all times and securing it from loss or theft.

Managing IT that supports the business comes in different forms and the following are 7 common mistakes SMBs make and how to avoid them.

“ 66% of businesses could not survive without a solid technical department. ”

-Poll performed by AT&T

“ 94% percent of small businesses are concerned about cybersecurity. ”

- NSBA survey

“ Companies that aren't able to resume operations within 10 days of a disaster hit are not likely to survive. ”

-Strategic Research Institute

✕ No Standardization

Buying technology on a piecemeal basis can leave your business vulnerable to higher service costs and network security threats.

Most companies start small and grow over time, accumulating new workstations and tech systems as increased demand and revenue call for it. Usually, the hardware and software purchases made by SMBs aren't part of a carefully planned investment strategy.

Thus, SMBs often end up with whatever was on sale at the time, or recommended, or requested by an employee - a fine short-term strategy, maybe, but one that can leave you with a hodgepodge of technology to operate and unnecessarily high IT costs down the road.

The smarter approach to tech purchases is standardization. Recommended by IT and security experts, standardization essentially means that instead of buying whatever device you like the most or found for the cheapest price, your hardware, software, and system purchases are guided by a clear technical norm.

Focus on security, not tech sales

An appetite for the latest tech deals generally leads to piecemeal purchases, and that can make it harder to keep business and customer data secure.

Generally, small businesses don't standardize technology at all, because they're always thinking about deals. When you're just buying parts, you can get really good deals. But most small companies either lose their purchase-price savings to increased maintenance costs later, or to shorter hardware lifespans because they've skipped maintenance altogether. And there's another consideration: The tangible and intangible costs of network security issues that arise when business systems aren't properly designed and serviced.

Having standardized IT technology makes it easier to not just secure your network, but also to respond and mitigate a threat in case you do become a target.

The more systems you use, the less likely your network administrator is to have mastered any one of them; standardization narrows the focus to one system, which puts the business in a more agile position when an emergency arises.

Business owners need to think long-term and plan ahead. Standardizing your IT hardware and software will help achieve just that.

Weak Network Security

Three common factors emerge when dealing with network security; vulnerability, threat and attack.

Vulnerabilities

An experienced hacker knows that every network or device has a certain degree of vulnerability or weakness and they take advantage of each security weakness or loophole to exploit the network. A hacker works round the clock in search of unsecured networks or devices to exploit. These includes routers, switches, desktops, servers and even security devices.

They use a variety of tools, programs and scripts to accomplish these threats. The primary network vulnerabilities or weaknesses are: Technological, Configuration and security policy weaknesses:

Technological weaknesses: every computer network and device has an inherent security weakness. These include TCP/IP protocol (HTTP, FTP, SMTP, SNMP) on which the Internet was designed, operating system (Unix, Linux, Mac OS, Windows OS), and network equipment weaknesses (Routers, Firewalls, Switches etc.).

Configuration weaknesses: incorrect configuration or application of security software or firewall devices due to laxity can compromise a network. These include unsecured user account information or passwords, system account information or passwords, misconfigured internet services, unsecured default settings within products, misconfigured network equipment – ACLs or routing protocols. All of the above enable the creation of security holes that every experienced hacker is looking out for.

Security policy weaknesses: Every organization must have a security policy that governs and maintains how the network or company information should be used. Security risks to the network exist if users do not follow the security policy. Security weaknesses emerge when there is no clear cut or written security policy document. A security policy meets these goals:

- To Inform users, staff, and managers of their obligatory requirements for protecting technology and information assets
- Specifies the mechanisms through which these requirement can be met
- Provides a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy

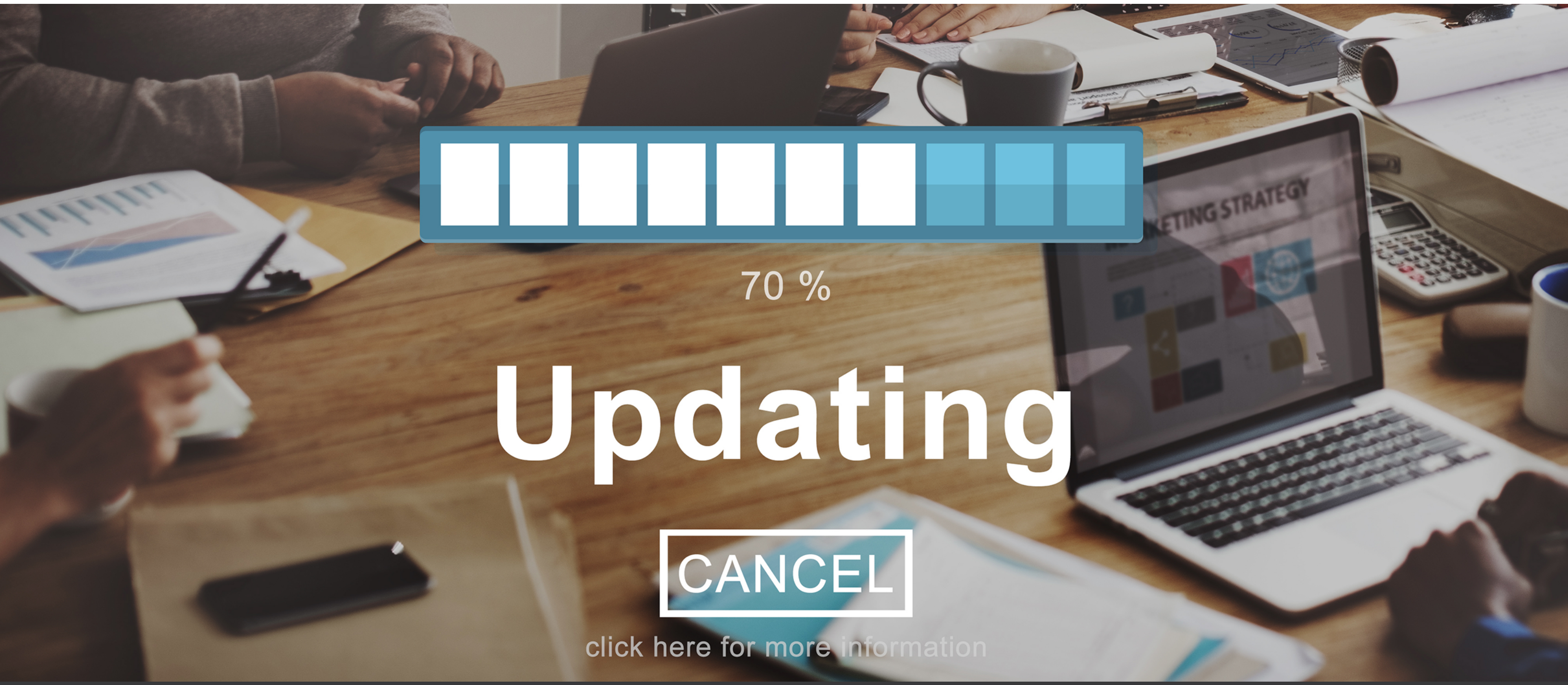
Unpatched Software

To prevent security threats most organizations implement multiple security tools. However, unpatched software provides a backdoor for hackers to penetrate systems and the entire IT infrastructure. Over the past decade, software vulnerabilities have increased drastically. Most security breaches occur by exploiting unpatched operating software, network equipment, internet related software, including add-ins and browser helper objects.

Once penetrated, a business is at risk to any number of threats:

- Installing malware to steal data or disrupt normal operations
- Corrupt or destroy data file
- Steal sensitive company information
- Complete hard drive erasure
- Encrypt data files and demand ransom payment to restore

All these threats can be very simply avoided or at the very least minimized by following a documented security audit policy to periodically check all operating systems, firmware and application software for updates. Updates are provided free of charge and often include new features and productivity enhancements.



Legacy Infrastructure

Organizations rely on computing systems to run their operations, but for many, those networks have been built up over a number of years. As a result, many organizations find themselves relying on legacy infrastructure.

Maintaining legacy systems can be costly. A recent U.S. Government Accountability Office (GAO) report found that in 2015, 26 federal agencies spent $60 billion of their $78 billion technology budget on legacy investments. In a recent poll of the banking sector conducted by Temenos, 80% of respondents agreed that "aging IT is the biggest threat to banks today." It also found that three quarters of most IT budgets is spent maintaining legacy systems.

Legacy infrastructure can lead to undesirable situations. If Windows XP is still in use, Microsoft says that it is 6 times more likely to be infected with malware than newer versions of Windows. Other problems include systems that are impossible to patch or for which no patches are available.

Legacy technology is both a security issue and a hindrance to innovation according to FierceGovernmentIT.

New technologies provide greater flexibility, efficiency, intelligence, automation and security. They allow an organization to be more agile, remain innovative and align costs to actual usage. They are generally less complex and easier to manage, and many come with embedded capabilities such as policy management, encryption, au-thentication and continuous monitoring for greater control.

Given the high cost of maintaining legacy systems and the risks they can introduce; risks that lead to dented reputations, reduced profitability and hindered competitive-ness from inability to innovate.

New technologies will also give organizations the opportunity to increase revenue by providing better customer service across multiple channels, which will set an organi-zation apart from its competitors.

Organizations should take a good look at their infrastructure.

No data access policies

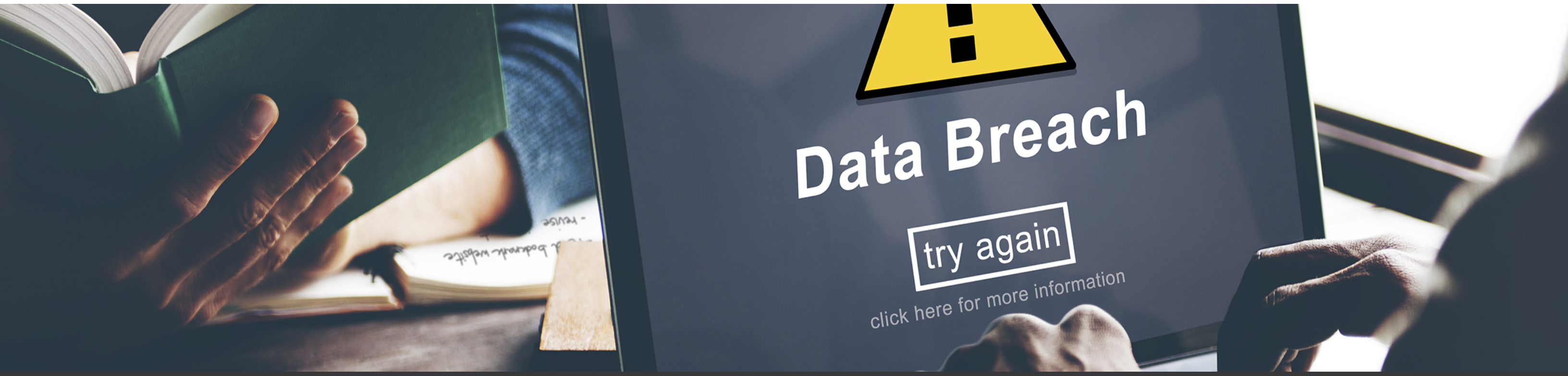
Think of how much chaos there would be if everyone in your organization had access to all the company's information on all their systems and applications. Employees could make changes to secure data, such as payroll and customer information. Surprisingly, many organizations have minimal access management structures in place or they think they are managing access properly, when they actually don't. Without proper access management, security risks are high and it is easy to lose track of who has access to what, easily leading to a security breach.

Organizations often focus mainly on protecting the network from outside hackers, but in reality, many breaches come from employees within a company. This is why it's important to ensure that all employees only have access to resources they need to perform their job or function, especially if your business deals with highly sensitive company and client data.

Even if proper access rights are set for an employee, often they share their access and passwords with others on certain projects, which are never changed. Even more im-portantly, access rights should be removed for employees that have changed roles or leave the company, so a disgruntled former employee cannot access any company data.

Access management becomes even more important when it comes to audits and compliance issues. Without proper access management, organizations can't ensure they meet governmental standards or audit rules. This exposes the company to signif-icant penalties including financial ones.

To mitigate risk, there needs to be an access management plan in place. The minimum plan should include a process to creating and managing user access rights to data and applications, both on premise and in the cloud. This ensures that employees, depending on their role and location, have the correct access to only the application they need for their jobs and not to everything on the network. There are many role-based access control solutions available that makes it easy to quickly apply access controls.



✕ Don’t understand Cyber threat

No business is completely safe from security vulnerabilities. Just look at Target, Home Depot and TJ Maxx. While these companies may seem like a more attractive target for hackers, small businesses face the same, if not more, threats from cyber attackers looking to disrupt a company.
Even as we deploy security solutions to our infrastructure, another source that is seldom addressed is employee awareness of how they could inadvertently expose the company to cyber threats from simple actions like opening email attachments or clicking on a link within an email (phishing) from sources they don’t recognize.

Crypto-Ransomware Hostage Crisis

A very prominent threat today is Crypto-Ransomware, a family of malware that take files on a PC or network storage, encrypts them and then extorts money to unlock the files. When Ransomware Malware is found.

Employees need to understand the expensive and sometimes horrific impact a simple action can inflict on a company. Businesses need a backup solution for disaster recovery and business continuity, but with Crypto-Ransomware attacks, it’s more important than ever that the backup be secure. Even when an organization pays the ransom, there’s no guarantee they’ll get their data back easily or intact – and they may be targeted continually afterward as an easy mark.

As employees engage in sales and networking across social networks, new pathways into the business open up and cyber criminals know how to exploit them. One of the most effective actions businesses can take to reduce the risks that come from our in-terconnected marketplace is to provide knowledge. Many users do not understand how cyber criminals leverage social tools and technologies to gain access to business-es and their data.

People remain the biggest security risk to any sized organization

As threats become more sophisticated, even careful employees may find themselves victims of phishing or accidently opening attachments with viruses. The best defense is ensuring that staff get consistent education to keep security top of mind. A busi-ness needs to be smart about balancing in-house security resources and building a strong team, while leveraging third-party security services. Every organization should consider bringing in a third party to get a vulnerability assessment. Even if you have a dedicated security team, a second pair of eyes will help identify risks and start work-ing towards remediation. Most companies don’t take security seriously enough until something happens. It is generally a lot more expensive to clean up after a security breach, than addressing it proactively.

No data backup or disaster recovery plan (BDR)

Bad things happen to good businesses

Floods, fires, earthquakes, the outside thief and the insider thief, and of course malware are all factors that can impact the safety of stored data. Data loss is costly and extremely risky; that's why every business needs a backup and disaster recovery (BDR) solution.

BDR solutions keep businesses safe when trouble strikes. When a small business doesn't have a BDR solution in place, it's probably because they're unclear about the true value of BDR. Here are the top reasons why these solutions are so important to the health of your organization.

Protects against the effects of natural disasters – whether it's a flood, earthquake, hurricane, blizzard or some other extreme natural disaster, there are plenty of uncontrollable circumstances that can cause your business to experience downtime. According to the National Archives and Records Administration, more than 90% of companies that experience at least seven days of data center downtime, go out of business within a year. So while a BDR plan won't prevent a natural disaster from occurring, it will pro-tect your data and ensure that downtime doesn't compromise your company.

Lessens impact of cyber-attacks – as more data is moved online, cyber criminals are increasing their efforts and focusing on businesses they believe are unprotected. Again, a BDR plan can limit the impact of an attack and can prevent your business from losing valuable data.

Keeps client data safe – if you store a lot of confidential client or customer data, you can't afford to lose this data or let it slip into the wrong hands. A BDR plan ensures that all of this information is properly stored and controlled. As a result, you don't have to worry about damaging your brand reputation unforeseeable incident arise.

People make mistakes – while we focus primarily on natural disasters and cyber-attacks, the reality is that our own employees are sometimes responsible for the big-gest data losses. Mistakes happen and a single poor choice can end up comprising data. That's why it's equally important to train employees properly as we invest in backup solutions.

Systems fail – we all know that hardware, machines and other systems fail, regardless of how much you spend on your technology – no solution is perfect. Even systems with 99.9% uptime guarantees will fail once in a while. That's why businesses must invest in robust BDR plans to recover from all these risks.

Summary

In case you're wondering if you're the only one making these mistakes – you're not alone. Limited knowledge, inadequate resources, competing priorities and real world distractions often make it difficult to avoid error in both judgement and execution.

That's why so many small and medium size organizations are leveraging third party expertise to ensure their IT systems are up and running when people need them. For more information about The Swenson Group's exclusive approach to Managed IT Services, we invite you to take advantage of our IT Assessment Services. A quick and easy way to expose opportunities to improve productivity and reduce costs.

The TSG IT Assessment Service, we're ready when you are.

Engage us for a complimentary IT & RISK ASSESSMENT and benefit from our experi-ence working with IT professionals like you.

RISK ASSESSMENT FOCUS

☑ Disaster recovery readiness
☑ Critical data backup for business continuity
☑ Recovery time predictability
☑ Device and network capabilities
☑ Infrastructure redundancy
☑ Change management preparation
☑ Security protection

You'll receive our **FACT BASED IT ASSESSMENT REPORT** with observations and suggestions you can use to benchmark your infrastructure vs. like environments.

The Swenson Group is an award winning, privately owned Managed Service Provider that provides IT services, document management and office equipment at a low predictable monthly expense.

People. Passion. Purpose.