



[ISSA](#)



[ASIS](#)



[HTCIA](#)



[InfraGard](#)

Joint Meeting of October 30, 2001 Protecting New England: A Call to Action

Anton Chuvakin, Ph.D. (anton@chuvakin.org)

Outline

- Executive Summary
 - Information on the participant organizations and their missions
 - Action items discussed at the meeting
- Action items
 - Discussion of the proposed actions
 - Web resource list for each subsection
- How to help?
 - Further actions planned by participant organizations
 - Areas of involvement targeted to various levels (etc. if you are a CEO, a CTO or a network admin, etc)

Executive summary

The Oct 30, 2001 meeting of the New England chapters of Information Systems Security Association (ISSA, <http://www.issa-ne.org>), InfraGard (<http://www.infragard.net>), American Society for Industrial Security (ASIS, <http://www.asis-boston.org/>) and High Technology Crime Investigation Association (HTCIA, <http://www.htcia-ne.org/>) was aimed at discussing recent events and determining measures that need to be taken to insure the collective readiness for any future terrorist activities. More than 180 people attended the conference, organized by New England ISSA chapter. Some brief information on participant organizations follows.

ISSA is an international organization of information security professionals providing educational forums, publications and peer interaction opportunities.

ASIS is an international organization for professionals responsible for industrial security and asset protection, including managers and directors of security.

Protecting New England: A Call to Action

HTCIA is an organization for security and law enforcement professionals designed to encourage the voluntary exchange of information about methods, processes, and techniques relating to investigations and security in advanced technologies.

InfraGard is a partnership between private industry and the U.S. government (represented by the FBI) developed to encourage the exchange of information by the government and the private sector members.

Invited speakers were US attorney for Massachusetts Mike Sullivan, Massachusetts Attorney General Tom Reilly and FBI Special Agent in Charge Charlie Prouty. They addressed current government initiatives to combat terrorism, creation of new anti-terrorism taskforces in Massachusetts and an increase in cybercrime. The speakers called for increased sharing of information between the private sector and the government and also between different sectors of the industry. SAC Prouty's speech concentrated on the ongoing investigation of September 11 events.

Following the speakers was an open discussion session. Using questions submitted by the audience, the issues of thinking like a terrorist and obtaining more information on the adversaries in order to create the accurate profiles and predict possible future actions of the terrorists were raised. Other discussion topics included selection of targets by terrorists, inventory of protected assets, profiling of terrorists and detecting terrorist intelligence gathering activities. It was suggested that enhanced information sharing would help both law enforcement and industry to mitigate risks and pursue the attackers more efficiently. Background information on some of the above issues and the ongoing projects to address them can be obtained from many of the government web sites.

Further discussion was structured around the following five areas:

- Physical security
- Cybersecurity
- Incident response
- National initiatives
- Critical infrastructure

Physical security – Discussion touched on inventorying the assets and then identifying those of high interest for terrorists, developing emergency response plans and escalation procedures. These procedures should be thoroughly tested using developed attack scenarios and updated as soon as the information of new attacks becomes available. The response plans should contain provisions for collecting and preserving evidence in a manner admissible in court. The participants also called for more attention to basic physical security measures such as frequent reviews of access controls and increase in background checks for employees. Another important aspect discussed was a need for enhanced security awareness and information sharing between all parties responsible for asset protection. The information that should be made accessible includes documented best practices, emergency response procedures and disaster notification trees. Subject matter experts who can assist with the above tasks should be identified in order to be mobilized in case of emergency.

Protecting New England: A Call to Action

Cybersecurity was given a high priority on the meeting. Similar to physical security, collecting information on protected resources is the necessary first step in any disaster recovery planning. Creating, following and sharing of the effective best practices across all industries and branches of the government is needed to increase the overall security against cyberattacks¹. The participants were made aware of several important online sources of documented best practices. In addition, having too much disaster recovery information publicly available was classified as risky, since it might provide terrorists with inside information on the organization. Utilizing the principle of “need to know” to prevent information leaks and complicate attackers agenda was suggested. The necessity of implementing and testing basic network protection measures before moving towards more advanced safeguards was frequently mentioned by the participants. Regular vulnerability assessments were recommended as another basic but effective way to boost security.

Designing programs to educate enterprise and home computer users on the infosecurity issues was also deemed a required step towards the more secure environment. On the other hand, enterprise leaders should be made aware of the nationwide and local emergency procedures and notification trees for the cyber-intrusions. It was also suggested that coordination between physical and information technology security controls should be improved to produce a more secure environment.

Several of the measures proposed in the area of **incident response** overlapped with physical and cyber security. Those included having an emergency response plan and crisis notification tree, which should be tested on a regular basis using pre-developed disaster scenarios. The plans should define communication with both business and civil authorities. If an organization chose to deploy an automated crisis response system, the procedure and the designated person to override the automation should be defined. It was also proposed to create a pool of skilled personnel on-call for consulting on incident response in case of disaster. The importance of information sharing for more effective incident response was also stressed.

Critical infrastructure² discussion focused on protection of New England resources. In the framework of “thinking like a terrorist,” several parts of infrastructure were listed as being of potential interest to terrorists. From the government side, several local and federal initiatives such as Federal Emergency Management Agency (FEMA, <http://www.fema.gov>) and Emergency Management State Offices were pointed out. The importance of collaboration between organizations on protecting critical resources was emphasized. Companies were advised to learn from the industry sectors that long understood the need for disaster planning (such as financial industry) and from the existing industry initiatives. Additionally, the need to create incentives for companies to pay more attention to security concerns, record formal procedures and measure their

¹ In this document, “cyberattack” is any attack against computer systems performed across the network such as the Internet

² As defined by the President's Commission on Critical Infrastructure Protection critical infrastructure includes telecommunications, transportation, electric power, oil and gas, banking and finance, water, emergency services, and continuity of government services.

Protecting New England: A Call to Action

efficiency was recognized. Use of the Public Relations (PR) methods was suggested to educate and inform the general public on the steps taken to protect the critical infrastructure and also to increase the level of vigilance and concern about potential threats.

National initiatives mentioned at the meeting were related to advancing the information sharing between various government agencies, local authorities, and the industry sectors. Among suggested concrete steps were the creation of a national database of investigative information accessible by all government agencies via portable devices and the need to increase awareness of information posted on the government websites. It was also proposed that we reevaluate recently passed laws such as HIPAA³ and GLB⁴ in light of the September 11 terrorist attacks.

Overall, the meeting served as an important step towards improving the collaboration for infrastructure protection between public and private sectors in New England. The participant organizations will continue to investigate the five action categories above and will provide specific details in the near future.

Action items

Lets us consider the areas in detail.

Physical security/Asset Protection

Physical security covers a wide area from procedures for mitigating bomb damage to a building to protecting smart cards against PIN extraction. Measures proposed at the meeting were mostly focused at diminishing large-scale physical attacks by a terrorist or terrorist organization. Below are the discussed issues related to physical attacks.

Assets inventory

This topic was discussed from several points of view. First, the importance of doing the assets inventory before embarking on any protection program was emphasized. It was stressed that before assets are identified any talk about the terrorists' motivations to attack them is less than substantial. Furthermore, several classes of targets were named as "high risk." Those included:

- ◆ American icons (Hollywood, Statue of Liberty, Disneyland, etc): attacking those will cause an extreme emotional distress, but relatively little long-term financial damage. Due to the last fact, the objects usually boast lesser protective measures.
- ◆ Everyday use facilities (gas, electricity, water, mail, etc): destruction or interruption of those will be noticed by all the population of the affected area. Since these facilities are parts of the defined critical infrastructure, they are supposed to be protected better.

³ The Health Insurance Portability and Accountability Act of 1996 affects security and privacy requirements for the healthcare industry.

⁴ The Financial Modernization Act of 1999 (also called the Gramm-Leach-Bliley Act) influences security and privacy requirements for the financial industry

Protecting New England: A Call to Action

- ◆ Important financial institutions: destroying those might cause large short term damage (such as in the case of World Trade Center) and create a potential for a long term damage as well, due to undermined consumer confidence and infrastructure damage.
- ◆ Any place with a large population, sporting event, etc: attacking the people at such gathering will cause an extended media attention, useful for terrorists, as well as widespread panic.
- ◆ Other infrastructure facilities: those might include airlines, other transportation, Universities, etc

Basic physical security measures

The importance of implementing basic physical security measures such as ID checks at critical facilities, was emphasized by participants. It is understood that the improvement in basic security measures should come before any advanced techniques are applied. For example, deploying biometric solutions before personnel security training or confiscating sharp objects at the airports before confirming the identity of the passenger. Additionally, it was suggested that USA must learn some basic antiterrorist techniques from other countries that have been fighting terrorism for a long time. For example, as was reported by one participant, public trashcans in airports were used for bombs by terrorists in Great Britain. They are now removed to reduce the risk of bombing. Background checks for all employees were also suggested as a step to reduce the risk of an attack by providing a reasonable level of trust in employees. Even something as simple as wearing an ID badge while at company premises might help to reduce certain risks. Recent events of September 11 have also demonstrated the importance of the off-site backups. Companies that had a hot site or other fast recovery provisions were able to return to normal business process within a day or two.

Security Awareness

All security measures will fail without the cooperation of the personnel implementing them. That certainly applies to physical security. The most often quoted example is airport security: it was reported in the media that people who operate control gates at the airports are underpaid and undertrained. That makes people the weakest link in the security chain rather than luggage scanning machinery. Every enterprise that has something to lose to terrorists should design and implement a personnel security awareness training program. As emphasized in the previous chapter, such program should at least focus on the basics: such as not letting strangers through the secured doors and alerting the proper authorities upon seeing a suspicious individual in the protected area.

Proper incident handling

When security violation occurs, the proper incident handling process should be executed. It was reported at the meeting that such a program should be designed in advance. It is well understood, that such a program should include preventing or reversing the loss and also assist in tracking the responsible party. The participants were told that the incident response plan should also include the evidence handling procedures in case law enforcement were to take over. The emergency procedures should also include the

Protecting New England: A Call to Action

documented crisis notification tree. Another critical aspect of incident response was also mentioned: all the procedures must be tested using realistic incident scenarios. Just having the procedures without the test phase will make the response actions much less effective in case of an actual disaster. It was also suggested that an organization should seek expert advice for designing the crisis response procedures and have the experts contact information available.

Information sharing

Increasing information sharing between various government agencies and the sectors of the industry was one of the main purposes of the meeting. It was said, that industry sectors with more expertise in physical security should share their documented best practices in order to create a safer environment for everybody. Creating and applying industry-wide best practice guides on various aspects of physical security will also help to reduce overall risk of doing business.

Other suggested physical security improvements

Biometric solutions such as fingerprint scanners, face and voice recognition and others were called an important future safeguard against physical attacks. These tools allow fine-grained access control to the organization resources, effective prevention of outsider access with no reliance on weaker human elements. Organizations were encouraged by meeting participants to evaluate biometric solutions in the near future. The media has reported that some airports chose to deploy the face recognition technology despite its current limitations. Another important facet of physical security is its transitive nature: employees leave the company, get transferred, promoted or demoted. Most of the above actions result in the need to change the physical access controls so that a person who used to have an access, for example, to the company server room while being a system administrator will not need such access if moved to another department. Thus the need was established to have a mechanism for keeping the access control rules current. Similar mechanism should allow the updating of the response plans in relation to changing priorities, enterprise resources and appearance of new threat factors.

Web resource list for physical security:

Center for Education and Research in Information Assurance and Security (CERIAS) link list on physical security	http://www.cerias.purdue.edu/coast/hotlist/physical/
National Security Institute (NSI) about bomb threats and physical security	http://nsi.org/Library/Terrorism/bombthreat.html
SANS on physical security	http://www.sans.org/infosecFAQ/firewall/phys_sec.htm
ASIS has some physical security resources	http://www.asisonline.org/

Protecting New England: A Call to Action

Cybersecurity

Cybersecurity was treated as an important priority at the meeting. While recent events did not involve cyber terrorism, the possibility of disastrous information warfare attacks was long predicted by the experts. It is well known that DDoS⁵ attacks in February 2000 have cost the victim companies, such as eBay, Yahoo! and others millions of dollars of damages in lost revenue and customer confidence. Many smaller companies suffer from denial of service today without that much media attention. It has been reported, that more than 4000 DDoS attacks take place every week (http://news.cnet.com/news/0-1003-200-6006924.html?tag=mn_hd).

The first step in approaching cybersecurity is that, as in the case of physical threats, the assets should be inventoried and classified by risk level. The discussion of cybersecurity issues touched upon the following issues:

Data security practices

Similar to the case of physical attacks, the basic host and network security measures should be practiced diligently. Updating the system and application software, setting up system logging and auditing, installing and maintaining firewalls and intrusion detection systems (IDS), performing risk assessments for critical systems are to become standard procedures for all organizations. People aspect of data security should not be ignored as well, since people are often the weakest link.⁶ A person explicitly responsible for information security should be assigned. In addition, the significance of periodic vulnerability scanning and penetration testing cannot be underestimated: it is the only way to keep up with system vulnerabilities and weaknesses for large-scale computing environment. Some experts recommend performing vulnerability assessments every month and more in-depth penetration testing by outside experts every quarter. In fact, the frequency depends upon the organization security requirements and available resources. It was mentioned that every deployed data security technology should have a clear metric of its efficiency. The goal is not attainable now, but it should be kept in mind. Such prevention and notification technologies should also be tested on a regular basis in a manner similar to fire drills. Another thing to remember, which was brought up at the meeting, was the need to apply basic security principles such as minimizing access rights. In this way, utilizing the “need to know” access principle can hinder information leaks that plague some companies.

Infosecurity awareness

Keeping employees aware of the infosecurity issues is even more important than for the case of physical threats, since the cyber risks are much less understood. “Nobody cares to hack my small business” was still used even a short time ago as a valid excuse not to

⁵ DDoS (distributed denial of service) attack is caused by malicious hackers by assembling a large number of machines (sometimes called “DDoS zombies”) connected to the Internet and setting them up to send lots of information packets to victim computer causing it to stop functioning for the period of the attack

⁶ Just remember that Social Engineering attack is often much more cost-effective than network probing.

Protecting New England: A Call to Action

implement network security⁷. Infosecurity awareness and education should become mandatory for all employees using information systems. In addition, people responsible for critical computing resources should complete a more rigorous infosecurity training to understand all of the security implications of their job functions. Enterprise security education should be kept up to date with technology and current best practices. One possible way to assure the adequate level of cybersecurity knowledge is periodic tests and quizzes based on current policies and procedures accepted by the management.

Educating business IT end-users and home users on the issues of cybersecurity was also considered critical. DDoS attacks can be deployed on unsuspecting home computers on broadband links to attack government and commercial targets. The problem is particularly hard since most home users do not want to know anything about security and there is no easy way to compel or motivate them.

Information sharing

Increasing information sharing between the government and businesses has a chance to significantly improve defenses against cyberattacks. Knowledge of attacks, effective countermeasures, policies and procedures to combat cybercrime will help make Internet a safer medium for both business and government users. InfraGard (<http://www.infragard.net>) was specifically created for this purpose. The ISACs (Information Sharing and Analysis Centers) were also aimed at increasing cyberintrusion information sharing between large companies. It was reported, that the financial ISAC (<http://www.fsisac.com/>) is effective in protecting the financial industry from cyber intrusions.

Creating best practice guides on various aspects of information security will also help to reduce overall risk of doing business on the Internet. CASPR (<http://www.caspr.org/>) is a project to develop the set of best practices on all areas of information security using the expertise of many CISSP-certified professionals.

Coordination should also be increased in the area of crisis response: companies should be aware of local and state regulations governing disaster management. The same applies to notification trees – disaster notification should include provisions for notifying the government and local authorities.

Other issues

Participants considered the risk of leaving too much information publicly available on the company web site. The Department of Justice reported (<http://www.epa.gov/ceppo/pubs/dojdoc.pdf>) that keeping emergency response procedures public presents a risk for the organization since terrorists might be able to amplify the damage using weaknesses discovered in the response plan.

⁷ Now that malicious hackers often use automated hacking tools that scan random hosts to be used for DDoS zombies after exploiting, this excuse does not hold anymore.

Protecting New England: A Call to Action

Another vital aspect of security is improving coordination between information and physical security controls. Revoking somebody's facilities access card is no use if a person still has full access to company computers over the network. Similarly, changing the password will not stop a former employee from erasing the database, if he can steal the hard drive from the server. In particular, ASIS (www.asisonline.org) membership combines security professionals from industrial, information and other areas of security and can serve as a medium for increasing the interaction.

The need to arm law enforcement agents with effective tools for investigating digital crime was raised by one of the participants. Currently, it appears that industry infosec professionals are more skilled in using such tools. Thus, educating law enforcement and developing easy-to-use tools becomes a priority.

Privacy seems to be a universal concern nowadays. Several new laws impose privacy requirements on industries such as healthcare and finance. They have to be taken into account when planning any new anti-terrorist measures.

Important web resource list for Cybersecurity:

Commonly Accepted Security Practices & Recommendations (CASPR) project	http://www.caspr.org
SANS Institute and SANS Top 20 Vulnerabilities	http://www.sans.org/ and http://www.sans.org/top20.html
Information Security Portal site	http://www.securityfocus.com
NIST (National Institute of Standards and Technology) Computer Security Division	http://csrc.nist.gov/
CIAC (Computer Incident Advisory Capability)	http://www.ciac.org/ciac/
CERT Coordination Center	http://www.cert.org/
NSA 60 Minute Network Security Guide	http://www.sans.org/newlook/resources/NSA_60_Min_NS_Guide.doc
I4 (International Information Integrity Institute)	https://i4online.com/

Incident response

Incidents will happen in spite of all the prevention measures deployed, but mitigating the damage and apprehending the perpetrators depends upon an effective and timely incident response program. Several important suggestions were made in the area of incident response. As a first step in such a program, it was recommended to construct scenarios for disastrous events with corresponding response plans. As mentioned in sections on physical and cybersecurity, incident response planning is essential for any organization. This plan should include the communication tree for the emergency. This tree should clearly show the people who should be notified in case of various security incidents. It

Protecting New England: A Call to Action

was suggested that notification should involve local authorities who might have their own incident response programs. Participants mentioned several of the organization that can be helpful for response planning. Those include: FEMA (Federal Emergency Management Agency, <http://www.fema.gov>), DRIE (New England Disaster Recovery Information Exchange, <http://www.drie.org/>) and other state and local organizations. It was also suggested to create a New England Advance Response program for improved disaster-related coordination in New England. Another helpful proposal was to create a pool of skilled infosec personnel on-call (volunteer basis, something like New England “National Guard” for incident response) for consulting on incident response. Again, any created plans and procedures should be frequently tested and their efficiency measured before actual disaster strikes. If your emergency response involves an automated reaction procedure, it is of crucial importance to designate a human to override an automatic emergency response system and have a documented procedure to do so. It was mentioned that automated fire response system might contain taped messages that will advise people to stay in offices if case of smoke. On the other hand, if the building were about to collapse due to, for instance, plane impact, to stay inside would not be sound advice. Thus appropriate manual overrides are required.

Immense importance was given to sharing the information related to security incidents. It was proposed that companies share documents with organizations that already have effective incident response program documentation, tools and best practices.

In case an organization decides to prosecute the parties responsible for the damage, the issue of evidence comes up. The incident response program should contain requirements for evidence collection and assurance that the evidence is admissible in court. For example, it was stated that certain kinds of video recording compression ratios produce records inadmissible in court, since what shows on the display is not “an exact copy” of what happened before the camera.

Important web resource list for incident response:

FIRST (Forum of Incident Response and Security Teams)	http://www.first.org/
FedCIRC (Federal Computer Incident Response Center)	http://www.fedcirc.gov/
Incident Response, Electronic Discovery, and Computer Forensics site	http://www.incident-response.org/
Handbook for Computer Security Incident Response Teams (CSIRTs)	http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

National initiatives

Discussion on national initiatives was related to existing US-wide regulations and proposing new ones. Information sharing with government agencies that were formed to protect critical infrastructure should be encouraged (see resource section for links to their web sites). Government agencies might benefit from the information on security incidents

Protecting New England: A Call to Action

provided by businesses while industry sectors can use some of the best practices guides developed by government (such as NIST security publications at <http://csrc.nist.gov/>).

Recently, several laws that impose security and privacy regulations upon healthcare and financial industry were passed.⁸ Participants called for reevaluation of some of the new legal requirements in light of the September 11 attacks.

Another suggestion was relevant to improved cooperation between government agencies. It was planned to create a database for federal information sharing with remote access via PDA-like device to speed up antiterrorist investigations. This database should be accessible by all branches of law enforcement.

Important web resource list for national initiatives:

GAO (General Accounting Office)	http://www.gao.gov/
CIAO (Critical Infrastructure Assurance Office)	http://www.ciao.gov/
NIPC (National Infrastructure Protection Center)	http://www.nipc.gov/
PCCIP (President's Commission on Critical Infrastructure Protection)	http://www.ciao.gov/PCCIP/
Office of Homeland Defense	http://www.whitehouse.gov/homeland/
FEMA (Federal Emergency Management Agency)	http://www.fema.gov/
HIPAA (Health Insurance Portability and Accountability Act)	http://www.hcfa.gov/hipaa/hipaahm.htm
GLB (Gramm-Leach-Bliley Act)	http://www.senate.gov/~banking/conf/

Critical infrastructure

US critical infrastructure presents a high profile target to potential terrorists. It was suggested that by “thinking like a terrorist”, one can gain valuable insights on motivations and internal processes of the attackers.

The discussion on critical infrastructure then turned to a search for the definition of critical infrastructure. As defined by the President's Commission on Critical Infrastructure Protection critical infrastructure includes telecommunications, transportation, electric power, oil and gas, banking and finance, water, emergency services, and continuity of government services.

For all action areas above, the value of collaboration and sharing was highlighted. Attacks on critical infrastructure influence the livelihood of all people, thus collaboration

⁸ HIPAA and GLB, see footnote above

Protecting New England: A Call to Action

with other companies and all branches of the government on the protection of critical resources is of paramount importance. Companies should become familiar with various local and state protection initiatives such as New England FEMA, local Emergency Management Director (EMD) offices, especially with their parts related to coverage of the IT resources. While protection of critical infrastructure might not always bring immediate business advantage, it was suggested that incentives for companies to recognize new security concerns, record formal procedures and measure their efficiency should be created.

Moreover, for protecting US critical resources, the cooperation of all population might be required. Thus the development of wide population awareness programs to increase vigilance and concern is required. The programs should utilize visual reminders to ensure constant awareness. Using Public Relations (PR) methods to educate public on infrastructure protection was suggested.

It was noted, that amateur terrorists have plenty of resources online as well. Such document as The Anarchist Cookbook (see http://directory.google.com/Top/Society/Politics/Anarchism/Issues/The_Anarchist_Cook_book/)

Important web resource list for critical infrastructure:

InfraGard	http://www.infragard.net
Department of Justice on critical infrastructure protection	http://www.usdoj.gov/criminal/cybercrime/critinfr.htm
Paper about PDD63 (Clinton's administration on critical infrastructure protection)	http://www.usdoj.gov/criminal/cybercrime/white_pr.htm
Department of Commerce on critical infrastructure protection	http://www.doc.gov/cio/oipr/CIP.html
Research project at Sandia Labs on critical resources	http://www.sandia.gov/CIS/

How to help?

NE ISSA, New England InfraGard, HTCIA and ASIS will continue their efforts in making New England better prepared for potential terrorist attacks in five action areas (*Physical security, Cybersecurity, Incident response, National initiatives and Critical infrastructure*). The participant organizations welcome any help your company or agency can offer.

To conclude, the biggest help in making New England a safer place to live would be to implement the security measures outlined in this document in your organization, educate your employees on critical resource protection, create emergency response teams and help law enforcement (when asked) to hunt down the terrorists responsible for the September 11 attacks.