



The InfoGram

Volume 12 – Issue 50

December 20, 2012

Highlights:

[SWPC Introduces New Space Weather Bulletins](#)

[Identifying an Insider Threat](#)

[Suicide in the Fire and Emergency Services](#)

[FBI Issues Warning about Hacked Webcams](#)

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.



The U.S. Fire Administration maintains the **Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC)**.

For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: **(301) 447-1325** and/or emr-isac@fema.dhs.gov.

SWPC Introduces New Space Weather Bulletins

Space and solar weather is in a period of high activity, potentially affecting communications, navigation systems, and the power grid. The Federal Emergency Management Agency (FEMA) delivered [Critical Communications During and After a Solar Superstorm](#) (PDF, 5.95 Mb) at the 2011 [Space Weather Workshop](#). The presentation lists past events, potential effects today, and how FEMA has planned its response based on a variety of scenarios.

The Space Weather Prediction Center (SWPC) has new resources available to people and organizations with duties to strengthen and secure communication lines. SWPC's [3-Day Forecast and the more detailed Forecast Discussion](#) are published twice daily. Email subscriptions are available, and the SWPC is accepting feedback on the new experimental documents through Jan. 11, 2013.

Other available information includes a listing of videos and training in the [Education and Outreach Resources](#) (PDF, 698 Kb) document, [Space Weather Data and Products](#), [Education and Outreach](#), and [Space Weather Alerts](#) listing information on current and archived alerts.

(Source: [Space Weather Prediction Center](#))

Identifying an Insider Threat

An insider threat is defined as someone who has or had valid access to data or systems and misused that access to negatively impact the organization. Intellectual property theft and industrial espionage are common examples, and the FBI [believes the threat is on the rise](#).

While many examples show people stealing from companies and industry for personal financial gain, fire, EMS, and other [emergency services departments are still at risk](#). For example, theft or deletion of medical files, tapes from the back-up 9-1-1 log, or any personally identifiable information (PII) from employee or customer files by disgruntled employees could be disastrous for the organization.

The FBI lists warning signs such as financial need or high debt, feelings of anger or revenge towards the organization, family or personal problems, divided loyalty, substance abuse, or gambling problems. Behaviors to note are copying material without need, unexplainable affluence, interest in information or work outside the scope of their normal duties, odd work and teleworking hours.

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.

None of the signs individually should raise a red flag. Organizations that believe they are being targeted should contact law enforcement.

(Source: [FBI](#))

Suicide in the Fire and Emergency Services

The report [Suicide in the Fire and Emergency Services](#) (PDF, 952 Kb) was released recently by the National Volunteer Fire Council (NVFC), with support from the U.S. Fire Administration ([USFA](#)), the Firefighter Behavioral Health Alliance, and the HOPE Health Research Institute.

The report explores a variety of causes for firefighter mental health concerns, suicide, and depression. It also discusses what behavioral concerns and indicators (anger, lack of confidence, self-isolation, substance abuse, etc.) to look for in individuals as well as steps to take if such indicators are seen.

The report states: "While nearly 90 percent of adults have experienced at least one intense traumatic event in their lifetime, firefighters are exposed to traumatic incidences as part of their routine." These exposures lead to an increased likelihood of stress and depression.

A 46-minute [webinar video](#) shows an overview of statistical findings with informal discussion about suicide in the fire service and related things such as Critical Incident Stress Management (CISM), the "Hidden Victim," survivor guilt, and the need to change fire service organizational behavior.

(Source: [National Volunteer Fire Council](#))

FBI Issues Warning about Hacked Webcams

The Federal Bureau of Investigation (FBI) issued a warning this week for people who own webcams. Hackers are [using software to gain access to webcams](#), making it possible for them to watch the computer user remotely. The FBI is considering this a form of cyber terrorism.

Downloadable software allows hackers to turn your webcam on remotely and even turn off the light indicating it is in use. With the webcam light off, the computer user will not know the camera is on. Being so portable, laptops are used anywhere in the house, at work, at the park, or on vacation, putting the computer user's personal life, privacy, and job duties at risk of being watched.

A few ways to guard against webcam hacking is to make sure your anti-virus or anti-malware software is up to date and always running. You can also disable the webcam or unplug it if it is connected via USB. You may also put a piece of electrical tape or sticker over it, although the microphone will still work.

The FBI warns young women and children are especially at risk for this type of crime, as illustrated in [a California case in 2010](#). The warning does not only apply to personal or work computers, but for any webcam including security cameras and daycare cams. Any suspicious activity should be reported to law enforcement.

(Source: [KTRK-TV, Houston, TX](#))

Fair Use Notice:

This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes 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.

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](#).

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.