FEMA

Sharing Information
Enhancing Preparedness
Strengthening Homeland Security

Lessons Learned
Information Sharing
LLIS.gov

DISCLAIMER *Lessons Learned Information Sharing (LLIS.gov) is the Department of Homeland Security/Federal Emergency Management Agency's national online network of lessons learned, best practices, and innovative ideas for the emergency management and homeland security communities. The Web site and its contents are provided for informational purposes only, without warranty or guarantee of any kind, and do not represent the official positions of the Department of Homeland Security. For more information on LLIS.gov, please email feedback@llis.dhs.gov or visit www.llis.gov.*

INNOVATIVE PRACTICE

Cybersecurity: Developing Secondary Teams to Increase Cyber Response Capabilities

SUMMARY

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

Rhode Island supplemented its existing Cyber Disruption Team (CDT) by creating a cybersecurity secondary team, composed of volunteers with cyber-specific skills, to assist emergency responders during incidents with cyber implications. The Rhode Island secondary team provides a valuable resource to state emergency managers and offers an example of how whole community volunteers can provide technical expertise and surge support during cyber incidents.

Rhode Island Cyber Disruption Team Seal *(Source: Interview with Doug White, March 5, 2014)*

DESCRIPTION

In June 2011, Rhode Island announced the creation of the CDT for the purpose of preventing and responding to cyber incidents and improving critical infrastructure security preparedness. The CDT was one of the first cyber teams in the Nation, and it includes members of the Rhode Island State Police Cyber Crimes Unit and individuals representing higher education, finance, hospitals, utilities, and defense. It identifies weaknesses within the state's computer infrastructure and proposes solutions to state emergency officials. While the CDT provides valuable assistance to state emergency officials, planners recognized that Rhode Island needed additional resources and expertise in the event of a cyber emergency. Therefore, the CDT developed the cybersecurity secondary team.

The cybersecurity secondary team consists of volunteers from government, military, higher education, and the private sector—all possessing cyber-specific skills. Secondary team members can provide surge support to the CDT during response efforts, and emergency managers can use the secondary team to support responders during emergencies.

Secondary Team Goals
The secondary team accomplishes two cyber preparedness goals:

1. Improving cyber response units by giving state managers access to experts and resources.
2. Improving trust and facilitation of information sharing between cyber, government, private sector, and response officials.

LLIS.gov defines Innovative Practice as successful and innovative procedures, techniques, or methods developed and/or implemented by the emergency management or response community to adapt to changing circumstances that others may wish to emulate.

Recruiting a Secondary Team

In Rhode Island, secondary team organizers used specific processes to recruit team members with essential expertise and experience. Organizers first identified the skills needed for the secondary team and the individuals or companies that could best provide those skills. Organizers then reached out to those targeted individuals and companies about joining the secondary team. In the first phase of recruitment, organizers focused on recruiting members with the primary, disaster-related skills. Secondary team organizers could then prioritize recruitment based on the four most relevant skill sets:

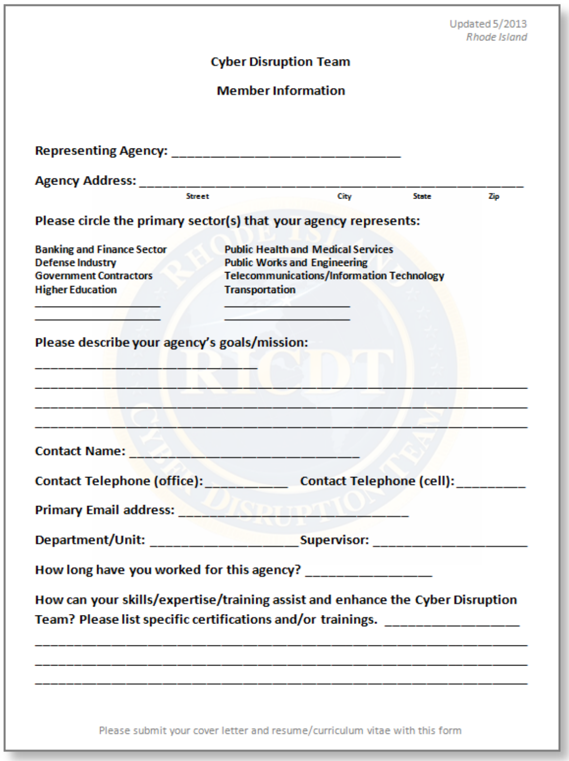
- routing and switching
- server maintenance
- penetration-testing
- cabling

After the initial recruitment, secondary team organizers began recruiting for increasingly broader skill sets. Secondary team members serve on an ad-hoc basis in response to specific incidents, limiting the required time commitment and making it easier to recruit members. While secondary team members come from all sectors, recruiting focuses on the private sector, as the private sector generally has extensive resources and some of the best-trained personnel. Additionally, to maximize the availability of useful skills, organizers do not limit membership to only recruited individuals, but also accept volunteers with relevant skills and experience.

Secondary team organizers also conduct ongoing open-ended recruitment during exercises and cyber training events hosted by the state police. These events attract attendees by providing access to experts and free training, and can build awareness of the cybersecurity secondary team's mission.

Organizing a Secondary Team

All secondary team members fill out a form that includes professional information and self-identified relevant skills. Organizers upload these forms into a database that sorts and organizes team members by skills and other factors. Due to the diverse nature of cybersecurity, organizers incorporated detailed skill descriptions into the database to maximize the usefulness of the secondary teams. Maintaining a detailed skills database ensures that, when addressing specific problems, emergency managers have access to the information needed to activate the secondary team members with the most relevant skills and training.



Updated 5/2013
Rhode Island

Cyber Disruption Team

Member Information

Representing Agency: ______________________________

Agency Address: ____
Street City State Zip

Please circle the primary sector(s) that your agency represents:

Banking and Finance Sector
Defense Industry
Government Contractors
Higher Education
____
____

Public Health and Medical Services
Public Works and Engineering
Telecommunications/Information Technology
Transportation
____
____

Please describe your agency's goals/mission:

____
____
____
____

Contact Name: ______________________________

Contact Telephone (office): ___________ **Contact Telephone (cell):** _________

Primary Email address: ______________________________

Department/Unit: ___________________ **Supervisor:** ___________________

How long have you worked for this agency? ________________

How can your skills/expertise/training assist and enhance the Cyber Disruption Team? Please list specific certifications and/or trainings. _________________
____
____
____

Please submit your cover letter and resume/curriculum vitae with this form

The Rhode Island Cyber Disruption Team developed this form to register cybersecurity secondary team members. Each member's self-identified skills and contact information feed into a database that organizers can use to activate individual team members. See the whole form in the LLIS.gov Library. (*Source: Interview with John Alfred, April 23, 2014*)

Effective organization of secondary team members also helps keep team members engaged and ready for activation. Communication tools (e.g., the Homeland Security Information Network information sharing portal, or HSIN) also help team members stay up-to-date on the most recent cyber threats and incidents.

Activating the Team

During an incident that could impact cyber systems, the Operations Director and the CDT advise the Incident Commander on what secondary team resources may be required to address the threat or incident. By using the database program, emergency managers and the CDT can identify which secondary team members are best suited to support the incident by sorting or filtering members by skill set. The Incident Commander then authorizes the CDT to activate the selected secondary team members. Secondary team organizers use tools within the database program to identify, notify, and dispatch selected team members to their duty locations.

APPLICABILITY

Cyber issues are gaining prominence in emergency management as cyber incidents frequently impact or result from all–hazards incidents. Emergency managers can use a cybersecurity secondary team as a tool to leverage whole community resources to meet these evolving challenges. By developing and implementing cybersecurity secondary teams, emergency managers can:

- Increase trust and collaboration between public and private sector partners;
- Develop and maintain a readily accessible roster of people who are available to assist in emergencies; and
- Improve the quality and accuracy of cyber exercises by incorporating specialists who can share technical expertise and experiences.

Customizing Activations to Match Resources to Needs

By extensively detailing secondary team members' skills in a database, emergency responders can activate broad or specific elements of the secondary team roster. During a 2012 exercise, a simulated solar flare threatened sensitive electronic equipment throughout the state. Responders issued a broad activation to find all available personnel who could disconnect and protect at-risk equipment. After the simulated incident, responders used the secondary team database to activate team members with the necessary skills to reconnect and restore the affected systems and equipment.

REFERENCES

Doug White, "Cybersecurity at RWU and in RI." Rhode Island Economic Development Corporation. 2011.

Doug White, Professor & Director of the Center for Forensics, Advanced Networking, and Security – Roger Williams University. Email interview, January 28, 2014. Email interview, April 5, 2014. Personal interview, December 4, 2013.

John Alfred, Corporal – Rhode Island State Police, Computer Crimes Unit. Email interview. May 9, 2014.

Laura Crimaldi. Boston Globe. "R.I. Forms Cybersecurity Partnership." July 12, 2011. http://www.boston.com/news/local/rhode_island/articles/2011/07/12/rhode_island_forms_cybersecurity_partnership/.

State of Rhode Island – Press Releases: Cyber Disruption Team, July 1, 2011. http://www.ri.gov/press/view/14202/

State of Rhode Island: Rhode Island State Police Computer Crimes Unit, Cyber Disruption Team Information. http://www.ccu.ri.gov/cyberdisruptionteam/information.php