GRIT TECHNOLOGIES

Managed IT: Your Ally Against Downtime

HOW MSPS MITIGATE THE RISK AND EFFECTS OF DOWNTIME ON YOUR BUSINESS

MANAGED IT: YOUR ALLY AGAINST DOWNTIME

TABLE OF CONTENTS

What is the cost of downtime to your business?

Unplanned IT downtime can impair or stop your operations. It is more than just a simple inconvenience; in fact, it can have a number of severely damaging effects on your business, including:

Loss of productivity and revenue

"Time is money" may be a cliched adage, but it remains very true in business. When your operations cease for even just a few minutes, your company loses precious time that employees could have used to complete their tasks.

Additionally, any amount of unplanned downtime will almost certainly prevent you from making sales, manufacturing products, or rendering service to your customers. In a survey of small- and medium-sized businesses (SMBs), respondents reported losing up to $50,000 for every hour of downtime. Moreover, 25% of SMBs said they had lost clients because of the issue.

Damaged brand

Your customers rely on you for quality products and services. Unplanned downtime prevents you from using key IT systems, which may result in a dip in the quality of your outputs, or prevent you from providing any results.

Now, it's understandable for any business to encounter the occasional outage or two, but if this were to happen repeatedly, even your loyal customers may feel frustrated. Disgruntled clients may even share their negative experience with others, damaging your reputation and making it difficult to attract potential customers.

Loss of important data

Without proper measures in place, IT downtime can have unpredictable consequences. For instance, a server outage can lead to lost or corrupted data. Network security failure, on the other hand, can lead to data exposure or theft. These scenarios are already dire, but will be even more so if your company handles and relies on protected information and other sensitive data.

Service level agreement (SLA) payouts

SLAs are a guarantee that clients have consistent access to a vendor's products and services. In some cases, SLAs contain provisions that assure clients of financial compensation should the vendor be unable to deliver the expected output or service because of downtime. If you have such provisions in your SLA with your clients, then repeated downtime can result in heavy losses for your company.

Fines and penalties

Businesses in regulated industries like healthcare and finance are obligated by law to ensure the security and integrity of their clients' data. If an outage were to result in a data breach, industry regulators will look into the possibility of noncompliance. Your company will likely be subject to various lawsuits, as well as hefty fines and other penalties.

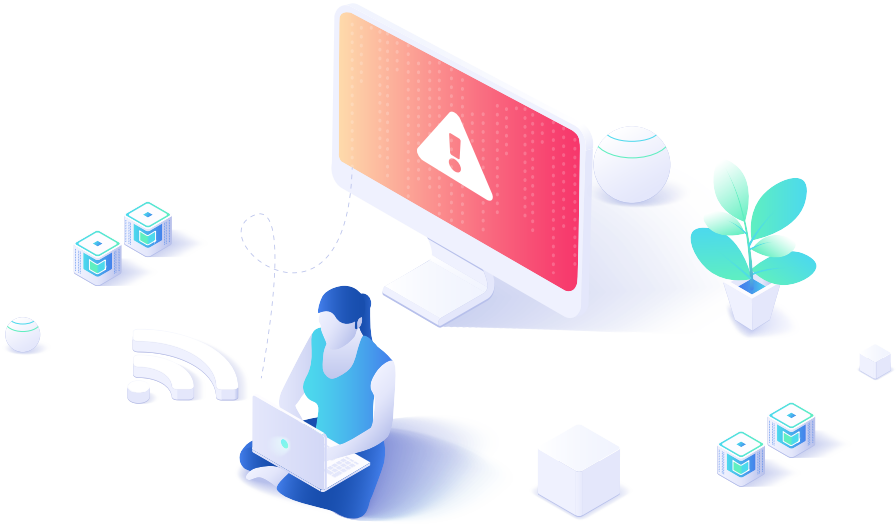
What are the common causes of downtime?

Downtime can occur for many reasons, but these are five of the most common:

1 Human error

Human error is one of the leading causes of IT downtime. In fact, it is blamed for 75% of data center outages. Many instances of human error result from a lack of knowledge of IT processes, while others occur because of disregard for best practices and correct procedures. These mistakes can be addressed through regular training and consistent updates, as well as strict documentation of key processes.

Some incidents, such as people tripping on wires or unknowingly pulling the wrong plugs, are accidental and are not completely preventable. Precautionary measures, such as tidying up wiring and limiting access to crucial hardware and applications to select personnel, can help minimize the risk and impact of these unforeseen mishaps.



2 Cybersecurity threats

Various cyberthreats can paralyze your operations in different ways. Ransomware, one of the most notorious types of malware, blocks your access to vital data or IT systems until you pay the ransom specified by the attack's perpetrators. In some cases, the attackers also erase the ransomed data or expose it to the public whether or not you pay the ransom. Reports for Q1 of 2021 reveal that a ransomware incident can cause businesses 23 days of downtime on average.

A distributed denial-of-service (DDoS) attack, on the other hand, floods your web servers with large volumes of traffic. This cyberthreat can slow down your servers, shut down your website, and prevent you from responding to your customers' requests. Some perpetrators of DDoS incidents even demand a ransom before they cease the attack. Q2 of 2019 saw a DDoS incident that lasted for three weeks, one of the longest recorded as of this writing.

Cyberthreats can also be an indirect cause of downtime. Data breaches and phishing attacks, for instance, can occur without stopping your operations. But if you belong to a regulated sector and end up falling victim to these cyberattacks, your company will most likely be the subject of investigation by industry regulators. Depending on the severity of the incident, you may have to scale down or cease your operations for the duration of the investigation.

3 Hardware failure

The failure of critical hardware, such as the servers that house your business's data, will prevent your staff from accessing important files and completing their tasks, causing your operations to grind to a halt. Such incidents usually occur because your hardware needs to be repaired or replaced.

Unfortunately, this problem may not be resolved as quickly as you need it to be. If you don't have in-house technicians, you may have to wait up to several hours for third-party service personnel to arrive and repair the broken machine. Replacement often takes much longer, as purchasing new machines and setting them up can take up to several weeks.

Taking note of your hardware's average life span is one way to remedy this issue. Servers, for instance, need to be replaced every three to five years.

4 Legacy systems

The "if it ain't broke" mentality doesn't always work to your advantage in IT. Instead of holding on to legacy systems because "they still work just fine," consider upgrading to newer and more powerful hardware and software. Newer business tools and applications often require computing power that old hardware simply cannot support or provide. What's more, these apps tend to be incompatible with older programs and operating systems (OSs). Incompatibilities result in errors, which may lead to downtime.

Using old OSs, such as Windows XP, Vista, and 7, can also make your company more vulnerable to security risks. This is because these legacy OSs no longer receive support and security updates from Microsoft, which means they are not equipped to defend against more recent cyberthreats.

5 Natural or man-made disasters

Different disasters can affect your operations in various ways, depending on their severity and the area they affect. Hurricanes, earthquakes, and floods, for instance, can damage infrastructure and result in power and internet outages. A fire or terrorist attack can damage your building and the equipment inside, including your servers. Pandemics, on the other hand, make it unsafe to leave the house and congregate in closed spaces like offices.

Most disasters are unpredictable, so you need to have precautions in place to keep resulting downtime to a minimum. These should include redundancies, such as generators, battery backups, and alternative internet connections, as well as measures that will help you quickly regain access to your data following a disaster. You must also ensure that your staff can access data and complete their tasks outside the office should the need arise.

How can MSPs help address downtime?

Mitigating the risk and effects of IT downtime, all while growing their business, can be a considerable and costly challenge for any company. Partnering with a managed IT services provider (MSP) like GRIT is the best way to overcome this challenge.

An MSP is a team of IT specialists to whom you can outsource key IT functions. These experts assume responsibility over your IT system, helping you maximize the benefits you gain from your technology investments. Different MSPs tend to offer different services, especially if they specialize in specific industries, but most of them provide cybersecurity, data backup, and network monitoring solutions.

It's impossible to completely eliminate the risk of downtime. The expertise that MSPs bring to the table, however, can help you manage the risk of downtime, shorten its duration, and keep its negative effects to a minimum. There are several ways in which MSPs accomplish these.

They monitor your network

One of an MSP's primary goals is to ensure that your network is functioning optimally at all times. They don't wait for components in your IT system to break before they act.

Instead, MSPs proactively monitor your network 24/7/365 for any issues and irregularities that can bog down its performance. Should they find an issue, the MSP resolves it as quickly as possible. For most issues, they do this remotely, so you no longer have to wait for them to arrive on site to address the problem.

If you don't have an internal IT team, working with an MSP ensures that the critical task of overseeing your network is handled by experts who are well versed in IT procedures and best practices. This cuts the risk of mistakes that trigger outages and cause downtime for your company.

They strengthen your cyber defenses

Global cybersecurity spending is projected to reach $150 billion in 2021 — and a significant portion of this comes from businesses paying MSPs for their cybersecurity services. Here's how MSPs improve your cyber defenses and lower the risk of downtime caused by cyberattacks:

- Proactive monitoring helps detect potential threats to your IT system, such as irregular traffic and hacking attempts.
- MSPs can conduct vulnerability assessments to identify weaknesses in your IT infrastructure that cybercriminals can exploit to harm your business.
- An MSP can recommend tools, applications, and measures to keep cyberthreats out of your network.
- Part of an MSP's responsibilities is ensuring that your firewalls, anti-malware software, data backups, and OSs are updated to their latest versions.
- MSPs stay abreast of cyberthreats, key processes, and cybersecurity best practices.

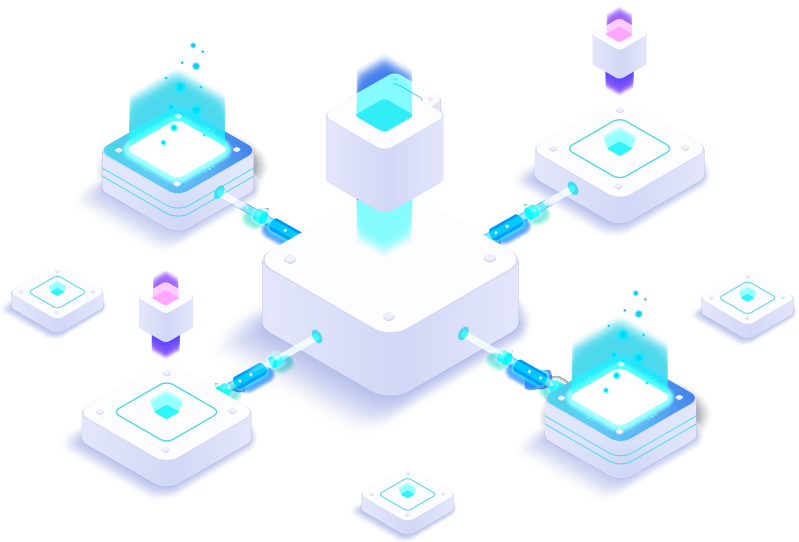
MSPs that cater to specific industries also specialize in compliance with industry regulations. For example, if your business is part of the healthcare sector, an MSP that specializes in your industry can help you comply with HIPAA's data security requirements.

They keep your systems up to date

MSPs reduce the risk of hardware failure through professional maintenance and repair services. As maintenance and fixes can be disruptive to your operations, you can arrange with your MSP for these processes to be performed when they would have the least impact on your company's day-to-day activities.

If the cost of upgrading your system prevents you from letting go of legacy systems, then your MSP might be able to help. Some MSPs can secure top-notch business solutions at lower prices, while others offer convenient services like Hardware-as-a-Service (HaaS).

HaaS allows you to rent IT equipment at an affordable cost, allowing you to acquire new and powerful machines for your business. In this arrangement, the MSP usually takes care of maintenance and future hardware upgrades, so you don't have to budget for those. You can also increase or decrease the number of machines you rent according to your business's needs.



They help with data backup and disaster recovery

On the off chance that you lose access to crucial business data following a cyberattack or natural disaster, you can avoid prolonged downtime as long as you have backups of your files. Your MSP can implement on-site backups or cloud backups — or both — depending on factors like data regulation requirements, how critical your data is to your operations, and how quickly you need to resume your operations. Additionally, data recency requirements will dictate how often your data will be backed up.

They can train your employees

When your employees are trained in IT, they are less likely to make mistakes that can result in downtime. What's more, they will know how to prevent and respond to incidents that can potentially disrupt your operations.

MSPs are usually composed of experts with years of experience in various fields of IT. If you're looking for people who can train your staff on IT-related matters, look no further than your MSP. For instance, they can help your employees identify telltale signs of cyberattacks and behaviors that compound the risk of a security breach. You can even arrange for your MSP to conduct regular training sessions designed to update your staff on evolving cyberthreats and new IT best practices.

How can GRIT help?

IT downtime can hurt your business in many ways. It can lower your revenue, compromise your data, damage your reputation, and subject you to costly penalties. And while you can't completely eliminate the possibility of downtime, you can minimize its risk and impact by partnering with an MSP.

GRIT monitors your IT system, keeping track of possible vulnerabilities and identifying opportunities to further bolster your defenses against factors that can disrupt your operations. We are dedicated to ensuring that your IT network is in the best condition to help your company grow. After all, your business's success is our success as well.

Let us help you address downtime in your organization.

CONTACT US TODAY!

Phone: **Detroit 586.286.8324/ Grand Rapids 616.251.1117**

Email: **info@grittechs.com**

GRIT TECHNOLOGIES

www.grittechs.com