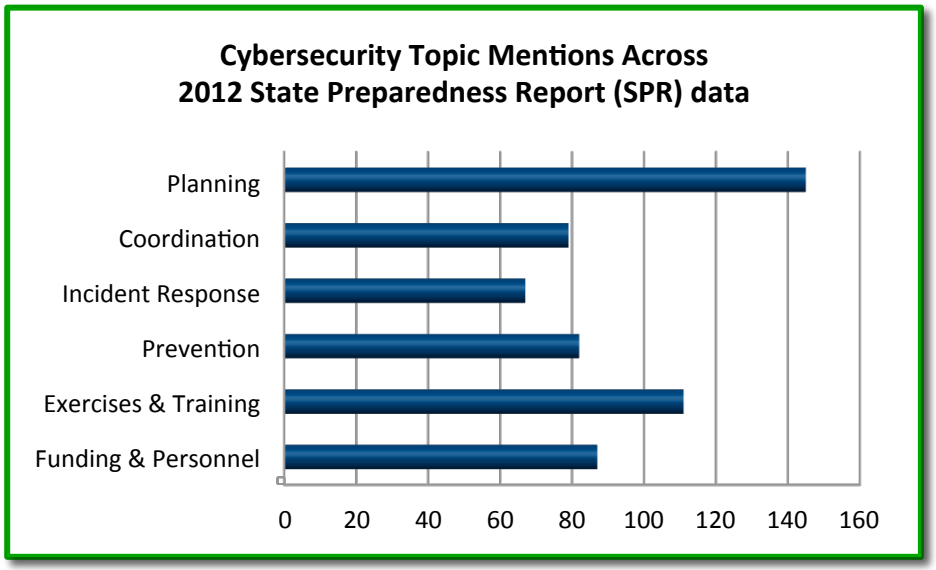
CYBERSECURITY TRENDS

Lessons Learned Information Sharing

Exploring and understanding key gaps in the cybersecurity capability of the emergency management community in order to help reduce the risk of cyber threats and enhance cybersecurity efforts.

The *Lessons Learned Information Sharing* research team conducted a trend analysis to explore and understand key gaps in the cybersecurity capability of the emergency management community and examine the challenges confronting cybersecurity efforts. To identify overall trends within cybersecurity, the research team conducted research and analysis across the 2012 State Preparedness Reports (SPRs) and 16 After Action Reports (AARs) related to cybersecurity. The goal of the analysis was to identify recurring issues to help emergency managers address challenges in cybersecurity efforts and establish a framework for further research into specific cybersecurity issues. The following are key trends identified as a result of the analysis.



KEY TREND

Planning Many states and localities lack effective plans to manage cybersecurity efforts and ensure the availability of necessary resources.

Key topics, gaps, and areas of interest within planning in cybersecurity:

- Developing a cybersecurity plan at a state or local level
- Establishing pre-defined support agreements
- Establishing or including resource acquisition plans

KEY TREND

Coordination Proper coordination to ensure all entities are working in unison to prevent and respond to cyber incidents is an integral element of cybersecurity. It is essential that entities at all levels of government work together, including working with the private sector, to overcome the broad scope and rapid spread of cyber incidents. This includes facilitating information sharing about threats and attacks and leveraging resources to reduce risk and mitigate damage.

Key topics, gaps, and areas of interest within coordination in cybersecurity:

- Handling incident coordination
- Improving information sharing & information gathering
- Forming public-private partnerships
- Enabling coordination between state and federal resources

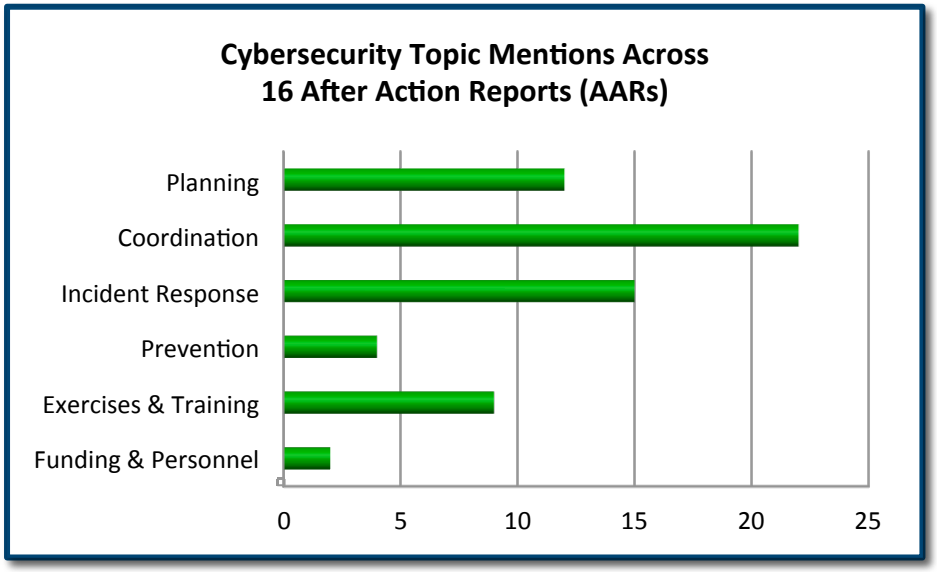
KEY TREND

Incident Response Understanding roles and responsibilities of federal and state authorities, as well as use of response tools, can help effectiveness of response efforts to cyber incidents. Issues with communication and outreach about cybersecurity threats and the impact of ongoing cyber incidents can further impede response capacity.

Key topics, gaps, and areas of interest within incident response in cybersecurity:

- Agency response tools and tactics (including, but not limited to, electronic tactical response, and response from law enforcement, firefighting, medical/ public health, and public works personnel)
- Determining the role and decision-making process of federal entities
- Determining the role and decision-making process of state entities
- Maintaining and improving communications and outreach

CYBERSECURITY TRENDS



KEY TREND

Prevention Authorities can help prevent the occurrence of cyber incidents and mitigate risks by performing assessments of system's capacity to handle incidents and by taking steps to limit potential opportunities for unauthorized access to systems.

Key topics, gaps, and areas of interest within planning in cybersecurity:

- Preventing unauthorized access to systems
- Situational awareness & threat detection
- Identifying new threats and innovations in the cyber field
- Evaluating continuity of service capability & establishing redundancies in essential systems

KEY TREND

Training & Exercises Authorities at all levels could benefit from improvements in training and exercise programs to increase awareness of cybersecurity issues, identify potential threats to systems, and evaluate the effectiveness of existing plans and response capability.

Key topics, gaps, and areas of interest within training and exercises in cybersecurity:

- Developing and executing programs to improve awareness & recognition of issues
- Creating and conducting cybersecurity exercises
- Cybersecurity training programs and educational materials

KEY TREND

Funding and Personnel Insufficient funding and personnel shortages create capability gaps by impeding employee training, the development of institutional knowledge, and response capacity.

**Although issues with funding and personnel shortages contribute to cybersecurity capability gaps, this issue was not addressed as part of the research effort due to the nature of the issue and work done by the LLIS.gov team.*

About *Addressing Core Capability Gaps*

The *LLIS.gov* team is focusing its efforts on helping communities build, sustain, and deliver the Core Capabilities assessed as being areas of both high priority and low proficiency. The goal is to gather lessons learned, innovative practices, and resources from subject matter experts at all levels of government, NGOs, and the private sector and disseminate them to the whole community.

Additional work is needed at all levels of government to address the myriad capability gaps in cybersecurity preparedness and response. Protecting critical information systems requires prioritizing cybersecurity efforts and focusing on areas for improvement.