

JUNE ISSUE 15

"SAVING LIVES BY SAVING SYSTEMS"

UPCOMING EVENTS

Executive Meeting

Friday, June 20th
2130 hours
11th Floor

General Meeting

TBA

All students interested in writing or contributing to the newsletter in any way is encouraged to attend.

**Remember this is a way to become published and get your name out there!!*

This newsletter is not only seen by us here in the program, but is seen by many who have a monthly subscription, other chapters, and is on FEMA Higher Ed

MCNY's EMHS TEAMS DELTA, ECHO AND FOXTROT TRAVEL TO ISRAEL FOR TRAINING



Members of MCNY's EMHS program in Israel.

Margaret Vazquez
Public Relations

Members of MCNY's emergency management and homeland security graduate program, from teams Delta, Echo, and Foxtrot traveled to Israel to participate in Emergency, Security and Crisis Management training.

Hosted by Israel's own Israeli Military Industries Academy for Advanced

Security and Anti-Terror training, the academy offers a broad range of high level security, counter-terror and anti-crime, together with intelligence and counter-intelligence training.

These services are offered to local and foreign government agencies, as well as private institutions. Its interdisciplinary team is made up of former commanders from elite Israeli security units. They have been chosen for their experience and their ability to pass on their expertise to others.

Established in 1933 as Israel's first defense equipment manufacturer, it was incorporated in 1990 as a state owned enterprise. Today Israeli Military Industries is

recognized world-wide as a leader in the design, development and manufacturer of innovative, high performance defense and military systems.

To effectively train our teams to confront the 21st century issues and threats in emergency management and homeland security, IMI exposed us to various crisis simulation exercises and classroom training.

The training that we received further helped us understand how to respond and transform, based on the rapid assessment of new threats and hazards.

Hospital Evacuation Drill

By Karen Miller, EMHS graduate student

On May 30, 2008 Coler-Goldwater Specialty Hospital and Nursing Facility conducted an evacuation drill as part of the NYS Dept of Health city-wide drill. The scenario was a CAT-2 hurricane. The purpose of the drill was to test our ability to transport patients, and communicate with staff on the units and the staging area. Volunteer workers and LPN students were acting as patients that closely resemble the population at Coler-Goldwater. Fellow MCNY Emergency Management graduate students evaluated the exercise; Alice Moise evaluated the EOC, Susamma Seeley evaluated the Staging Area and Claude Majette evaluated the evacuating unit. Their input was invaluable. As in all drills, issues were discovered, like the need to improve communications and to train alternates to replace staff in pre-assigned roles in the Hospital Incident Command System. It was a great experience for me, and I would like to take this opportunity to thank my fellow graduates for their assistance as well as the others that volunteered their time.

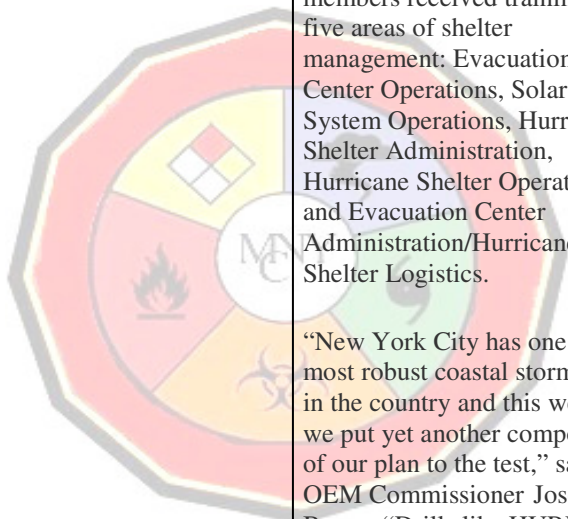
CONTENTS

| | |
|--------------------------|---|
| Upcoming Events..... | 1 |
| EMHS News | 2 |
| Good Word..... | 2 |
| IAEM Grapevine..... | 3 |
| Month in History..... | 3 |
| Academic Article..... | 3 |
| Membership..... | 5 |
| Contact Information..... | 5 |

“THE GOOD WORD”



For the past few months all current EMHS students, alumni and Faculty have been receiving emails asking if you have any news you'd like to share. Please make sure to check your email and respond with any and all good news you'd like to share. Let us share in your accomplishments and help celebrate your successes. I will be sending out the email for July's edition soon!!



NYC OFFICE OF EMERGENCY MANAGEMENT (OEM) CONDUCTS HURRICANE DRILL

Regional Hurricane Preparedness Exercise Features Deployment of Emergency Supply Stockpile and Shelter Setup

The New York City Office of Emergency Management (OEM) Commissioner announced the successful completion of HURREX 2008, a multi-agency field exercise to test the deployment of the City's emergency supply stockpile and the setup of shelters.

During the two-day exercise, held on May 31st and June 1st, 24 pallets from the City's emergency stockpile were delivered to IS 187 in Brooklyn, where more than 100 staff members from City agencies, the American Red Cross (ARC) and OEM's Community Emergency Response Teams (CERT) set up a shelter capable of providing housing and essential supplies for up to 500 people for four days. The supplies included cots, blankets, hygiene and medical kits, baby food and diapers, pet supplies and bottled water. In addition to setting up the shelter, staff members received training in five areas of shelter management: Evacuation Center Operations, Solar System Operations, Hurricane Shelter Administration, Hurricane Shelter Operations and Evacuation Center Administration/Hurricane Shelter Logistics.

“New York City has one of the most robust coastal storm plans in the country and this weekend we put yet another component of our plan to the test,” said OEM Commissioner Joseph Bruno. “Drills like HURREX help ensure the City is ready if

we ever have to face the real thing.”

In a major coastal storm, such as a category 3 or 4 hurricane, as many as 2.3 million people would need to evacuate coastal areas and up to 600,000 people would require temporary shelter. To meet those needs OEM has developed a comprehensive Coastal Storm Plan that includes detailed procedures for evacuating and sheltering residents. The City's shelter system consists of 65 evacuation centers and up to 509 hurricane shelters, including eight special medical needs shelters. To supply and staff the shelter system, OEM maintains an emergency stockpile of essential supplies and a database of nearly 25,000 City employees who would be called upon to manage evacuation centers and emergency shelters.

City officials will evaluate the exercise and study the response and decisions made by the participants for future training in New York City and in other jurisdictions. HURREX was funded by SEMO and a contribution from American International Group, Inc. (AIG).

“As an insurance company with a clear understanding of the importance of emergency preparedness and risk mitigation, AIG is proud to support the New York City Office of Emergency Management's HURREX coastal storm exercise,” said Ned Cloonan, AIG Vice President for International & Corporate Affairs. “We value our relationship with OEM and look forward to continuing to work with them as they test and refine New York City's preparedness plans and

emergency response protocols.”

Hurricane Season in the United States begins on June 1 and ends November 30. HURREX took place on the final day of National Hurricane Preparedness Week 2008, which ran from May 25 through May 31.

HURREX 2008 is part of the City's continuing efforts to test and refine its Coastal Storm Plan. The exercise was designed specifically to test the deployment of supplies from the City's emergency stockpile and staff from the city's volunteer database, and to set up a simulated emergency shelter.

Agencies that participated in HURREX include:

- * American Red Cross in Greater NY
- * NYC Administration for Children's Services
- * NYC Community Emergency Response Teams
- * NYC Department for the Aging
- * NYC Department for Citywide Administrative Services
- * NYC Department of Education
- * NYC Department of Environmental Protection
- * NYC Department of Finance
- * NYC Department of Homeless Services
- * NYC Department of Information Technology and Telecommunications
- * NYC Department of Parks and Recreation
- * NYC Department of Housing Preservation and Development
- * NYC Fire Department
- * NYC Housing Authority
- * NYC Human Resource Administration
- * NYC Law Department
- * NYC Mayor's Office
- * NYC Office of Emergency Management
- * NYC Police Department

This Month in History...

By Margaret Vazquez
Public Relations



June 14 Beirut, Lebanon

TWA Flight 847 was hijacked by the group Hezbollah, on Friday, June 14, 1985, the aircraft with its passengers and crew endured a three-day intercontinental ordeal during which one passenger, a U.S. Navy diver, was murdered

Emergency Professionals, Have You Considered Your IT Vulnerabilities?

John Muniz
MBA, CHS-III

Vocabulary:

Digital Subscriber Line (DSL): A group of technologies providing high capacity transmission over existing copper telephone lines

Hacker: A person who gains unauthorized access to a computer network for criminal or terrorist purposes

Sniffing: Eavesdropping program that monitors information traveling over a network

Spoofing: Hacker misrepresenting him or herself by using fake e-mail addresses or masquerading as someone else; also, spoofing can also involve in the redirecting of

a web link to a different address than the one intended

Virus: A corrupted software program that attaches itself to other software programs or data files in order to be executed usually without user knowledge

War driving: Eavesdroppers drive by buildings or park outside and try to intercept wireless network traffic

Worms: Independent software programs that propagate themselves to disrupt the operations of computer networks

The events of September 11th have forever changed the psyche of the American people. No longer can we assume that we are isolated from radical groups on distant shores. Missiles are able to reach our coasts which can destroy infrastructure and more importantly human lives. Our infrastructure is vulnerable to any potential attack. One such infrastructure is our information technology systems. Emergency managers and emergency professionals must have a better understanding of what can go wrong with their IT systems that they rely upon during an emergency, hazard or even a disaster. It is important to understand what the vulnerabilities for many existing IT systems are and what needs to be done in order to provide the required protection that will ensure that our systems will continue to provide critical information during a natural

disaster, hazard, or biological and even a limited nuclear attack (dirty bomb). Our focus here will be to have a basic understanding of what types of vulnerabilities we can be exposed to the existing IT infrastructure that we have to work with during a crisis. Also, this article will provide a recommended procedure to help in conducting a vulnerability analysis.

Before the automation of files, data about individuals, organizations or government agencies were maintained and secured as paper records. These records were kept in centralized locations or dispersed in separate business units. However, with the advent of personal computers, information was stored electronically and this has created a potential for computer files to be accessed by even those outside of the organization. When large amounts of information are stored electronically this creates the potential for vulnerability for many types of threats than when this data existed in manual form. Therefore, through communication networks, information systems in different locations can be interconnected and the potential for unauthorized



Margaret Vazquez
Public Relations and editor, "Presser"

Each month in this Newsletter, we bring you some of the latest news from the International Association of Emergency Managers (IAEM). You can find more of this information at <http://iaem.com>, where you can also find information about becoming a member.

[IAEM Announces Call for Entries for the IAEM 2008 Awards Program](#) deadline for entries: Aug. 15, 2008

[IAEM Student Council Announces Expanded Opportunities in the IAEM 2008 Poster Competition](#) deadline for abstracts: Oct. 1, 2008

[Fifth Annual Homeland Security Conference](#) [details](#)

July 7-8, 2008 ~ Arlington, VA
Supported by IAEM - visit the IAEM booth!

[IAEM 56th Annual Conference & EMEX 2008 ~ "Putting a New Spin on Emergency Management" Nov. 15-20, 2008 ~ Kansas City \(Overland Park\), KS](#)

[complete details](#) | [location/hotel](#)

Emergency Professionals, Have You Considered Your IT Vulnerabilities?

Continued From Page 3

access, abuse, fraud and terrorism is not limited to a single point of entry but can occur at any access point in the network and throughout its communication links (telephone lines, cables or Digital Subscriber Line-DSL).

The vulnerabilities of IT systems

Figure 1-1 shows the most common threats against present day information technology systems. These potential threats can stem from human error, technical incompetence, organizational and environmental factors and poor management decisions. It can also stem from outside forces such as hackers, vandalism and terrorist attacks. The failure of electrical systems can impact the operation and reliability of IT systems. For example, power outages, electrical problems and poor grounding systems can impact the performance of IT systems. In addition, Hurricanes, Tornadoes and earthquakes can severely damage IT systems. What type of backups do we have in place? What different technology is easily available in order to make the necessary changes? Our modern day IT systems is based upon multitier client/server computing environment. Potential vulnerabilities exist at every layer or level of the IT platform and in the communications between the layers. For example, at

the client/user layer, the user can introduce error by writing the wrong work instruction or having unauthorized access to the workstation and eventually the network. This can result in stealing sensitive information over the network and introducing viruses and even corrupting source code. Another level or layer that is vulnerable is the communications lines. Communications lines can be exposed to tapping, sniffing, message alternation, theft and fraud. Terrorist attacks can disrupt communications lines which can basically halt computer operations over the network unless other means of communications is in place or can be implemented in a timely matter. The next layer or level is the Corporate Servers. This layer is vulnerable to hacking, viruses and worms, theft and fraud, vandalism and denial of service attacks. The last layer to be vulnerable is the Corporate Systems. This includes hardware and operating systems software including databases. This layer can be vulnerable to theft of data, copying data, alternation of data, hardware and software failure. It is important to note that the architect of a web-based application typically includes a Web client, a server, and corporate information

systems linked to databases and is therefore subjected to potential vulnerabilities and security challenges. For example, floods, fires, power failures, grounding and other electrical problems can cause disruptions at any point in the network. In addition, there are other vulnerabilities and challenges such as the internet and wireless applications. When the internet becomes part of the corporate IT infrastructure the organization is at risk and is vulnerable to activities from the outside. Hackers, terrorists and criminals can infiltrate the organization's information systems and create havoc. Computers that are constantly connected to the net via cable, modems or Digital Subscriber Lines (DSL) are exposed to hacking, vandalism, viruses, worms and theft and fraud. Having fixed internet addresses leads to easy identification and exposure. With a dial-up service, a temporary internet connection is establish and assigned for each session whereas fixed internet addresses create a fixed target for hackers, terrorists and criminals. However, the tradeoff with using a dial-up service is when downloading files it becomes a time consuming process. The use of wireless technology poses security challenges. Wireless technology such as Wireless Fidelity (WiFi) can be easily infiltrated by

outsiders armed with laptops, wireless cords, and external antennas and hacking software. Note: Hackers use these tools to detect unprotected networks and they monitor the traffic across the net in order to try and gain access to organizations. The use of spy ware, sniffers, spoofing, war driving and denial of service are some of the tools that hackers and others use.

Another area of vulnerability is the use of e-mail. E-mail can contain attachments that serve as springboards for special software to transmit valuable trade secrets such as financial data, or confidential customer information to unauthorized users. Further, computer users giving their access codes to others poses whether internal or external one of the greatest threats in IT security.

The value of security and control

In the light of potential terrorist's attacks, it is critical for businesses, organizations and the like to ensure that an adequate amount of monies is allocated to protect information systems. Investment in information systems is critical because when a computer system fails to operate or perform as required, organizations that depend on such systems experience a

Membership

For information on joining IAEM – MCNY and / or IAEM, please contact the current IAEM – MCNY Treasurer, at: treasurer@iems-mcny.org or at MCNY during class. Membership supports the groups' goals of fostering academic excellence, professional development, networking and alumni relations, camaraderie and organizational growth. It also includes social events, field trips, guest speakers, workshops, and free lunch at monthly meetings.



Requirements for the Associate Emergency Manager® Program:

The AEM program today is an entry level credential that better allows beginning professionals to engage in the certification program and begin establishing a benchmark of their professional activity. To earn the AEM, requirements now include: three references, 200 hours of training (100 each in emergency and general management), an essay, and an examination.

The Certified Emergency Manager® (CEM®) credential additionally requires experience and professional contributions.

IAEM – MCNY

c/o Metropolitan College of New York
Student Services, 12th Floor
431 Canal Street
New York, NY 10013
info@iems-mcny.org
www.iems-mcny.org

Susamma Seeley
President

William Bodt
First Vice-President

Marina Diaz
Second Vice-President

Tiffany Bailey
Secretary

Margaret Vazquez
Public Relations & Editor, Presser

Jake Neufeld
Assistant Public Relations & editor, Presser

Prof. Robert Patterson
Advisor

MCNY

Prof. David Longshore
Program Executive Director
431 Canal Street
New York, NY 10013
(212) 343-1234
dlongshore@metropolitan.edu
www.mcny.edu/emergency

IAEM

Brian Silva
President – Region XII
bsilva05@gmail.com

International Headquarters
201 Park Washington Court
Falls Church, VA 22046
(703) 538-1795
info@iaem.com
www.iaem.com

INFORMATION / VOLUNTEERS
If you would like to volunteer or have information you think should be in the newsletter please contact publicrelations@iems-mcny.org

SUBSCRIPTIONS
To subscribe to the IAEM-MCNY "Presser" please send an email with the word "SUBSCRIBE" as the subject and your name in the body to publicrelations@iems-mcny.org

What Is a Certified Emergency Manager®?

A Certified Emergency Manager® (CEM®) has the knowledge, skills and ability to effectively manage a comprehensive emergency management program.

A CEM® has a working knowledge of all the basic tenets of emergency management, including mitigation, preparedness, response and recovery.

A CEM® has experience and knowledge of interagency and community-wide participation in planning, coordination and management functions designed to improve emergency management capabilities.

Why Become a Certified Emergency Manager®?

There are many reasons why emergency managers decide to pursue certification as a Certified Emergency Manager®. Here are some of the benefits:

To receive recognition of professional competence.

To join an established network of credentialed professionals.

To take advantage of enhanced career opportunities.

To gain access to career development counseling.

To obtain formal recognition of educational activities.

Requirements for the Certified Emergency Manager® Program:

Emergency management experience: Three years by date of application. Comprehensive experience must include participation in a full-scale exercise or actual disaster. Three professional references. Including current supervisor.

Education: Any 4-year baccalaureate degree; or additional experience may be substituted to satisfy this requirement, 2 years per 30 college credits up to the 120 credits comprising most baccalaureates.

Training: 100 contact hours in emergency management training and 100 hours in general management training. Note: No more than 25% of hours can be in any one topic.

Contributions to the profession: Six separate contributions in areas such as professional membership, speaking, publishing articles, serving on volunteer boards or committees and other areas beyond the scope of the emergency management job requirements.

Comprehensive emergency management essay: Real-life scenarios are provided, and response must demonstrate knowledge, skills and abilities as listed in the essay instructions.

Multiple-choice examination: Candidates sit for the 100 question exam after their initial application and the other requirements are satisfied.

The longer that computer system is down, the more critical becomes the operability of the organization. Revenue generation will be affected and the economic impact can be detrimental to the organization. The danger is that much business and organizations are depended upon the internet and networked systems. It is important to note that organizations are more vulnerable than ever to disruption and harm. Hence, a major concern for emergency management which is in part depended upon computer systems. Security incidents have been growing at an enormous rate. For the fiscal year of 2003, the number of security incidents reported to the Computer Emergency Response Team (CERT) was approximately 160,000. According to the research firm Computer Economics, viruses and worms caused an estimated \$ 12.5 Billion in damage worldwide in 2003 (Hulme, 2004). Also, according to the 2004 joint Computer Security Institute and FBI (CSI/FBI) "Computer Crime and Security Survey" found that losses were \$ 141,496,560 among 486 companies due to security problems and cyber crimes. Therefore, companies have valuable information to protect such as tax information, financial assets, medical records, trade secrets, process systems, military information and other confidential information. Further, lack or inadequate IT security controls can lead to serious liability issues for an organization. Businesses

must not only protect their information but that of clients, employees and other business partners such as venders and suppliers.

The need for risk assessment

Before an organization commits financial resources for IT security, it must determine which assets require protection and the extent to which of these assets are vulnerable. Therefore, a risk assessment is critical in order to answer these types of questions and to help determine the most cost-effective IT controls to implement in order to protect the assets. The risk assessment is a methodological identification and measurement of threats to a system and provides the probability, or risk, that a given threat could exploit the vulnerabilities. A matrix should be developed in order to help determine the value of information assets, the number of potential vulnerabilities, the potential frequency of a problem, and the potential for damage. A check list would be helpful in order to determine which controls are presently used and which additional controls should be used to provide adequate security for the system

and reduce the risk to an acceptable level that the organization can live with. The organization or the person or group in charge of IT security would perform periodic vulnerability testing of the existing controls to monitor the continued adequacy of system security. A scaling system should be used in order to help assess the potential loss which will then allow for prioritizing the specific security protection. In addition, in the process of performing a risk analysis, consideration and attention should be given to business continuity plans and disaster recovery plans. Also, in this process, it should be considered a part of the business process and should be conducted by a trained facilitator who can move the process along without having any bias. There should be subject matter experts on the team. This will guarantee the success of the analysis. A recommended procedure would be:

1. Identify assets to be considered.
2. Determine the risks, threats, and concerns.
3. Prioritize by providing a scale.
4. Implement corrective controls and agree to accept the potential risks.
5. Monitor the effectiveness of the controls that has been implemented.
6. Make the necessary changes as required as technology changes, the level of threat changes or the introduction of new threats that were not considered earlier.

Included with this analysis would be a cost-benefit analysis and a

risk analysis report that will record the actions, findings and recommendations and the cost that will be associated for such implementation of controls.

What type of security policy does an organization has?

It is important for organizations to have a firm security policy in place that is clear and coherent. A policy that takes into account the potential nature of the risks, the information that needs protection and the procedures and technologies that are needed to implement such security. It will also require some type of auditing component to ensure that these procedures and technologies are providing the required level of protection and are continuing to provide such protection. There should be a Chief Security Officer (CSO) in charge of a group that will provide training and educating the workforce and system users. Also, they will keep management inform of security threats and breakdowns. They will also maintain the tools chosen to secure security. The CSO is responsible for enforcing the organization's security policy.

In summary

There must exist across the board a commitment to IT security and other forms of security by each member of the organization if the investment is to pay off. Many times the weakest link is not in the technology but in the people who are not consistent in being vigilant to the potential dangers. Another area of concern is that there must be a constant communication between management and the workforce to ensure that the security measures that are put in place are working and are adequate for the potential risks. Service talks should be given on a continual basis. Also, a copy of the written IT security strategy should be given to every member of the organization. Management needs to emphasize the importance of maintaining secured IT systems. Security must become every one's business if we are to protect our IT systems and other infrastructures. The weakest link must be safe guarded and it begins with our personal computers assigned to us by the organization.

References:

Gruber, R., *Physical and Technical Security: An Introduction*, (2006)

Laudon, C. L., Laudon, J. P. *Management Information System, Managing The Digital Firm*, (2006)

White, J. W., *Terrorism and Homeland Security*, (2006)