EXTERNETWORKS
MANAGED SERVICES AT A HIGHER LEVEL

Working in the Dark
Denying the True Cost of Network Downtime

As the price of downtime increases each year, it's more important than ever to stay connected. Does your business continuity plan have a failover option for unexpected outages?

How Often Does Downtime Occur?

Even With 99% Uptime
Businesses Will Still Experience

87+ HOURS
OF DOWNTIME
PER YEAR

Average Cost of Downtime, With High Availability

AVERAGE COST PER HOUR OF DOWNTIME

All Companies (Averages)
$163,674

Small Companies
$8,580

Large Companies
$686,250

Medium Companies
$215,637

What are the Top Causes of Network Downtime?

- Faults, errors or discards in network devices.
- Device configuration changes.
- Operational human errors and mismanagement of devices.
- Link failure caused due to fiber cable cuts or network congestion.
- Power outages.
- Server hardware failure.
- Security attacks such as denial of service (DoS).
- Failed software and firmware upgrade or patches.
- Incompatibility between firmware and hardware device.
- Unprecedented natural disasters and ad hoc mishaps on the network such as a minor accidents, or even as unrelated as a rodent chewing through a network line, etc.

How Downtime Impact Business?

Loss of Data
50 percent of employees report losing access to critical data during outages.

Risking a Security Breach
Employees often turn to unsecured devices during downtime, which could cause sensitive company data to leak.

Loss of Productivity
Downtime can result in 30 to 40 percent reduced productivity for employees.

Loss of Customer Goodwill
If the downtime occurred during peak business hours, it can substantially hurt your organization reputation.

Loss of Revenue
All of the above factors add up to substantial costs; including the revenue that your organization could have generated during the downtime.

How to Eliminate Network Downtime?

1. **Strengthen your shields**
The first level of defense is ensuring firewalls are configured properly & systems are patched with the latest security updates.

2. **Achieve full transparency of the entire incident management process**
Everyone in the IT department, but particularly those in management, should be able to determine who is working on what, the status of each incident and what next steps are needed.

3. **Automate your incident management processes**
Identify & solve any incoming incidents before they have the chance to cause serious problems to your systems, applications and/or entire network.

4. **Facilitate data analysis to develop and hone best practices**
Generate in-depth reports on incident resolution performance & mean time to repair (MTTR), which will provide valuable insight.

5. **Employ sophisticated notifications and escalations procedures**
In order for the incident management process to be executed flawlessly, the right individuals must receive notification in a timely and efficiently a manner as possible.

6. **Assign responsibility**
Ownership empowers & confers accountability. It is extremely important to designate someone in the IT organization to be responsible for the security posture of the company.

Visit www.extnoc.com to Learn More

References:

1. http://v1.aberdeen.com/launch/report/knowledge_brief/11603-KB-dedicated-network-storage.asp
2. https://www.networkworld.com/article/3142838/infrastructure/top-reasons-for-network-downtime.html
3. https://www.digitaldealer.com/prevent-network-downtime/
4. https://www.evolven.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html
5. https://www.networkcomputing.com/networking/how-avoid-network-outages-go-back-basics/257686406

EXTERNETWORKS
MANAGED SERVICES AT A HIGHER LEVEL

Global Headquarters – USA
10 Corporate Place South,
Suite 1-05, Piscataway,
NJ 08854

Toll Free: (877) 825-1575