TAG SOLUTIONS
We make IT work. We make IT easy. No excuses.

What is a Network Outage?

When a network outage occurs, users cannot access the resources in a network. It happens in different ways, and can impact devices and services like routers and switches, lead to partial and complete failure of hardware and software and networks shutting down completely. Time is money, and even a short network outage can be crippling to a company. Industry estimates show that average downtimes cost companies around $5,600 a minute or $300K an hour: In 2013, Amazon was down for approximately 30 minutes and it cost them an estimated 2 million dollars. Imagine how much that would be today!

Those sobering monetary statistics are only part of the consequences, though. Outages put private data at risk, and when that information is made public or used in other illegal ways, consumers, customers and your company are put at risk. After a major data breach, the bond of trust is broken and a company's reputation can be impossible to repair – and when this happens, businesses can also be targeted for lawsuits involving breach of privacy. Besides all that, an indirect cost of network outages is lost time working. And once employees get back online, it takes even more time to return their focus back to work.

IT experts predict that this problem is not going away anytime soon, and that network outages will keep getting worse until they get better. In 2021, another Amazon outage affected their delivery and fulfillment operations, Venmo, hundreds of other services, websites and apps. An earlier one the previous June affected the content delivery network Fastly. This hit The New York Times, CNN, Reddit, Bloomberg, Spotify, PayPal, Twitter and Amazon and was caused by a bad software update.

With all of these potential dangers out there, network outage best practices have to focus on both internal and external weaknesses. The most frequent kinds of threats are often preventable, so it makes sense to be proactive rather than waiting until a minor or major problem occurs. What are the most common reasons why networks go down, and how can your company prepare for them?

Why Networks Go Down

Network outages can be planned for things like updates and scheduled maintenance, and these usually do not lead to problems. Unplanned ones can be caused for a variety of reasons, including an act of nature like a hurricane that knocks out power lines. Another cause is hardware failures, which are also unpredictable. These can happen from a virus, firmware corruption, overheating, mechanical failures or when hard drives reach their storage capacity limits. Software patches and updates can also causes problems when drivers are not correct, not updated or are incompatible with the hardware.

Human error also causes service outages. Networks run 24/7/365, and many times IT professionals are called in after hours to complete updates and repairs; staff shortages can also be problematic. A staff member might configure hardware or software incorrectly – a study by the University of Michigan found that these kinds of mistakes counted for over 1/3 of network downtimes caused by routers. These errors can break down web-browsing services, internet connections and other network services.

Hacking and cyberattacks also lead to network downtime by spreading viruses and allowing unauthorized access to protected data. They are happening more often and becoming more sophisticated than ever before, and include amateur hackers sending out phishing emails, cyber espionage, ransomware attacks and complete network shutdowns.

Direct and Indirect Costs of Network Outages

Companies come in different sizes, so the losses you might experience during and after a network outage depend on a variety of factors. To determine an hourly outage cost for your business, you could multiply the number of employees you have by their average hourly wage. Another way to figure it out is to add up your labor costs per hour to the revenue lost per hour; you can take your average daily sales figure and divide it by the number of operating hours you have each day. Add onto that the costs of IT employee overtime to fix the problem or hiring more employees to recover your lost data.

Customers quickly become impatient and often angry when networks are down, and many decide to find new companies to work with. You may be able to win them back, but you will probably have to offer them pricey incentives. When you factor in the loss of revenue you may have experienced, the numbers can be shocking. And if the shutdown corrupts files and damages hard drives that are not backed up, that data could be lost forever.

Inventory disruptions caused by network outages can also be overwhelming for companies to deal with. Downtimes mean less time to sell inventory, and can create production, ordering and shipping back logs. As a result, customers may turn elsewhere and you may have large numbers of unsold inventory. Your equipment could get damaged, too – electrical surges can occur when power is restored.

IT Backup and Disaster Recovery

IT backup plans and disaster recovery plans are two different components of a company's infrastructure, and both are essential for your operations. A backup plan ensures that your critical data, applications, files and other information is all backed up and ready to restore your system if there is a catastrophic event like a cybersecurity attack or hardware failure. It is best to have several backup options – this way, the information

will be available when needed. Your system can be backed up on-site, offsite or in the cloud. Some of the highest rated servers for small business data storage include the Dell PowerEdge T30, Lenovo ThinkServer TS150 and HPE ProLiant ML350 Gen 10. Backup cloud servers are also thought to be some of the safest options available; top choices include Microsoft OneDrive, Google Drive and iDrive.

Another way to prepare for unplanned power failures is an Uninterruptible Power Supply (UPS). These provide backup battery power for IT systems that take over immediately when regular power goes offline. A redundant network connection is another option that can kick in at the onset of an outage, and these use different network carriers and providers. Office servers should also be connected to power sources with surge protectors.

An IT backup plan should be part of a comprehensive disaster recovery plan that provides an overall strategy for how your company can maintain its continuity in a network interruption or failure. Besides the backup plan, a disaster plan will focus on accountability and the steps needed to get the business up and running again. Critical team members and their responsibilities will be identified, and all the protocols that will apply. In addition to this, a well-designed disaster recovery plan includes proactive measures for preventing networks from going down in the first place.

Your final disaster recovery plan can be housed in a "runbook" or guide that contains all the steps of the process. We advise our clients to conduct regular practice scenarios with their runbooks to ensure that all team members are aware of their responsibilities and how to complete them efficiently and quickly. If this sounds like too much effort, here's something to keep in mind: Approximately 90% of companies without disaster recovery plans end up failing when facing disasters.

Other Ways to be Proactive

It also makes sense to have extra equipment in your office, like networking cables, routers, modems, servers and switches. Be sure to limit access to all of your network equipment to certain personnel, otherwise staff members who have good intentions might push the wrong switch and bring down the whole system. Also keep your equipment locked up until access is needed by authorized workers.

You can also have on-call employees who can come in to address network outages as soon as they happen, and an active service contract with your equipment manufacturer. Outages are inevitable, and when they occur you should also have a notification system in place to alert you and everyone else that needs to know. Fixing the problem sooner means less money lost and less risk.

Having a top-quality enterprise-level network infrastructure is also proactive. While it can cost your company a little more, lower-grade hardware cannot stand up as well to internal and external network threats. Better equipment is more reliable, and is less vulnerable to downtime. Also know that technology can become obsolete in the blink of an eye, and when your computers and equipment become outdated they are more vulnerable to outages and data breaches.

Being Prepared for Cyber Threats

The average downtime caused from a ransomware attack is 16 days, and during this time your information can be held hostage and be inaccessible to you and your customers. Other attacks like trojans, denial of service and spoofing analyze network infrastructures to crash networks and gain access to private information. These cyber criminals can work their ways into networks and take control, leaving you helpless as you try to figure out a solution.

To combat security attacks, keep all network devices closely monitored and updated regularly with security patches. Your malware applications and virus detection software should also be current. Network scanning tools can look for vulnerabilities in PCS, servers, network appliances, software, firewalls and routers. These can also scan your different applications for weaknesses like missing patches, bad scripts and open ports. Identifying those weak spots and correcting them before problems occur makes good business sense, no matter what industry you are in.

A zero-trust approach is another best practice IT security measure that is quickly gaining traction. With so many people working remotely these days, many use their own equipment and access company networks from different locations. The same thing applies to vendors that you may be working with. Outdated security perimeters can be useless for keeping out threats from unsecured devices and networks, especially since so many businesses have moved their operations onto the cloud. Multi-factor authentication is also vital for protecting your networks, and can be used to allow employees to log in. You'll also want to research and monitor other networks that your company interacts with as well.

More Tips For Preventing Network Outages

- Eliminating single points of failure is critical for maintaining a system's consistent uptime. You will want to have multiple external paths to cloud data; this way if one is unavailable you can use a secondary path. This kind of redundancy is key for ensuring uptime, and using virtualization is one of the best ways to do it.

- Even though computers, servers, wireless access points, network switches and other electronics can seem like they will last forever, they usually last for 36 to 72 months depending on how they are used. As they age, they perform less efficiently and have higher failure rates. Documenting when your devices were purchased and installed is important, because they should be replaced before they have a high risk of failing.
- "Fill 'er up" might be good at the gas station, but not for equipment storage capacity. For example, an almost full mechanical hard drive has to be defragmented to work properly, and defragmenting reduces a mechanical drive's overall lifespan. Initial server purchases often don't take into account the need for additional file storage or increased processing. Keep your equipment storage capacities below 100% and purchase more – the cost of storage is not as expensive as it used to be.
- Software updates and patches notifications should not be ignored, because they are designed to improve performance, fix bugs and protect against cyber threats. Procrastinating can expose your data to preventable risks. Essential updates and patches can be automated through IT tools that may be worth looking into.

What to Do When Your Network Goes Down

It is essential to respond and react quickly when your network goes down in order to minimize the damage, and these steps can all be worked into your disaster recovery plan. The first thing to do can be compared to calling 911 – alert all network end users and your IT help desk. See if the power supply has been compromised and if it has, reach out to your service providers to see if the problem is at their end.

The equipment should be logged into, and any error message can then be analyzed. These errors often direct you to the source of the problem. You may also want to contact the manufacturer, because they may be able to troubleshoot and solve the problem with you. Your ticketing system should also be updated with all the information pertaining to the outage.

IT professionals can establish estimated repair and completion times, although these can be hard to predict. With longer outages, employees might have to work remotely until the problem is solved. You will want to have built-in systems that allow people to work when your network is down – for example, cloud-based software or files that are stored locally on employee computers. Once you are given a green light to get back to work, remember to inform all of the end users. You will also want to take steps to prevent the same problem from happening in the future.

TAG Solutions and Network Outage Prevention Best Practices

Working with a managed service provider (MSP) like TAG Solutions can protect your vulnerable data and decrease the risk of network outages. Compared to having one IT person or a small IT department, TAG understands how to identify and repair problems quickly – we have an entire technical squad that is dedicated to getting to the root of your IT problem when time is of the essence.

When vetting an MSP, you will want to know about their history, reputation and security certifications. Based in Albany NY, TAG Solutions has 30 years of experience in managed IT services, cybersecurity and unified communications. Although technology has changed radically since we started in 1991, the values remain the same. Our goal is to demystify the confusion surrounding IT services and to keep company IT operations up-to-date, efficient and safe. Our long list of satisfied customers and their testimonials can be seen on our case studies page.

SOC-2 compliance is one of the most important security certifications that an IT provider can have, and TAG Solutions is proud to have it. This certification was developed by the American Institute of CPAs (AICPA), and has five main "trust service principles": security, availability, processing integrity, confidentiality and privacy. An MSP that achieves SOC-2 certification has demonstrated a commitment to ensuring business and business network safety and integrity.

Being proactive matters when it comes to minimizes network outages. An experienced MSP like TAG Solutions can tell you well in advance what security you need, when your computers need to be replaced, and when your technology will be obsolete and vulnerable to a breach and/or be unsupported by important updates. Our experts can consult with your staff, and analyze your network and equipment for weaknesses. We will collaborate with you develop a solid, unified communications plan, and backup and disaster recovery strategies to minimize the damages than downtime can cause.

https://www.tagsolutions.com/how-to-create-your-perfect-disaster-recovery-plan/

https://www.tagsolutions.com/backup-vs-disaster-recovery-plans-do-you-know-the-difference/

https://www.tagsolutions.com/5-ways-to-ensure-network-uptime/

https://www.tagsolutions.com/what-is-soc-2-compliance/

https://www.tagsolutions.com/what-can-you-do-to-prevent-an-outage/

https://brightlineit.com/5-ways-to-avoid-network-downtime-for-businesses/

https://www.comptia.org/blog/how-to-respond-to-a-network-outage

https://www.ciscopress.com/articles/article.asp?p=361409&seqNum=4

https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

https://www.emarketer.com/content/2022-predictions-internet-network-outages-will-continue-worse-before-they-better

https://www.lucidchart.com/blog/common-reasons-for-network-downtime

https://www.seattle.gov/Documents/Departments/Emergency/PlansOEM/SHIVA/SHIVAv7.0-Cyber.pdf

https://www.pcmag.com/picks/the-best-cloud-storage-and-file-sharing-services

https://www.techradar.com/news/best-small-business-servers