Recover from cyber attacks
Effectively and efficiently restore operations after an incident.

A comprehensive security recovery strategy includes

Mitigating the attack’s impact → Rebuilding compromised services and devices → Restoring operations → Analyzing and learning from the incident

Steps for advancing cybersecurity maturity

1. Incident containment
   Disconnect affected systems from the network, disable compromised accounts and stop further harm.

2. System/device restoration
   Rebuild compromised systems, reinstall software and apply security patches and updates.

3. Data recovery
   Restore data from backups or use specialized data recovery techniques to retrieve lost or encrypted files.

4. Forensic analysis
   Examine the attack’s mechanics and the exploited vulnerabilities to prevent future incidents.

5. Incident response evaluation
   Post-recovery, evaluate the process to identify areas for enhancement.

6. Utilize AI/ML
   Accelerate recovery by rapidly identifying affected systems and data and automating the restoration process from backups.

Professional services and partnerships
Cybersecurity partners offer valuable expertise and resources:
- Forensic analysis
- Breach cause identification
- Measures to avert future incidents

Cyber recovery is a team effort.

Learn more about implementing a comprehensive cybersecurity strategy.

Explore e-book →