ADDITIONAL EMERGENCY MANAGER CYBERSECURITY RESOURCES

ADDITIONAL EMERGENCY MANAGER CYBERSECURITY RESOURCES

Below you will find a variety of additional resources for emergency managers regarding preparing, responding, and recovering from a cyberattack.

- MS-ISAC Security Primer on Ransomware
- US DHS Cybersecurity and Infrastructure Security Agency (CISA) Ransomware Website
- National Governors Association Disruption Response Planning Memo
- NASCIO Cyber Disruption Planning Guide
- Emergency Services Sector Cybersecurity Initiative
  A Department of Homeland Security resource to better understand and manage cyber risks and to coordinate the sharing of cyber information and tools between subject matter experts (both inside and outside the federal government) and the Emergency Services Sector disciplines.
- Emergency Services Sector Cybersecurity Framework Implementation Guidance
- US DHS Emergency Services Sector Cybersecurity Best Practices
- Ready.gov
  Ready.gov is a national public service campaign designed to educate and empower the American people to prepare for, respond to, and mitigate emergencies, including cybersecurity.
- US DHS Cybersecurity and Infrastructure Security Agency (CISA) Cyber Resilience Review (CRR)
  The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.
  - Information Sheet - Summary of the CRR process.
  - Method Description and User Guide - Walk-through for how an organization can conduct a CRR self-assessment.
  - Self-Assessment Package - Self-assessment form and report generator.
  - Question Set with Guidance - Self-assessment question set along with accompanying guidance.
  - CRR NIST Framework Crosswalk - Cross-reference chart for how the NIST Cybersecurity Framework aligns to the CRR.
- National Cyber Incident Response Plan (NCIRP)
  The NCIRP, developed by the United States Computer Emergency Readiness Team (US-CERT), describes a national approach to dealing with cyber incidents; addresses the important role that the private sector, state and local governments, and multiple federal agencies play in responding to incidents and how the actions of all fit together for an integrated response.
- National Cybersecurity and Communications Integration Center (NCCIC)
  A 24/7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement.

For more information for individuals, businesses, government, educators, and more, visit www.in.gov/cyber.