OPERATIONAL INCIDENTS

Operational incidents are unplanned disruptions to the network and computing operations of a company. Depending upon the scale and severity of the incident, access to electronic files and data may be seriously impacted. This can result in a disruption of normal workflow, lost business opportunities, even a loss of data or electronic records. The priority is to restore services as quickly as possible and return to normal operation.

Operational incidents can be the result of environmental impact such as from a fire, power failure or natural disaster. They can also be caused by computer hardware failure or by a malware attack that impacts the operating system or software applications.

EXAMPLES OF OPERATIONAL INCIDENTS INCLUDE
- Network hardware failure, resulting in loss of communication and data flow outside of the organization.
- Server crash, impacting access to internal network files, storage devices, email, etc.
- A computer virus or other malware attack that renders one or more primary computers unavailable.
- Extended power failure that disrupts the supply of electricity to network and computing devices.
- Natural disaster such as a hurricane, earthquake, flood, tornado or other event that may damage or destroy computing infrastructure.

AN INCIDENT RESPONSE PLAN CAN HELP TO MINIMIZE THE IMPACT
- Design a plan that addresses the critical needs of the organization and prioritizes the order in which to restore operations.
- Ensure that a comprehensive backup and recovery plan is in place for restoring critical data files.
- Identify the team members that would be needed to return to normal operation given each type of potential threat.
- Assign specific roles and responsibilities for returning to normal operation.
- Develop a plan for communicating status updates and progress toward restoration of services.
- Develop an alternative contingency plan for events that are beyond the ability to quickly restore.

Key Points
- Can disrupt all computer operations of a company.
- May be human-related or environmental.
- Can result in data loss.
- Operational incidents can be expensive to recover from.