Hagerty Consulting

Cybersecurity Preparedness, Response, and Recovery

WHO IS HAGERTY?

Hagerty Consulting, Inc. (Hagerty) is a full-service consulting firm that helps clients prepare for, respond to, and recover from disasters.

Since our founding in 2001, we have supported some of the nation's most impactful disaster recovery efforts, bringing expertise in crisis response, emergency preparedness strategies, and federal grants management.

By blending deep programmatic knowledge with practical, results-driven solutions, we deliver lasting impacts that strengthen resilience for those we serve.

To learn more about the innovative solutions we can provide to your business or organization, contact:

development@hagertyconsulting.com

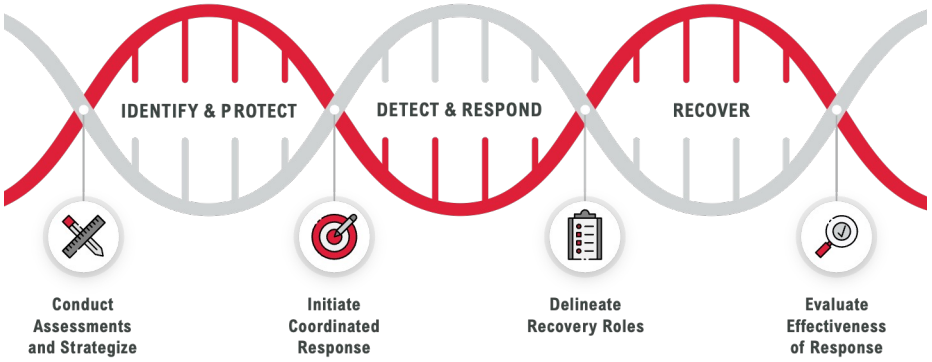
Integrating Cybersecurity and Emergency Management

Cybersecurity incidents remain one of the most persistent threats to critical infrastructure, underscoring the need for effective preparedness, response, and recovery strategies. Although no organization can eliminate every cyber threat, proactive planning, cross-functional coordination, and targeted investments can help mitigate risks and minimize disruptions.

Hagerty helps clients navigate this rapidly evolving environment with an interdisciplinary, emergency management-centered approach to cybersecurity. We empower organizations of all sizes to identify funding opportunities, launch transformative projects, and build the partnerships they need, including with local, state, and federal governments, to establish and grow a robust cybersecurity program.

The Cyber Nexus Approach

The Cyber Nexus Approach (CNA) is Hagerty's framework for building and strengthening cybersecurity programs. Leveraging existing practices and research, CNA unites emergency management and information technology (IT) stakeholders to prepare for, respond to, and recover from cyber incidents and their cascading physical impacts.



Managing complex cyber incidents requires IT and emergency management teams to work together while maintaining their distinct areas of expertise. The double helix in Hagerty's CNA represents the recurring collaboration between these teams throughout the cybersecurity program management process, from preparedness through incident response and post-incident activities.

Hagerty's Cybersecurity Capabilities

Whether enhancing cybersecurity resilience or navigating effective incident response, Hagerty delivers strategic solutions that safeguard both infrastructure and public safety. Our comprehensive suite of cybersecurity capabilities includes:

- **Partnership and Integration:** We facilitate integration between emergency management and cybersecurity teams by aligning priorities, clarifying roles, and fostering a shared understanding of operational needs to promote coordinated planning and cross-functional support.
- **Planning:** We develop operationally focused plans informed by stakeholder engagement, using proven tools and templates to ensure actionable strategies.
- **Training:** Hagerty designs and delivers cybersecurity training through web-based courses, seminars, workshops, and other tailored programs that build organizational knowledge and readiness.
- **Cyber-Kinetic Event Preparedness:** We create plans, training, and exercises that address the cascading impacts of cyberattacks on physical infrastructure.
- **Exercises:** Our Homeland Security Exercise and Evaluation Program (HSEEP)-trained professionals design and facilitate exercises ranging from discussion-based sessions to multi-day functional and full-scale exercises.
- **Programmatic Assessments:** We assess cybersecurity programs to identify gaps and improvement opportunities using federal guidance and methodologies such as the Planning, Organizing, Training, Equipping, and Exercising (POETE) model and National Institute of Standards and Technology (NIST) guidelines.
- **Continuity of Operations (COOP) and IT Disaster Recovery:** We develop continuity and IT disaster recovery plans, training, and exercises to help organizations sustain essential functions during disruptions.

HAGERTY'S CYBERSECURITY EXPERIENCE

- **Cybersecurity Strategic Planning and Grant Compliance:** Hagerty developed a Cybersecurity Strategic Plan for a state-level entity that met both State and Local Cybersecurity Grant Program (SLCGP) compliance requirements and grant funding needs. The plan was informed by extensive data collection and stakeholder engagement, bringing together existing and proposed cybersecurity projects. We also delivered a five-year implementation roadmap outlining the steps needed to carry the project forward.
- **Statewide Cyber Disruption Planning:** We helped a state IT department develop a statewide cyber disruption plan and an implementation strategy with actionable recommendations for deploying, communicating, and maintaining the plan. Hagerty also prepared cybersecurity annexes tailored to a state emergency management department and a transportation entity. Working closely with key stakeholders responsible for cyber operations, we identified threats, hazards, and response and recovery strategies. For the transportation entity, planning addressed cyber incidents that could disrupt operations. For the state emergency management department, our efforts refined operations for cyber incident preparedness, response, and recovery, enhancing statewide emergency readiness.
- **Cybersecurity Exercises and Program Improvement:** Hagerty designed, facilitated, and evaluated an executive-level cybersecurity tabletop exercise (TTX) for a transportation entity. The exercise brought senior leaders together to test strategic decision-making, crisis response, and operational resilience through a realistic scenario tailored to the entity's industry and risk landscape. On a broader scale, Hagerty also facilitated a series of iterative exercises for a state IT department to evaluate cybersecurity response capabilities and identify areas for improvement. The outcomes of these exercises informed the final phase of the project, which involved updating and enhancing the state's cyber disruption plan. Additionally, we provided a separate, long-term improvement plan to support the continued growth and development of the state's cybersecurity program.