A quick guide to recoveries

Different response and recovery methods are needed for cyber, disaster, and operational disruptions. Below is a high-level overview of incident types and the processes and methods for cyber, disaster and operational recoveries. Does your organization have the necessary capabilities for successful recoveries?

	Cyber Recovery	Disaster Recovery	Operational Recovery
Primary goals	• Expunge attackers from network • Minimize data loss and exfiltration	• Minimize downtime and data loss • Restore normal operations	• Restore business operations • Reduce business impacts risk
Primary team	Cyber team	IT team	Business continuity team
Incident types	Cyberattack	Major IT outage	Major disruption to business operations
Primary causes	• Data breach • Ransomware • System compromise: hacking etc • Social engineering: phishing, etc • DDoS	• Natural disasters: hurricanes, floods, fires, etc • IT infrastructure failure: network etc. • Infrastructure outages: power etc • Human error • Software failures	• Third party provider outage • Supply chain disruptions • Manufacturing process failures • Externally forced shut down • Personnel evacuations
How to respond	• Contain the incident • Determine the impact • Declare an incident event • Activate the incident response plan • Notify stakeholders	• Determine the impact • Declare a disaster event • Activate the disaster recovery plan • Notify stakeholders	• Ensure human safety • Determine the impact • Declare a business continuity event • Activate the business continuity plan • Notify stakeholders
How to recover	• Contain the attack • Remove unauthorized access • Determine needed recovery method(s) • Execute recovery plan • Test recovered systems	• Determine needed recovery method(s) • Execute recovery plan • Test recovered systems • Return to normal operations	• Determine needed recovery method(s) • Execute recovery plan • Test recovered systems • Return to normal operations
Recovery methods	• Clean infected systems • Restore from backup • Failover applications to DR site • Rebuild systems and restore data • Remediate attack vector	• Restore from backup • Failover applications to DR site • Failover to a different cloud region • Rebuild systems and restore data	• Activate alternative suppliers • Activate alternate site • Utilize remote access capabilities • Adjust production plans • Re-prioritize delivery schedules

FLEXENTIAL®

Cyber Resiliency

Cyber recoveries have become increasingly common due to a large number of bad actors and multiple organizational capabilities that must be programmatically managed to avoid impactful incidents:

- Assessing and mitigating risk
- Protecting and defending assets
- Detecting events quickly
- Responding quickly to incidents
- Maintaining data and application recovery capabilities

The best-prepared organizations have implemented and continuously improve a set of known best practices that increase their cyber resiliency. Our professional services team includes experts who can support you in:

- Assessing and mitigating security risks
- Strengthening your security posture
- Maturing the adoption of your chosen security or cybersecurity framework
- Developing and managing a successful cybersecurity program
- Managing a successful disaster recovery program
- Maturing your cyber resiliency and cyber defenses
- Building and managing your incident response program

For more information on what you can do today, take a look at the 451 Research Vanguard Report: Achieve cyber resiliency with the NIST Cybersecurity Framework, and contact us to learn how we can support your cyber resiliency journey.