FEMA

Sharing Information
Enhancing Preparedness
Strengthening Homeland Security

Lessons Learned Information Sharing
LLIS.gov

INNOVATIVE PRACTICE

New Hampshire's IT Leader Program: Improving Information Sharing to Enhance Cybersecurity

SUMMARY

The *Lessons Learned Information Sharing (LLIS.gov)* team identifies innovative practices within the whole community and documents these practices for emergency managers to consider when developing plans and exercises.

Established in 2003, New Hampshire's Information Technology (IT) Leader program aims to develop effective relationships between the New Hampshire Department of Information Technology (DoIT) and state agency partners to increase cybersecurity preparedness. DoIT uses the IT Leader program to raise cybersecurity awareness and collectively protect information assets by integrating cybersecurity into planning, operations, and business processes for state executive agencies. Through the IT Leader program, DoIT assists state agencies in responding to cyber incidents by improving the accuracy, speed, and effectiveness of information sharing on cyber threats, vulnerabilities, and incidents. By incorporating a similar IT Leader program into a cyber plan, emergency managers can address cyber threats and improve overall cyber preparedness.

The New Hampshire Department of Information Technology's IT Leader program helps improve collaboration and information sharing. *(Source: New Hampshire Department of Information Technology)*

DESCRIPTION

In July 2003, New Hampshire consolidated the IT services for state Executive Branch agencies into DoIT.[1] After its creation, DoIT developed the IT Leader program to establish and maintain working relationships between IT services and New Hampshire state agencies. DoIT assigns IT Leaders to serve as IT and cybersecurity liaisons between DoIT and state executive agencies.

DoIT selects business analysts, technical leads, or system developers from DoIT's Agency Software Division (ASD) or the Technical Support Services Division (TSS) to serve as IT Leaders. These IT Leaders are typically embedded within state executive agencies, and are responsible for building trusted professional partnerships with their dedicated agency. Every state executive agency partner has a designated IT Leader. Some IT Leaders are dedicated only to one agency, while others service multiple agencies. DoIT offers both a self-service and a full-service model, since each agency's needs vary based on size, funding, and requirements. These models provide varying levels of involvement from DoIT. In both models, the ASD ensures IT Leaders are familiar with their agencies' requirements and leadership.

Each designated IT Leader serves as the single point of contact to coordinate and disseminate cyber standards, advisory information, and cyber incident response communications to agency leadership and personnel. IT Leaders have a strong understanding of specific agency business requirements, as they serve as the main liaison for all IT-related efforts supporting the agency's business plan. In addition, IT Leaders work with their respective agency to fulfill a number of other responsibilities:

- Vetting, reviewing, and approving requests for data releases, remote access, and internet access;
- Reviewing and approving exceptions to cyber standards, lead application system development, and maintenance initiatives;
- Coordinating efforts and communications for cybersecurity preparedness improvement initiatives and incident response; and
- Working in partnership to develop and manage biennium budgets, procurements, and contracts.

State and agency leaders use the IT Leader program to stay engaged in cyber-related activities. Officials leverage the program's capacity to enhance communications, information sharing, and responsibility-sharing. IT Leaders serve as effective liaisons between IT personnel and state agencies, providing valuable IT services while facilitating critical information sharing.

Disseminating Cyber Threat Information to Agency Personnel

For DoIT, the IT Leader program is a key component of cyber preparedness and defending against cyber threats. The DoIT IT Security Group (ITSG) identifies threats, determines the level of risk, and posts advisory or threat notifications for IT Leaders to determine relevance and distribute within their agency, as appropriate. Given the volume of advisories and potential threats, distributing every notification would overwhelm employees. Therefore, IT Leaders serve the critical role of reviewing each notification and filtering those that may affect the agencies they support.

IT Leaders also receive situational or general cybersecurity notices from ITSG, and they are responsible for redistributing those notices within their agencies. Additionally, IT Leaders ensure the employees in their designated agencies receive relevant cyber information and updates. Using personal relationships to distribute cyber information increases the likelihood that employees will read the notifications, advisories, or updates because it is coming from a known source. IT Leaders also help implement solutions and patches. Providing in-person interpretation to agency leadership and answering questions regarding threat notifications helps to address potential issues more effectively.

Developing Effective Advisories and Notices

ITSG developed a protocol to standardize cyber advisory and notice dissemination through the IT Leaders. ITSG filters advisories and notices for risk and relevance. It then summarizes the information in plain English, includes practical examples to increase reader comprehension, and shares notices with IT Leaders for distribution to their agency business partners. This process creates products that are easier to read and resonate more with recipients.

(Source: Interview with DoIT personnel, December 5, 2013)

Sharing Agency Business Requirements and Operations to Improve Response and Expedite Recovery

In addition to helping safeguard against threats, the IT Leader program improves information sharing to help agencies better respond to and recover from cyber incidents. For example, during a potential cyber incident, IT Leaders serve as the IT point of contact for agency leadership, and they can quickly share essential information with the personnel addressing the cyber incident. IT Leaders serve as a pre-established point of contact, increasing communication speed and minimizing response times during an incident. Additionally, IT Leaders have access to system business requirements and other information for their specific agency, expediting information sharing with emergency managers during a cyber incident. Dedicated IT personnel can also identify priorities for recovery efforts and bring essential services and functions back online.

APPLICABILITY

States and localities can use the IT Leader program as a model to improve coordination and information sharing to prevent and respond to cyber incidents. Using existing personnel to serve as IT Leaders creates partnership and maximizes resources. While New Hampshire uses personnel with IT backgrounds to serve as IT Leaders, emergency managers with limited resources can identify and train any staff member within an agency to serve in this position. Employees selected for the program would need to be trained in order to understand and distribute cyber threat notices throughout their agency.

For emergency managers, the IT Leader program can help close cybersecurity capability gaps by improving the connections between emergency response and IT efforts. IT Leaders work with agency Information Security Officers to share threat and recovery data, emphasizing that cyber threats potentially affect every agency and department. By working to integrate IT Leaders into emergency preparedness and response efforts, emergency managers can more effectively mitigate cyber threats and the impact of cyber incidents.

DoIT recommends that emergency managers create a guide or checklist that describes the IT Leader program, details the responsibilities of the IT Leaders, and outlines the tasks and roles for all parties working with IT Leaders. Emergency managers can use the checklist or guide to improve the effectiveness of the program by clearly identifying the program's role in mitigating and responding to cyber threats and incidents. The IT Leader program is an example for directing and implementing the steps needed to share threat information and improve communications between agencies and IT personnel.

CITATIONS

Unless cited otherwise, information contained in this Innovative Practice document was obtained by the *LLIS.gov* research team from interviews with officials from the New Hampshire Department of Information Technology conducted between December 5, 2013 and May 21, 2014.

[1] *Public Information Technology and e-Governance: Managing the Virtual State,* G. David Garson, Jones & Bartlett, 2006.