

The background of the page features a large, semi-transparent seal of the State of Indiana. The seal is circular and contains the text "OF THE STATE OF INDIANA" at the top and "1816" at the bottom. The central part of the seal depicts a landscape with a sun rising over mountains and a river, with a star above the sun. The seal is rendered in a light blue color against a dark blue background.

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.

- [CISA Shields Up – Cyber Guidance](#)
- [MS-ISAC Security Primer on Ransomware](#)
- [US DHS Cybersecurity and Infrastructure Security Agency \(CISA\) Ransomware Website](#)
- [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.
- [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.
- National Institute of Standards and Technology (NIST)
NIST's [Computer Security Incident Handling Guide](#) assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively.
- [CISA Tabletop Exercise Packages](#)
CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios. With over 100 CTEPs available, stakeholders can easily find resources to meet their specific exercise needs.

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