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.*

LESSON LEARNED

Cybersecurity: The Need for Common Cybersecurity Terminology Between Information Technology and Emergency Management

SUMMARY

The *Lessons Learned Information Sharing (LLIS.gov)* team identifies lessons learned derived from real-world or exercise experiences within the whole community and documents these lessons for emergency managers to consider when developing plans and exercises.

On May 14, 2012, representatives from FEMA Region II participated in a cybersecurity Tabletop Exercise (TTX) that focused on information sharing. During the exercise, participants noted a number of misunderstandings between emergency management and information technology personnel. The key findings from the TTX included improvements in communication and collaboration that could be achieved through implementation of a common cybersecurity terminology. The private and public sectors have developed several resources that could serve as the basis for this common terminology, which are outlined in this Lesson Learned document.

FEMA organizes states and territories into ten regions. Region II chose to conduct a Tabletop Exercise in preparation for their participation in NLE 2012. *(Source: FEMA.gov photo library)*

DESCRIPTION

National Level Exercise (NLE) 2012 was part of a congressionally mandated series of national preparedness exercises designed to test and validate core capabilities.[1] NLE 2012 included four national exercises conducted between March and June 2012. These exercises examined the Nation's ability to implement the plans and capabilities necessary for effective coordinated response to and recovery from a significant national cyber event.[2] FEMA Region II (comprised of New York, New Jersey, Puerto Rico, and the U.S. Virgin Islands) conducted an exercise in May 2012 to prepare for their participation in the third NLE 2012 exercise. This discussion-based exercise examined the Region's ability to respond to a cyber event that both produced physical effects and had potential national security implications.[3]

The Region II Information Sharing and Cyber Management TTX provided regional stakeholders with an opportunity to discuss the information sharing processes in place

between emergency management and information technology personnel.[4] To facilitate the discussions, the TTX included a simulated scenario in which hackers attacked the websites of several regional transportation agencies and disrupted first responder radio communications.[5] These discussions resulted in several findings that included the need for a common terminology.[6]

The findings from this TTX indicated that significant gaps exist in information sharing between all organizations involved in a response to a cyber event, noting specifically that information technology and emergency management personnel lack a common terminology for communications during both steady state and response operations.[7] The lack of a common lexicon across these two groups led to misunderstandings during the TTX. One participant characterized the relationship between the two parties as "oil and water."[8] This lack of common terminology among TTX participants also required additional explanation of terms and concepts to ensure that all participants understood one another.[9]

RECOMMENDATIONS

After the TTX, the participants recommended that both information technology and emergency management personnel develop and utilize a common terminology across both fields. A common terminology can help reduce miscommunications and improve the relationship between the two groups. Participants also recommended that stakeholders from these two groups participate in joint training exercises.[10] These exercises would improve communications between information technology and emergency management personnel by increasing their familiarity with a common cybersecurity terminology, as well as common terms and processes used in each field.[11]

States within FEMA Region II have collaboratively and individually conducted subsequent cyber exercises to address these issues. FEMA Region II is currently developing a partnership with the Federal Bureau of Investigation (FBI) and Long Island University to offer higher education courses in cybersecurity in the Region.[12] In addition, New York and New Jersey are actively engaged with the Department of Homeland Security's National Cybersecurity and Communications Center and several public/private partnership efforts, such as the FBI's InfraGard program, to identify solutions to this issue.[13]

Available Resources

Responders from the information technology and emergency management fields can address the issue of common terminology by consulting several available resources. These resources can streamline communications processes and improve information sharing needed to prepare for, respond to, and recover from cyber incidents. The following resources may assist development of a common lexicon for all relevant organizations across multiple jurisdictions:

- The Department of Homeland Security's National Initiative for Cybersecurity Careers and Studies maintains a glossary of common cybersecurity terminology on its website, including commonly used acronyms.[14]
- In May 2013, the National Institute for Standards and Technology (NIST) revised their Glossary of Key Information Security Terms, which can also serve as a focal point for developing common terminology within the emergency management community.[15] NIST also developed a cybersecurity framework that provides a common language for managing cybersecurity risks across all sectors and setting action priorities for reducing cybersecurity risks,[16] pursuant to the requirements in a February 2013 Executive Order.[17]

- In the private sector, the MITRE Corporation is also working to develop and socialize cyber threat registries, languages, formats, and protocols to encourage collaboration and communication by expanding the use of common terminology.[18]

CITATIONS

[1] National Level Exercise (NLE) 2012; *LLIS.gov*. Accessed on February 14, 2014. https://www.llis.dhs.gov/topics/nle-2012.

[2] Ibid.

[3] Federal Emergency Management Agency. *National Level Exercise (NLE) 2012, Region II Information Sharing and Cyber Management Tabletop Exercise (TTX), Exercise Summary*. May 22, 2012.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Devin Kerins, FEMA Region II Regional Exercise Officer. Email Interview with *LLIS.gov* Staff. February 13, 2014.

[10] Federal Emergency Management Agency. *National Level Exercise (NLE) 2012, Region II Information Sharing and Cyber Management Tabletop Exercise (TTX), Exercise Summary*. May 22, 2012.

[11] Ibid.

[12] Devin Kerins, FEMA Region II Regional Exercise Officer. Email Interview with *LLIS.gov* Staff. February 13, 2014.

[13] Ibid.

[14] "A Glossary of Common Cybersecurity Terminology"; DHS National Initiative for Cybersecurity Careers and Studies. Accessed on January 14, 2014. http://niccs.us-cert.gov/glossary.

[15] Richard Kissel (ed.). National Institute for Standards and Technology. *NISTIR 7298 Revision 2, Glossary of Key Information Security Terms*. May 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[16] National Institute for Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.0. February 12, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[17] The White House. *Executive Order 13636 – Improving Critical Infrastructure Cybersecurity*. February 13, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[18] Standards; The MITRE Corporation. Accessed January 14, 2014. https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-resources/standards.