The Small-Business Owner's Guide

to Avoiding an IT Disaster

willowbend SYSTEMS

Introduction

Today, every small business operates within a digital landscape of advanced information technology (IT) that makes all aspects of business operation possible. While small-business owners concentrate on running the business, the IT operating just beneath the surface that makes it possible is fraught with potential for disasters that can cripple or end the business.

According to Gartner. Inc., every minute of network downtime costs retailers an average of $5,600. That figure has gone up to $7,000 or more per the latest analysis. Retail or otherwise, network downtime at the storefront level means operations personnel can't meet the needs of their customers.

With many small businesses delivering their products and services through mobile apps, point-of-sale systems, and Web platforms, hacked systems could lead to customer data theft that triggers fallout that could end the business. Rather than hyperbole, these and other scenarios represent the eventual outcome of any number of IT disasters where data theft as well as network downtime or system incursions can cost the business its money, time, and reputation.

The first step to remedying the problem is understanding the threats that can lead to IT disasters. This eBook is designed to provide a compendium of the different threats and the ways that small businesses can guard against them with support from a skilled and experienced managed IT services provider.

Cybersecurity Threats

According to the 2016 Cybercrime Report from Cybersecurity Ventures magazine, nearly half of all cyberattacks are committed against small businesses. As threats and technology evolve, small businesses face difficult challenges that they cannot handle on their own.

In almost every case, the end goal of a cyberattack is the theft and exploitation of sensitive data. The truth of the matter is that the prudent approach is to view your business as either one that knows it's been hacked or a business that doesn't know it's been hacked. This perspective best illutrates the reality that no industry, sector, or business based on size is quarantined against a cyberattack.

Although today's hackers have technical skills that rival that of the most experienced security professionals, it is the indifference shown to cybersecurity by most small businesses that makes the threat so real. Small businesses are major targets for hackers because hackers know these companies are less careful about security.

One approach is for cybercriminals to target small businesses to compromise computers used for online banking and payments in order to commit fraud in a big way by emptying out business accounts. There are numerous types of small-business cyberthreat vulnerabilities with the following being the most prevalent:

Malware/Viruses

Malware (malicious software) is any computer program that can be introduced to a computer or network with the intent to cause damage or gain unauthorized access. Viruses like ransomware take it a step further by infiltrating a network and encrypting your business's data; the hacker then demands a fee for your data's release.

While the ransom can be thousands of dollars or more, restoring the data without paying the ransom can be much costlier if it is possible at all. It's important to understand that ransomware can infiltrate via several different access points.

According to a recent security report from cybersecurity provider Kaspersky Lab, the rate of ransomware attacks against businesses increased from one every two minutes to one every 40 seconds between January and September of 2016. As the number-one threat to businesses, a recent article in The Atlantic cited a cybersecurity firm that estimates extortive attacks now cost small and medium-sized companies at least $75 billion in expenses and lost productivity each year.

DDoS

Distributed denial of service (DDoS) is a cyberattack of brute force that uses many different systems to attack an individual target. This attack takes the form of a flood of incoming queries (messages, log-in attempts, etc.). That flood overwhelms the network and enables the attacker to gain entry and ultimately shut the network down. That means that clients, employees, customers, and other legitimate users cannot access the data, which stops the business in its tracks.

Hackers use botnets to "farm" the Internet for open ports on networks. When they find one with an opening, they flood it with queries. Today's DDoS attackers now have bitcoins (an online currency) that enables them to make money from such attacks, because the currency allows them to be paid anonymously. These types of attacks have happened to businesses with as few as five employees.

> "Small businesses are major targets for hackers because hackers know these companies are less careful about security."

Phishing

As per the 2016 Internet Security Threat Report published by Symantec, 43 percent of spear-phishing attacks were targeted against small businesses. These very common attacks collect sensitive information like log-in credentials and credit-card information through a fraudulent website, often sent to unsuspecting individuals in an email. There are numerous forms and levels of sophistication of these attacks that can target any individual in a business, including the owner.

Inside Attack

This is when an employee misuses credentials to access confidential company information. Former employees are usually the source of this type of attack, but it can also come from stolen credentials.

APT

Advanced persistent threats, or APTs, are long-term targeted attacks that break into a network in multiple phases to avoid detection. What is important to understand is that most of the cybersecurity threats mentioned in this guide can be APTs (malware, DDoS, phishing and other email/password attacks). This is really more of a broad industry term for the most sophisticated attacks that are characterized as potentially ongoing toward and within a business network.

Password Attacks

Password attacks can come in the form of brute-force attacks (guessing at the password until gaining entry), dictionary attacks (using a program to generate dictionary-word combinations), and keylogging (tracking a user's keystrokes to get log-in IDs and passwords).

It would take several eBooks to cover all the different cyberattack methods, tools, and approaches, but these are the most prevalent. While they all exploit the vulnerabilities in your business's IT infrastructure, there are a host of other dangers that can bring IT disasters from networking and technology dangers.

Unsecured Networks

Your data network is the foundation for the daily operation of your business and is often less secure than it needs to be. All the cyberthreats that we have discussed so far are ultimately targeting your network to gain control in one way or another.

An Information Age article cited the fact that "a business that tries to restore from a ransomware attack off of traditional backup usually loses weeks of work due to lost files, plus a day or more of downtime while computers are wiped and reloaded."

Network downtime in retail environments or eCommerce sites means the workforce or the site cannot meet customer needs. Consequently, customers unable to complete transactions may walk away from potential purchases online or in-store, while businesses that provide services will lose customers to competitors that can be immediately responsive.

Social media becomes the means to spread disparaging remarks that tarnish your brand, which ensures the network outage has a much longer impact on the health of your business.

Outdated and Inefficient Technology

The “end of life” issue for hardware and software can introduce a series of costs and compliance and security risks to an organization. Outdated hardware and software are not only vulnerable to attackers, but they slow down your productivity, which also has huge potential costs when:

A five percent productivity slowdown for a single employee due to inefficient older technology equates to 100 hours annually.

A single employee stopping for 30 minutes each week due to the repair of an older technology adds up to 125 hours over a year.

These figures are extrapolated across an entire workforce.

The goal of IT asset lifecycle management is to ensure that your hardware and software provide the maximum return on investment over their optimum life. A major part of that is to have the technical support to plan for IT hardware investment and replacement based on a defined schedule that coincides with quantifiable end of life.

All the potential IT disasters that have been discussed so far, and many more, have clear proactive remedies. These and other security solutions do more than enable a business to keep operating. They collectively form a security foundation that enables your business to lower costs, increase productivity, and, ultimately, let you concentrate on running the business rather than technology.

“ The goal of IT asset lifecycle management is to ensure that your hardware and software provide the maximum return on investment over their optimum life. ”

IT System Security Solutions

Proactive prevention is the key to stopping cyberattacks as well as hardware and software challenges that can lead to IT disasters. Most small businesses lack the basics in terms of knowing what solutions are available, which are best suited to their needs, and how to implement and monitor them. The first step is to gain a basic familiarity with some of these vital solutions.

Firewalls

Your first line of defense in preventing a DDoS attack is your firewall. Firewalls utilize hardware and/or software to protect your IT infrastructure like the network, computers, and applications from outside attackers. These protections can also be added separately to routers and servers. An experienced managed IT services provider (MSP) is in the best position to help you make the right choice about a solution and to install, configure, and monitor it to ensure its optimal protection performance.

Good Anti-Virus Software

The best security software products on the market offer guarantees, automatic updates, and support, but an experienced MSP can help make the best choice and provide additional remote monitoring support.

Regular Patch Updates

Most small businesses don't have someone to ensure that system and software updates are always done immediately to keep operating systems and applications up to date and vulnerabilities low. This can be automated in several different ways via the use of cloud-enabled business applications and systems (like Office 365, desktop as a service, and VoIP) as well as by automation software that can be monitored off site by an MSP.

Email Filtering with ATD

One of the most common methods to deploy a virus is through email attachments that are unwittingly opened by someone in your business. Email filtering software can scan inbound emails for potential threats found in both attachments and links and prevent that attachment from even entering your network.

In many cases, the victim opens a phishing email message with an attachment laden with malware that will let the attacker begin infiltrating the network. Spam filters work to catch these phishing emails and other junk. Web-surfing controls can introduce protection from Web-based malware that can enter through the business's Internet use.

Advanced threat detection (ATD) can notify your system of a virus within an hour of being found on the Internet to better protect your network. Advanced malware protection systems can track targeted attacks in various ways, while setting up a dedicated computing resource strictly for online fund transfers can be another option.

Bandwidth Monitoring

While high-growth companies may max out their bandwidth a few times a day, this bandwidth maxing can be a sign of attack for most small companies. This can start with an infected machine blasting outbound messages like an external DDoS attack. Bandwidth-monitoring software will identify if you have an unusual spike in Internet usage, both internally and externally.

Automated Hardware Monitoring

An MSP can implement software capable of automatically taking readings from hard drives, computers, and other hardware. Network traffic analysis and Internet usage analysis can be done remotely or on site via software that enables analysis of network traffic to uncover bottlenecks and bandwidth issues. This allows correction before your business is adversely affected.

Data Backup Solutions

Floods, fires, earthquakes, the outside thief and the insider threat, and, of course, malware are all factors that can impact the safety of stored data. For your business to continue functioning when the computer system goes down, you need to have a detailed data backup plan in place. Off-site backup prevents data loss even if there is some sort of physical disaster.

This should include:

- Automated backup to ensure up-to-the-minute copy of all network data to prevent loss during a disaster
- Having a virtual backup of your entire network to preserve your business data in case of a hardware or software failure
- Other solutions like encryption software to protect sensitive data such as employee records, client/customer information, and financial statements either in on-premises servers or in cloud-based storage
- Disaster recovery as a service is a turnkey solution service that is based on cloud services and that utilizes virtual servers and cloud storage for disaster recovery.

Identity and Access Management

The human factor in business is the greatest vulnerability source for cyber attackers, so system and data access requires a complete identity and access management system and approach. This is all about implementing software solutions that make it easier to codify and track access to IT systems and data as well as business premises. this can include things like multi-factor authentication (MFA), single sign on (SSO), passkeys biometrics, and password management among others.

> “The fact of the matter is that small businesses face the same number of, if not more, challenges faced by a large enterprise.”

Support for a Mobile Workforce

Today, it’s common for even a small business’ workforce to use mobile devices to access business applications like Office 365, CRM systems and more to work and collaborate outside of the office. This mobile workforce trend continues to grow. This is often an outgrowth of Bring-Your-Own-Device (BYOD) programs, which continue to proliferate where employees can use their own smartphones and tablets for business. A mobile device strategy might include mobile device management software, which provides the tools and framework to put safeguards in place to ensure a high level of device and network security.

It can be daunting for a small business that may not even have an IT department to think about how to tackle network security. The fact of the matter is that small businesses face the same number of, if not more, challenges faced by a large enterprise. Despite that fact, it’s important to remember that every business and its needed security solutions may be different, so it’s best to have an MSP run a risk assessment.

Summary

Every day, businesses struggle to remain innovative and competitive in a digital world where implementing and managing IT infrastructure complexity is becoming more and more difficult. This is especially true for small businesses with limited or no IT support in-house.

Growing IT options and decisions that are vital to avoiding IT and business disasters require the range and depth of expertise needed to select, maintain, and optimize the right IT solutions. The most experienced and skilled managed IT services partners bring broad expertise in all IT systems and components as well as proven implementation knowledge of these best-in class technology solutions. These solutions are part of long-term partner relationships with leading technology vendors. Together, these attributes enable small businesses to achieve their goals and concentrate on running the business.

Today, more and more organizations are leveraging managed network services from MSPs. They provide the benefits from services that are foundational to mitigating downtime driven by many factors, including man-made and natural disasters. These services include:

- Remote monitoring and remediation
- On-site support (when required)
- OS patching and anti-virus updates
- Asset performance analysis
- Firewall firmware updates
- Managed moves, adds, and changes for firewalls, switches, and virtual appliances
- Change tracking
- Policy management
- Effectively and efficiently manage IT systems
- Maintain regulatory compliance
- Proactive system maintenance and monitoring
- Respond to problems
- Provide end-user support
- Advise and consult on IT projects
- Complete IT-related projects

By working with a skilled and experienced MSP, small-business owners can manage risk in ways that are supported by constantly tested and refined behaviors that mitigate and eliminate threats to business interruptions.

About Willow Bend Systems

At Willow Bend Systems, we leverage your existing technology to develop IT solutions that work for you. With managed IT services, infrastructure hosting, IT hardware sales, and IP phone systems, we deliver comprehensive, streamlined IT solutions that help you focus on your customers, not your technology.

Willow Bend Systems
www.willowbendsystems.com
214.785.6830

Interested in learning more? Speak to a Willow Bend rep to see how we can help your small business avoid IT disasters.

CONTACT US

willowbend SYSTEMS