CRITICAL STEPS TO PREVENT NETWORK DOWNTIME

MotorolaSolutions.com/Services

MOTOROLA SOLUTIONS

NETWORK OUTAGES ARE A FACT OF LIFE. NO MATTER HOW MODERN AND RESILIENT THE TECHNOLOGY, DOWNTIME WILL OCCUR.

From a 2016 survey by Center for Digital Government:

80% OF GOVERNMENT IT LEADERS EXPERIENCED AT LEAST 1 CRITICAL NETWORK OUTAGE IN THE LAST 3 MONTHS.

1/3 OF THESE EVENTS REQUIRED AT LEAST ONE DAY TO RESOLVE[1]

Additionally, cyber attacks constitute another increasing source of critical network outages. Forty-eight percent of information technology executives within critical-infrastructure organizations believe that a cyber attack has the potential to result in the loss of human life[2]. Quite simply, mission-critical networks must remain available 24 hours a day, seven days a week and 365 days a year with limited or no downtime. This demanding availability requires maintaining constant, acceptable levels of capacity and coverage, as well as availability during normal maintenance and upgrades.

The key to avoiding the threat to life and major disruption of mission-critical services is to proactively prepare to address the inevitable network issues that will arise.

ANALYZING CRITICAL NETWORK EVENTS FOR THE PREVENTABLE AND UNPREDICTABLE

For public safety agencies, mission-critical networks must:

- Remain reliable without delays or issues such as poor voice quality or lack of coverage
- Be secure in order to protect sensitive transmission of data
- Support increased capacity for planned and unforeseen events, such as a natural disaster
- Allow for seamless interoperability among agencies

The first step in maintaining uptime for mission-critical networks is understanding the types of failures that can adversely impact performance:

- **Preventable failures** occur when known measures and proactive maintenance are not taken
- **Unpredictable failures** occur regardless of how well the system is maintained
- **Graceful failures** occur during a state in which the system maintains limited functionality even with the loss of multiple components. Operating efficiency or speed may decline, but basic operations are maintained

CONDUCTING A ROOT CAUSE ANALYSIS CAN PREVENT THE SAME FAILURE FROM REOCCURRING

After a failure is corrected, network operations staff should determine if the issue will impact other areas or if it has occurred multiple times. If either case exists, further investigation and analysis will reveal a root cause that can be systematically corrected to improve response and restoration time or avoid future failures.

To improve uptime, the physical and environmental aspects of a mission-critical network should be reviewed. This includes:

- Power outage risks at remote facilities
- HVAC performance
- Unlocked, unsecured remote facilities
- Damage to physical site infrastructure

Remote monitoring and restoration along with onsite maintenance provisions for these items should also be part of your overall network performance management plan.

ADOPTING A PROACTIVE AND AGILE APPROACH TO EVENT MANAGEMENT

Around-the-clock network monitoring is critical to ensuring maximum uptime and should include procedures and resources to rapidly detect, analyze and respond to critical network events. Without the proper expertise and tools for comprehensive network monitoring, your operations staff is at a deficit and may experience:

- **Lack of foresight:** Not being aware of an issue until it results in a system failure
- **Misdiagnosis:** Attempting to resolve symptoms instead of the root cause of a problem
- **Inefficient troubleshooting:** Engaging multiple teams working in an uncoordinated manner and negatively impacting problem resolution
- **Incomplete case logs:** Inability to analyze and catalog the event for future intelligence and resolution

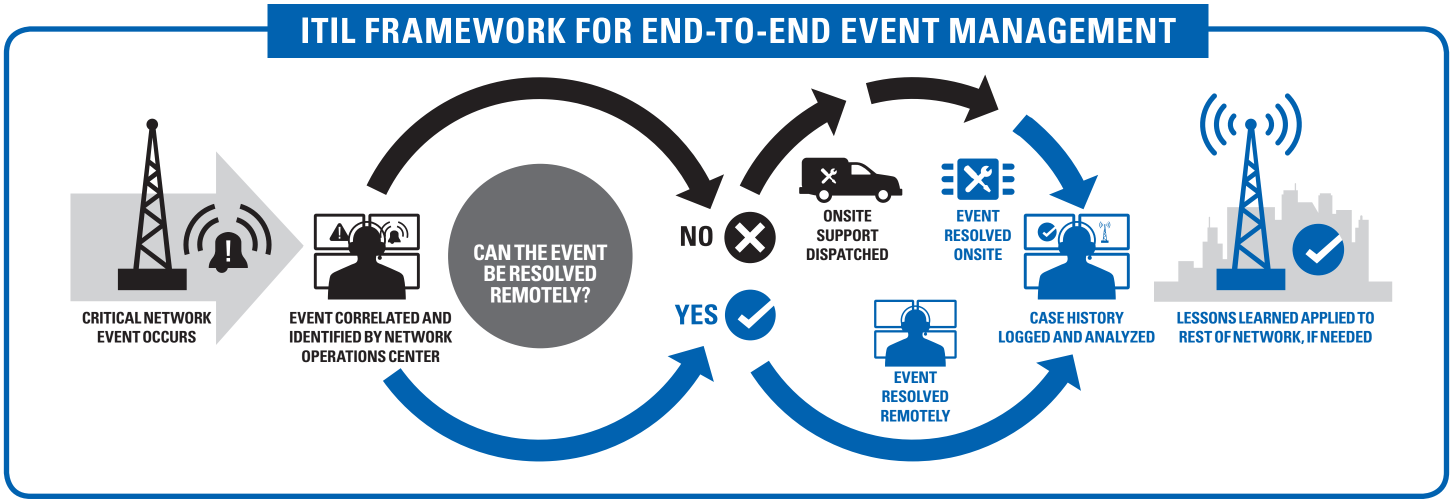
LEVERAGING ITIL FOR EVENT MANAGEMENT

Applying the Information Technology Infrastructure Library (ITIL) framework offers a proactive and agile approach to network event management. Using this discipline for critical network events enables improved outcomes to:

- Identify issues before downtime occurs
- Determine if situations can be resolved remotely by the Network Operations Center (NOC)
- Dispatch onsite support with accurate information required to resolve problems upon arrival
- Update the rules for addressing network issues
- Document procedures to ensure best practices are uniformly carried out
- Log and analyze case history to apply lessons learned
- Review steps taken to resolve previous issues and apply them if the situation reoccurs

As these steps are worked through repeatedly, the framework provides continuous learning and improves cycle time and restoration time on future outages that may occur.

ITIL FRAMEWORK FOR END-TO-END EVENT MANAGEMENT


CRITICAL NETWORK EVENT OCCURS
EVENT CORRELATED AND IDENTIFIED BY NETWORK OPERATIONS CENTER
CAN THE EVENT BE RESOLVED REMOTELY?
NO
YES
ONSITE SUPPORT DISPATCHED
EVENT RESOLVED ONSITE
EVENT RESOLVED REMOTELY
CASE HISTORY LOGGED AND ANALYZED
LESSONS LEARNED APPLIED TO REST OF NETWORK, IF NEEDED

ADDRESSING INCREASING CYBERSECURITY RISKS

As technology evolves, so have increasing security threats.

THERE WERE MORE THAN **430 MILLION** INSTANCES OF NEW MALWARE RELEASED IN 2015, UP 36 PERCENT FROM THE YEAR BEFORE.[3]

MORE THAN **1.1 MILLION** INSTANCES A DAY[4]

IN 2015, THE NUMBER OF ZERO-DAY VULNERABILITIES DISCOVERED MORE THAN DOUBLED, INCREASING **125%** FROM 2014.[5]

Safeguarding your mission-critical network from security threats requires a comprehensive cybersecurity strategy. Vulnerabilities stem from multiple sources which are not always obvious, including:

- Insider threats through phishing emails
- Remote access from unauthorized connections
- Connections to third-party devices such as cell phones via dongles and USB sticks
- Outdated hardware and software

Improving resiliency from cyber threats requires adhering to protocols including:

- Regular security patching to address known vulnerabilities
- Active password management enforcing strong passwords that must be changed in a regular cadence
- Unique logins for each individual user
- Locking down physical ports including USB ports
- 24x7x365 security monitoring
- Hardening operating systems by removing all unnecessary applications
- Conducting security risk assessment periodically to understand network vulnerabilities and know how to safeguard it from and respond to intrusions

Proper documentation of cybersecurity procedures and logging of configuration changes allows the network management staff to understand the history and current state of the network. It also provides insight into the causes and steps to resolve network issues.

PREVENTING HARDWARE AND SOFTWARE OBSOLESCENCE FOR REDUCED FAILURES

Quality network configuration ensures isolated issues do not cascade into catastrophic failures. This requires maintaining and upgrading hardware and software at the cadence recommended by manufacturers. Using obsolete network components beyond their recommended lifecycle will eventually lead to unpredictable system failures and cybersecurity risks.

Mission-critical networks are complex. Network components such as routers, switches, servers and workstations reach their end of support within three to four years. Simply replacing them when they reach end-of-life is not enough. Each component has numerous configurations and software requirements that must be addressed during this process. Hardware, firmware and software should be pre-tested and certified before they are added to the network to avoid system disruption. For example, ensuring a newly replaced server has the latest software, security patches and configuration will improve network resiliency and uptime.

It is important to plan network component updates without disrupting your operations. Doing this provides needed insights into your vendor support policies and enables you to properly budget for required hardware, software licenses and support plans.

MISSION-CRITICAL NETWORKS ARE COMPLEX. NETWORK COMPONENTS SUCH AS ROUTERS, SWITCHES, SERVERS AND WORKSTATIONS REACH THEIR END OF SUPPORT WITHIN THREE TO FOUR YEARS.

PLANNING AHEAD AND PRACTICING THE INEVITABLE

A mission-critical network must be reliable every second of the day. This requires that all users are knowledgeable about the network and have an understanding of how their environment and workflow will be impacted if an outage occurs.

All end users and outside agency personnel should be trained on what to expect and how operations can be impacted by outages. Conduct regular drills to provide hands-on experience with alternative equipment and communication networks and protocols.

Establish a notification plan to communicate network and operations status to the user community, as well as to the technical staff supporting the infrastructure. Ideally, these notifications are multimodal, including texts, phone calls, work orders and emails.

IS YOUR NETWORK READY FOR THE NEXT CATASTROPHIC EVENT?

Preventing network downtime is a continuous process. Applying best practices will help you develop strategic, efficient processes that not only minimize downtime, but also optimize network performance for operational excellence.

Below is a shortlist of procedures to help you proactively prepare for an adverse network event. To ensure your network support team is able to act on these items, it is important to conduct practice drills to ensure all stakeholders are aware of necessary procedures and network communication variances in these situations.

OPERATION STANDARDS

- Document standard operating procedures (SOPs) for catastrophic events
- Understand, follow and implement established emergency management protocols
- Verify spare parts and ability to coordinate delivery
- Review at-risk sites and support options
- Check availability of additional onsite and customer services support

NETWORK MONITORING

- Tools to remotely detect and resolve critical network events (e.g. power loss, link failures)
- Tools and resources to monitor and adjust for increased network traffic and busy signals
- Resources to monitor news and weather-related coverage
- Redundant, fully operational NOC that is available for emergencies

POWER SUPPLIES

- Verify backup generators' fuel levels and functionality can be monitored remotely
- Ensure backup generator will automatically turn on in the event of a power loss
- Designate resources to physically inspect and refuel generator
- Make sure fully charged portable batteries are available

PROVISIONING OPTIONS

- Confirm existence of pre-established talkgroup for catastrophic events
- Implement approved talkgroup protocols and assignments
- Set up dynamic regrouping capabilities for interoperability and site failures

COMPREHENSIVE MANAGEMENT IS CRITICAL FOR OPERATIONAL EXCELLENCE

Ensuring your communication network performs at mission-critical levels requires a comprehensive approach to support and maintenance. You need:

- The right team of experts with domain knowledge of your system
- Tools for comprehensive network management employing industry-leading frameworks and processes
- The ability to address all incidents as quickly as possible with visibility into how the work is being done

To achieve optimum mission-critical outcomes, it is imperative to ensure technology and processes are in place to address:

- Protection against outages via resilient and redundant systems
- Well-defined response to network issues
- Communication with end users and the public about emergency procedures
- Ongoing drills and practice of emergency procedures and use of backup equipment and networks

MOTOROLA SOLUTIONS SERVICE DELIVERY APPROACH

PEOPLE

- Dedicated professionals with IP, RF, and cyber security expertise
- Deep system domain knowledge

PROCESS

- ITIL service delivery framework
- ISO9000/IEC 2000 standards
- R56 RF site standards
- NIST framework
- PMBOK integration
- Six Sigma
- Drills

TOOLS

- Real-time visibility to system performance and services
- State-of-the-art network operations center (NOC)
- Standards-based predictive and analytical tools
- Reporting

SOURCE:

1. 2016 survey by the Center for Digital Government.
2. Aspen Institute's 2015 Critical Infrastructure Readiness Report.
3. Symantec 2016 Internet Security Threat Report.
4. Symantec 2016 Internet Security Threat Report.
5. Symantec 2016 Internet Security Threat Report.

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**