



Emergency Management and Response Information Sharing and Analysis Center (EMR-ISAC)

INFOGRAM 2-12

January 12, 2012

***NOTE:** This INFOGRAM will be distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures. For further information, contact the Emergency Management and Response- Information Sharing and Analysis Center (EMR-ISAC) at (301) 447-1325 or by e-mail at emr-isac@fema.dhs.gov.*

Emergency Services Cybersecurity

(Sources: GAO and PC Advisor)

Last month, the [Government Accountability Office](#) (GAO) released its study regarding the cybersecurity of critical infrastructure sectors. The [GAO Highlights](#) (PDF, 1 Mb) explained that each national critical infrastructure (e.g., the Emergency Services Sector) relies on networked computers and systems, which make them susceptible to cyber-based risks.

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) recognizes that the emergency services are dependent on an assortment of assets and systems to execute mission-essential tasks. These include databases, communications equipment, control systems, navigation systems, management systems, security systems, etc. The efficacy of the aforementioned (e.g., computer aided dispatch, alarm systems, geospatial systems, radio and telecommunications services, etc.) is critical to the survivability, continuity, and response-ability of Emergency Services Sector (ESS) departments and agencies.

In this New Year, ESS entities face a broad variety of cyber risks. These risks make emergency operations vulnerable to accidental or deliberate disruption before and during responses to man-made and natural disasters. An [article](#) in [PC Advisor](#) listed the following common security exploits or threats identified by the GAO and abbreviated by the EMR-ISAC for the awareness of ESS organizations:

- Cross-site scripting—uses third-party web resources to run script within the targeted web browser or scriptable application.
- Denial-of-service (DOS)—prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
- Distributed denial-of-service—variant of DOS using numerous hosts to perform the attack.
- Logic bomb—programming code intentionally inserted into a software system causing a malicious function to occur.
- Phishing—digital form of social engineering using fake emails and websites to request information from users.
- Passive wiretapping—monitoring or recording of data being transmitted over a communications link.
- SQL injection—involves the alteration of a database search in a web-based application to obtain unauthorized access to the database.
- Trojan horse— computer program that appears to have a useful function, but has hidden and malicious functions.
- Virus— computer program that copies itself and infects a computer without the knowledge of the user.
- War diving—driving down streets with a wireless-equipped computer and antenna searching for unsecured wireless networks.
- Worm—self-replicating, self-propagating, self-contained program using network mechanisms to spread itself.
- Zero-day exploit—takes advantage of unknown security vulnerabilities.

See the following sites for helpful information to prevent or mitigate the above listed threats:

- [National Cybersecurity Awareness Campaign](#)
- [OnGuardOnline.gov](#)
- [StaySafeOnline.org](#)
- [U.S. Computer Emergency Readiness Team](#)

Arson: A Destructive Weapon

(Sources: U.S. Fire Administration, Fire Engineering, and Washington Post)

An [article](#) at [Fire Engineering.com](#) discussed that the community of Novato in California has been plagued by 50 arson fires in recent days. Although all the blazes have been quickly doused, the Novato Deputy Fire Chief said the fires could have been deadly or caused serious damage. Another [article](#) at the [WashingtonPost.com](#) reported that a man confessed to a string of New Year's Day arson attacks at a cultural center and four other sites in New York City. In this case, there were no injuries and only little damage to most sites.

According to the U.S. Fire Administration's [National Fire Incident Reporting System](#) data and the [National Fire Protection Association](#), an estimated average of over 300,000 intentional fires are reported to fire departments in the United States each year. These fires cause needless injuries to nearly 8,000 firefighters and civilians, and an estimated \$1.1 billion annually in direct property loss.

When reviewing the [National Arson Awareness Week Media Kit](#) (PDF, 2.2 Mb), the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) learned that arson destroys more than buildings. It can trigger the loss of jobs, business revenue, tax dollars, and a decrease in property values. This heinous crime is particularly devastating because “it can rob a community of its valuable assets, lives, and property.”

Additional arson facts, prevention information, and deterrence projects such as the Arson Watch Program can be seen in the [media kit](#) (PDF, 2.2 Mb) mentioned above, and also at the U.S. Fire Administration Arson [website](#).

Partnerships are Key to Disaster Preparedness

(Sources Emergency Management and National Research Council)

The administrator of the Los Angeles County Office of Emergency Management explained in an [EmergencyManagement.com article](#) “the importance of bringing everyone to the table—government, nonprofit, and community partners—when creating plans and thinking about disaster preparedness.”

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) understands emergency managers must actively engage the private sector in the nation's disaster preparedness. Therefore, the EMR-ISAC reviewed a study conducted by the [National Research Council](#), which ascertained that the implementation of the following actions helps to make public-private partnerships feasible and sustainable:

- Embrace the culture of public-private partnership.
- Promote an attitude and atmosphere of trust and cooperation.
- Establish clear and definable goals for the partnership.
- Involve a diverse group of public-private partners.
- Build the foundation for promoting and strengthening relationships.
- Execute a needs assessment of the community and participating private organizations.
- Encourage leadership to incorporate a broad, organizational view to facilitate collaboration.
- Ensure information is rapidly and reliably disseminated throughout the partnership and committees.
- Look for local solutions for potential disasters.
- Remember that cooperative, uninterrupted communication is essential.

The Federal Emergency Management Agency Public-Private Partnerships [website](#) contains partnership models, templates, and tools. More information about effectively involving local, tribal, territorial, state, federal, academic, nonprofits, faith-based, and other private partners can be found in the recently released document: "[A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action.](#)"

Infrastructure Protection in 2012

(Source: DHS)

The [Department of Homeland Security](#) (DHS) defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Energy, water, information technology, financial services, and emergency services are some examples of national critical infrastructures on which our nation depends.

Critical infrastructures are also found in states, counties, and local municipalities that rely upon an array of physical assets, functions, and systems to maintain operations and the services expected by citizens. Local elected leaders, emergency managers, chief officers of the emergency services, and other infrastructure stakeholders are aware that their communities cannot survive without the protection of their critical assets and communication/cyber systems.

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) assembled the following 2012 recommendations from multiple DHS sources for the preparedness consideration of local infrastructure stakeholders:

- Achieve public-private partnerships.
- Initiate a "whole community approach" to preparedness.
- Update emergency operations plans.
- Revise continuity of operations plans.
- Amend list of hazardous materials in the community.
- Conduct emergency exercises.
- Sponsor familiarization tours of critical sites.
- Create and disseminate packets of floor plans, contact numbers, and other relevant information.

Consult the [National Infrastructure Protection Plan](#) for additional information regarding the protection of local critical infrastructures.

DISCLAIMER OF ENDORSEMENT

The EMR-ISAC does not endorse the organizations sponsoring linked websites, and does not endorse the views they express or the products/services they offer.

FAIR USE NOTICE

This INFOGRAM may contain copyrighted material that was not specifically authorized by the copyright owner. EMR-ISAC personnel believe this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

REPORTING NOTICE

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local FBI office and also the State or Major Urban Area Fusion Center. FBI phone numbers can be found online at <http://www.fbi.gov/contact/fo/fo.htm>. Fusion Center information can be seen at <http://www.dhs.gov/contact-fusion-centers>.

For information specifically affecting the *private sector* critical infrastructure contact the National Infrastructure Coordinating Center by phone at 202-282-9201, or by email at nicc@dhs.gov.

When available, each report submitted should include the date, time, location, type of activity, number of people, equipment used for the activity, name of submitting person and organization, and a designated point of contact.