INFRAGARD MEMBERS ALLIANCE

A COLLABORATION FOR INFRASTRUCTURE PROTECTION

Providing a trusted forum for exchanging knowledge, experience and information to help protect our nation's infrastructure from both physical and cyber threats

A Quarterly Newsletter **Issue #7 -- Winter 2008**

Predicting the Future: Threat/Risk Analysis (TRA) in a Dangerous World

By Scott Nelson and Alexandra Braconi

Turn on CNN, surf the Web with your BlackBerry®, catch the latest crime blog, or chat with your next-door neighbor and you will encounter news about terrorist acts, violent crimes and natural disasters that occur every day and affect you both personally and professionally. Incidents such as continued random attacks against American citizens and interests overseas, the recent bombings in London and Glasgow, the shootings at Virginia Polytechnic Institute and State University and the devastation of Hurricane Katrina are shocking examples of this increasing problem. We are a global community and cannot avoid the fact that what happens in Mumbai, India directly affects what happens in Albany, New York. (For breaking information about events occurring worldwide, go to http://www.globalincidentmap.com/home.php.)

As security professionals, we must identify threats, define the resulting risks and take substantive action to prevent or mitigate potential damage. We must try to identify when, not if, these events will occur and then ask ourselves – can we do something to protect our interests and assets? The answer is yes.

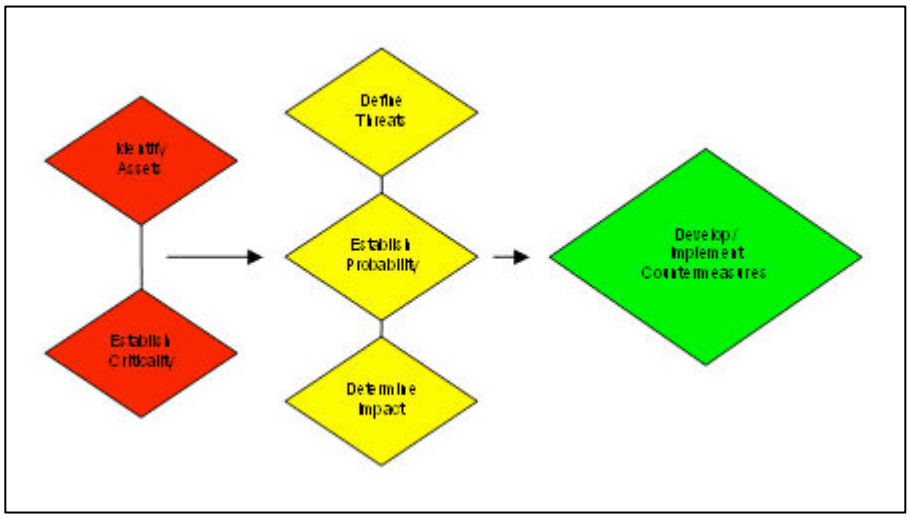
TRA – A Process Overview

TRA (often simply referred to as gap analysis) is an essential protection strategy that is equally effective for business and personal environments. The goal of TRA is to identify critical assets, define the associated threats and vulnerabilities, consider the probability of attack and develop and apply appropriate countermeasures to prevent, reduce, or mitigate potential damage. But this process – even when combined with the current profusion of public awareness, trained professionals and sophisticated planning – does not provide a simple solution. We can't protect ourselves and our assets all the time. Take a look at the events of September 11. One of the most sophisticated command centers in the world was located adjacent to the World Trade Centers, but it collapsed along with the other buildings after the attack. Moreover, effective protection against catastrophic, but unlikely, events such as weapons of mass destruction and natural disasters presents daunting challenges. It is costly, difficult and often requires mass intervention by local, state and federal agencies. These resources may be well beyond the capabilities of many families, businesses and governments.

A key aspect of any security program is an awareness of the assets that exist in a given environment, their importance to the overall function of this environment and any threats and vulnerabilities that they face. This knowledge can then be used, in conjunction with industry best practices and experience, to develop potential solutions to mitigate risk and proactively protect people, property, information and systems.

A key aspect of any security program is an awareness of the assets that exist in a given environment, their importance to the overall function of this environment and any threats and vulnerabilities that they face. This knowledge can then be used, in conjunction with industry best practices and experience, to develop potential solutions to mitigate risk and proactively protect people, property, information and systems.

(Continued on next page)



As part of the TRA process, security professionals must continuously ask themselves several important questions.

1. What are the critical assets? How are they defined and by whom? Do they include people, property, information and systems? What should be protected?
2. Are these critical assets vulnerable? How vulnerable? How accessible?
3. What is the probability and potential magnitude of attack or disruption? Would such an event adversely impact the environment as a whole or merely cause a small disruption?
4. What business issues impact the environment's security and safety? For example, what is the potential impact - perceived or actual - of workplace violence or targeted activity against infrastructure?
5. Where are the security and safety gaps? Can these gaps be plugged? If not, which should be plugged and how? Should selective mitigation be applied?
6. What countermeasures should be implemented? What is the cost/benefit analysis of action or inaction? Is doing nothing an option? Is doing too much problematic?

Identify Assets and Establish Their Criticality

The first step in the TRA process is to identify assets and establish their criticality to the overall function of the environment. What do we have that is important to our survival? This step is essential, because it is impossible to provide complete protection for everything at all times. Security professionals must consider the importance of an asset, balanced against the threats and vulnerabilities posed against it, when determining what countermeasures to apply in a given scenario to achieve the desired result.

The term asset applies not only to facilities, infrastructure and business processes, but to individuals as well. For example, if the CEO is injured or killed, will this adversely impact the operation of a company? If suppliers or vendors are harmed, will this impact a business' operations? It is also important to remember that all assets are not physical – information is a particularly valuable commodity in many industries.

Define the Risk

Once threats are identified, vulnerabilities are exposed. Demographics, business issues and crime trends all create an environment that is constantly changing. In light of this volatility, the goal of security professionals should be to define current threats and vulnerabilities, establish the probability that a given scenario will occur and determine the overall impact and consequences of an occurrence. This should be an ongoing process and include continual incident analysis to adapt to evolving risks.

Define Threats and Vulnerabilities

Threats can come from both internal and external sources. In actuality, we are most vulnerable to internal threats. While predictive analysis is often problematic, demographics and crime trend data are particularly valuable resources to use when identifying threats and vulnerabilities.

Accurate incident reporting is also key to this part of the process. The questions of what happened, when, how and why it happened must be answered and documented for future use each and every time an incident occurs.

Equally important is the issue of collateral damage. For example, you or your company may not be attacked directly, but the global impact of an event in another part of the world may affect your supply chain and your ability to conduct business in an effective, efficient and economical manner.

Probability

Determining probability is a tricky business because our perceptions of risk often clash with the actual facts. Fear may overcome reason and some people may be risk adverse while others are more accepting of negative consequences. Many individuals subscribe to the theory that we must plan for the worst and hope for the best.

Historical crime trend data provides significant indicators as to the odds of a particular criminal event taking place and under what circumstances it might occur. In addition, analysis of events such as earthquakes, hurricanes and other natural disasters can be helpful. Some industries even use complex actuarial tables to establish probability.

In addition to these resources and tools, there is an important tool at which many individuals scoff: intuition. Intuition is based on experience and emotion and can often be useful, particularly when making decisions in an emergency when time is of the essence and lives are at stake.

Impact and Consequences

It is important to evaluate the impact that an event would have in order to determine how to mitigate risk:

- Would it be a minor inconvenience or result in damage to critical assets?
- Would it result in a small financial loss to replace noncritical infrastructure or massive liability due to compromise of confidential data?

The Risk Matrix

Information gathered during this phase of the TRA process can be used to generate an overall risk score by rating six areas of potential risk on a scale of one to five. (Figure 2 provides an example of a risk matrix and the resulting score.)

Develop and Implement Countermeasures

Security professionals need to consider all of the information gathered up to this point when brainstorming possible solutions and implementing security and safety measures, policies and procedures. This part of the TRA process is both formal and informal and often based on the culture of an organization.

It is important to consider the practicality of solutions in light of technical or physical limitations, timelines and the available budget. Moreover, solutions should be holistic and include the cooperation of key stakeholders such as customers, vendors, citizens, law enforcement and emergency responders. A solid, workable communication plan is essential. Planning and testing also are critical.

Finally, consideration should be given to building on existing solutions that are already in place whenever possible rather than reinventing the wheel.

(Continued on next page)

Risk	Scale	Score
Policies, Practices, Procedures, Organizational Structure	1 – 5	5 (high risk)
Physical/IT Security	1 – 5	3 (medium risk)
Security Culture	1 – 5	3 (medium risk)
Demographics/Industry	1 – 5	4 (high risk)
Crime/Incidents	1 – 5	1 (low risk)
Law Enforcement, Fire, Medical Protection	1 – 5	1 (low risk)
TOTAL		**17 (medium risk)**

KEY
22 – 30 = high risk
11 – 21 = medium risk
0 – 10 = low risk

Figure 2. *Sample Risk Matrix*

While the prospect of providing effective security and safety is a daunting one in our increasingly dangerous global environment, a methodical TRA using recognized industry best practices is a valuable tool that allows security professionals to supply their clients and/or employers with timely, effective mitigation solutions. We cannot protect everything in a given environment at all times, but we can provide appropriate insight and countermeasure recommendations to successfully minimize risk.

TRA Concepts and Best Practices

There are several established concepts and best practices that security professionals can use while conducting a TRA.

Appreciative Inquiry focuses on what a company does well that should be emphasized and replicated. This concept identifies unique qualities and special strengths on which to build to improve security and safety performance enterprise-wide. This approach has real value because it promotes change by promoting success.

Process Consultation focuses on the evaluation and clarification of process events by an outside consultant. Events such as incident analysis, staffing, strategic planning, results, workflow, internal and external liaisons, communication channels and internal business unit relationships are included. In this role, the security professional is not necessarily the expert in solving all the problems. Instead, he or she attempts to be a problem identifier, resource gatherer and connector.

Gap Analysis involves examining the space between where a company actually is and where it ideally wants to be in the future.

The FBI Full Spectrum Analysis considers the following:

- People are a company's number one asset, as well as its number one threat and number one vulnerability. They equate to a higher probability of security challenges and concerns. Comprehensive training is vital to preventing, detecting and mitigating problems. Positive leadership also is essential, as is scrutiny of those with access to sensitive information and operating spaces.
- The proliferation and circulation of sensitive information from multiple channels is susceptible to exploitation. Promote security awareness, plug security gaps and properly store and discard information.
- The disbursal of operations and reliance on real-time access to cyber and cellular interconnections creates vulnerabilities. Implement security in all projects early on; enforce strict need-to know requirements; protect operational security at off-site and overseas locations; and integrate security compliance into all plans, policies, procedures and performance reviews.
- Screening, access and monitoring equipment are rapidly becoming obsolete and unable to counter evolving new threats. Therefore, integrating all fences, barriers, channels, sensors, monitors, alarms and human systems into a single cohesive system becomes increasingly important. Budgets should include expenses for backup equipment, supplies, maintenance, repairs, upgrades and replacement systems. Consider off-the-shelf systems to reduce research and development expenses.
- Both centralized and decentralized facilities present unique security challenges. Mitigation measures include improving 3-D security perimeters with multiple rings and layers of mutually supporting protection; denying adjacent facilities use of pathways; protecting off-site facilities with complementing security measures and providing separate visitor and package screening facilities.
- Socio-psychological threats are adversarial manipulations of public and organizational perceptions that affect community support and internal morale. Corporations should recognize the importance of security consciousness; earn and preserve public trust and confidence; understand the impact of social and psychological influences in daily operational security practices; and deter, detect and defeat internal security problems promptly and decisively.

The C.A.R.V.E.R. System (Criticality, Accessibility, Recuperability, Vulnerability, Effect on Population, Recognizability) was developed by the U.S. Army Special Forces to rate the relative desirability of potential targets and properly allocate attack resources. This process is interesting because it really looks at asset protection from the attacker's perspective.

Crime Prevention Through Environmental Design (CPTED) is a crime prevention philosophy based on the theory that proper design and effective use of the physical environment lead to reduction in fear and overall incidents of crime, as well as an improvement in the quality of life.

Low Probability, High-Consequence Events are worst-case scenarios that are unlikely, but could be deadly if they occur.

Incident and Crime Analyses provide a valuable snapshot of past events and future predictions.

Intuition and Common Sense play a big part in risk awareness and situational response.

Scott Nelson is the president of SRMG, a security company providing consulting services to infrastructure organizations. An adjunct professor of criminal justice, specializing in security management and business asset protection, at Webster University Graduate School of Business and Technology and the University of Phoenix Master of Science in Administration of Justice and Security, he is active in numerous professional organizations and previously served as a captain in the U.S. Marine Corps, a deputy assistant director in the Federal Bureau of Investigation (FBI), and global vice president of security for Warner Bros. Studios in Burbank, California and Time Warner in New York City.

Alexandra Braconi is the president of Blue Lizard Media, LLC, a company that provides corporate branding solutions; marketing/sales proposals and presentations; Web site development and maintenance services; and content development, editing, and layout design services for corporate documentation and communication. A member of the Society for Technical Communication, she has thirteen years of experience in technical writing and marketing communications. She is a member of the Society for Technical Communication (STC).

NCSD and US-CERT: Collaboration to Secure Cyberspace

— By Rob Pate

Public private partnerships like Infragard, the Electronic Crimes Task Forces (ECTFs), and the sector specific Information Sharing and Analysis Centers (ISACs) have long known that protecting cyber security depends on collaboration. These groups pioneered the way government agencies, private industry, academic institutions, and the law enforcement communities address the challenges in sharing sensitive information and proprietary processes. From the beginning, these partnerships owe their success to the skills, hard work and commitment to public service of their subject matter experts.

National Cyber Security Division

The National Cyber Security Division (NCSD) was established by the Department of Homeland Security (DHS) to serve as the federal government's cornerstone for cyber security coordination and preparedness, including implementation of the National Strategy to Secure Cyberspace. As part of this mission, the division has created trusted working partnerships with public, private, and international entities to secure cyberspace and America's cyber assets. They have also developed new resources and tools to help government and industry more efficiently combine efforts to prepare for and deter, respond to, and mitigate attacks on critical information systems.

US-Computer Emergency Readiness Team

In 2003, NCSD created the United States Computer Emergency Readiness Team (US-CERT) to protect the Nation's Internet infrastructure by coordinating defense against and response to cyber attacks. As the federal government's principal watch and warning center, US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. US-CERT stands ready, 24 hours a day, seven days a week to take reports of cyber incidents, vulnerabilities, phishing scams, or other events. US-CERT also acts as a trusted third party to assist in the responsible disclosure of vulnerabilities and coordinate the dissemination of information to key constituencies, including all levels of government and industry.

US-CERT Programs

Situational awareness is a critical factor in how we deter crime and protect information and assets. Without it, systems and networks are vulnerable for our adversaries to exploit. US-CERT sponsors several programs to foster and facilitate information sharing and collaboration on cyber security issues among government, industry, academia, and international entities.

The National Cyber Alert System

US-CERT has created the National Cyber Alert System to disseminate cyber security information and emerging cyber threat warnings. The system provides valuable cyber security information in the form of Technical Cyber Security Alerts, Cyber Security Alerts, Cyber Security Tips, and Cyber Security Bulletins. Subscription is free and is open to all who are interested at www.us-cert.gov.

The Einstein Program

US-CERT created the Einstein program as an automated process for collecting, correlating, analyzing, and sharing computer security information across federal government. By collecting and analyzing data from participating agencies, US-CERT is able to better determine the cyber activity being seen against the federal government as a whole. With this information, US-CERT is able to issue early notification of potential threats to agencies and other constituents. The program has been met with positive feedback, and in May of 2007, Federal Computer Week wrote a feature story about it. To read this article, visit http://www.fcw.com/article102730-05-21-07-Print&printLayout .

The Government Forum of Incident Response and Security Teams (GFIRST)

Shortly after the 2003 stand-up of the NCSD and US-CERT, DHS leadership recognized the need for horizontal collaboration among government cyber security professionals. The result was the creation of GFIRST, a community of over 1,000 technical and tactical practitioners from more than 50 federal, state and municipal cyber incident response teams, dedicated to securing government information technology systems across sectors and geographies.

GFIRST members work together to understand and mitigate computer security incidents, and to encourage proactive and preventative security practices within their organizations. The GFIRST community promotes cooperation among the full range of local, state and federal agencies, including defense, civilian, intelligence, and law enforcement.

US-CERT Incident Response Activities

US-CERT analysts and the law enforcement group work together to respond to cyber activity by:

- Assisting with ongoing federal law enforcement investigations
- Supporting cyber investigations with recursive analysis on artifacts
- Providing malware analytic and recovery support for government agencies
- Providing behavior techniques for dynamic and static analysis
- Providing fused, current, and predictive cyber analysis based on situational reporting
- Providing onsite incident response capabilities to federal and state agencies
- Coordinating federal programs of computer emergency response team and Chief Information Security Officer peer groups for sharing incident information, best practices, and other cyber security information
- Collaborating with domestic and international computer security incident response teams

Strengthening Participation

Broad participation is essential to improving cyber security, yet impediments to collaboration and information sharing remain. Private enterprise competes in the marketplace for clients, partners, suppliers and market share and may have less incentive to share proprietary information or discuss vulnerabilities with competitors or government. Government agencies are required to safeguard information as a means to protect national security and maintain public safety. Law enforcement and homeland security authorities are equally constrained and have a responsibility to control and manage information between jurisdictions on a "need to know" basis.

Helping to overcome these obstacles are US-CERT's partners: Infragard, the ECTFs, private sector security vendors, academia, federal agencies, ISACs, state and local governments, domestic and international organizations, and corporate computer security incident response teams.

Incident Reporting- Critical to Our Mission

US-CERT's ability to protect the infrastructure, respond to cyber incidents, and disseminate information is only as good as the data that is reported and shared across organizations. In July, 2006, the Office of Management and Budget (OMB) released a memo requiring federal agencies to report all incidents involving personally identifiable information (PII) within one hour of their detection. While this has improved security measures and incident reporting, it's important to note that PII isn't the only asset at risk. All cyber security stakeholders are encouraged to report cyber incidents, vulnerabilities, phishing scams or other events to the watch and warning center. Improving the Nation's ability to respond to the full spectrum of cyber hazards requires all sectors to report any type of cyber incidents as they happen. Reporting forms can be found on the US-CERT homepage at www.us-cert.gov. You can also submit incidents via:

soc@us-cert.gov (in the clear or encrypted), phone: 888-282-0870 or fax: 703-235-5965.

For more information on exchanging email with US-CERT, or to locate the public PGP key, visit http://www.us-cert.gov/pgp/encryptmail.html.

To receive free alerts and important cyber security information from the US-CERT National Cyber Alert System. Register at:

http://www.us-cert.gov/cas/signup.html .

Rob Pate is the Chief Security Officer at Renesys. He recently was Vice President for Cybersecurity and Privacy at McNeil Technologies. Prior to McNeil, Mr. Pate served as the Deputy Director of Outreach and Awareness at the National Cyber Security Division (NCSD) at the Department of Homeland Security as well as the Director of Focused Operations with the United States Computer Incident Readiness Team (US-CERT). He founded the Government Forum of Incident Response and Security Teams (GFIRST). This Government information sharing effort is focused on daily information exchange at the technical operators across different incident response teams representing the defense, intelligence, law enforcement, and federal civilian agency communities. In addition to his GFIRST activities, Mr. Pate led the US-CERT situational awareness program which was focused on providing the government with early indications and warnings as well as the Chief Information Security Officer's (CISO) Forum for the entire federal government. Mr. Pate came to the Department of Homeland security from an operational environment where he was the Director of an Incident Response Team for the largest federal civilian agency and the largest healthcare provider in the world.

Disaster Recovery Components of the NERC Reliability Standards

— James R. Stanton, Director of NERC Compliance ICF International

Operational Restoration of the Interconnected Electric Infrastructure

The epitome of a disaster for the interconnected transmission system is of course the blackout or the loss of all electric service to a significant portion of users. The most recent and most serious example of such a condition happened on August 14th, 2003 when the image of service interruption changed from isolated stories of spoiled food in dark refrigerators and random disabled traffic lights, to the scene of thousands of people stranded by the shutdown of mass transit systems walking across silent bridges, out of a crippled and sweltering Manhattan. The outage spanned multiple states and in an instant, reminded us all of how the system, interconnected for reliability, is also at risk to cascading outage events.

The figures are etched in the collective mind of the electric utility industry, 50 million people affected, over 61,000 megawatts of load lost. The cost estimated between $4 and $10 billion. Added to the human tragedy of the outage is the vulnerable position of critical infrastructure such an event enables. National security issues also come into play when huge segments of our electrical systems are disabled.

A reliable North American electric system, one that delivers consistent, uninterrupted power to every user, is not a dream or a far-fetched idea that we must begin to develop. To a large extent, that is what we have today. With the exception of infrequent, newsworthy outages, our level of reliability has never been higher. Still, with sporadic though devastating interruptions always a possibility, Congress saw fit to include electric reliability measures into its Energy Policy Act (EPAct) of 2005, signed into law August 8, 2005.

The EPAct contains provisions for the Electric Reliability Organization (ERO):

"The Commission shall have jurisdiction, within the United States, over the ERO certified by the Commission under subsection (c), any regional entities, and all users, owners and operators of the bulk-power system, including but not limited to the entities described in section 201(f), for purposes of approving reliability standards established under this section and enforcing compliance with this section. All users, owners and operators of the bulk-power system shall comply with reliability standards that take effect under this section."

The key element of the ERO function is the responsibility to ensure electric systems' reliability setting standards that are mandatory and enforceable. These Standards apply to all "users of the bulk electric system" with monetary penalties and other possible sanctions assessed to entities that fail to comply with the standards and their associated measures.

(Continued on next page)

NERC

Reliability operating procedures and planning standards have been a feature of the North America Reliability Council (NERC) since the late nineteen-sixties. Constantly refined and expanded over the years, they have served the systems well, but they were voluntary requirements. Peer pressure and public notice of violations were deemed sufficient incentives to assure reasonable compliance. It is obvious the drafters of EPAct and the legislators who endorsed it felt that such voluntary compliance was no longer acceptable, and so reliability, and the associated standards and measures developed under the auspices of the ERO now carry the weight and penalty of federal law.

NERC was formed in 1968 following the northeast blackouts to specifically address reliability. For many years NERC has worked with a small staff and legions of volunteers to address reliability concerns, draft the (formerly) voluntary rules, and develop new measures to keep up with the ever-increasing power needs of North America. In 2003 NERC took the historic step of becoming an ANSI (American National Standards Institute) approved standard setting organization. The ANSI requirements ensure standards are developed in a fair, open, balanced and inclusive manner, that all industry stakeholders are afforded the opportunity to participate in their development, and that all comments both pro and con and their provisions are responded to by the Standards Drafting Teams in a public forum.

There are 12 categories of Reliability Standards that span responsibilities such as Communications, Transmission Planning, and Emergency Operating Procedures. Four of them deal with features of disaster recovery:

COM-002-2 Communication and Coordination was written, "To ensure Balancing Authorities, Transmission Operators, and Generator Operators have adequate communications and that these communications capabilities are staffed and available for addressing a real-time emergency condition. To ensure communications by operating personnel are effective."

A critical component of any disaster recovery plan is the viability and integrity of communication systems. In the event of a widespread contingency or blackout on the electric system (the industry's most immediate example of a disaster), the entities involved in identifying, mitigating and correcting the cause must have the ability to communicate with each other and coordinate their activities.

COM-002-2 outlines who is responsible for what:

- Balancing Authority - The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
- Transmission Operator - The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission facilities.
- Generator Operator - The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.

In the event of a blackout or other significant contingency on the electric system, such as avoltage collapse, relay mis-operation or frequency disturbance, the entities that can identify and correct the problem must have the communication ability required in the COM-002-2 Standard to work together in resolving and recovering from the problem.

EOP-006-1 Reliability Coordination – System Restoration defines the responsibilities of the Reliability Coordinator. Part of such recovery mechanisms are the Restoration Plans that each Transmission Operator must have in place. The Reliability Coordinator is tasked with coordinating these various plans and is defined as, *"The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision."*

The standard's purpose is to insure that there is a central coordinator who will make certain that reliability is maintained during restoration and that the priority will be restoring interconnection. The Reliability Coordinator also serves as the primary contact for disseminating information and making sure that neighboring Reliability Coordinators and Transmission Operators or Balancing Authorities.

Restoring the interconnected electric system to full functionality, and resuming service to end use customers, requires that the recovery plan of each entity involved in the restoration is implemented in a coordinated fashion. Disabled portions of the grid must be reenergized and then synchronized to the non-disabled portions so that generation to load balance and frequency are maintained within tolerances.

Black Start generators are another critical factor in restoring service. These are typically small, gas fired units or hydroelectric facilities that can start themselves without any incoming electrical service and begin the process of restoration by injecting power into the grid. Power from Black Start units is often used to re-energize the systems of larger generators allowing them to resume operations.

EOP-009-0 Documentation of Black Start Generating Unit Test Results delineates requirements to insure the designated generators playing a role in this unique operation are ready and able to perform. The Black Start facilities must be periodically tested in order to confirm their start up and run capability and the standard mandates a Blackstart Capability Plan to make sure that their location and quantity is such that they can perform as part of a coordinated Regional System Restoration Plan.

It is clear the requirements of the NERC Reliability Standards play a key role in restoring electric service in the event of a large scale interruption, and such restoration will play a huge role in other disaster recovery activities. The communication capabilities of InfraGard are ideal mechanisms to make the larger group of key infrastructure protectors aware of the role an interconnected electrical system plays in disaster recovery, and may engender avenues of coordination as plans are refined and improved.

James R. Stanton is the Director of NERC Compliance ICF International

USGS Use of Technology After Hurricanes Katrina and Rita and Planning for Future Emergency Response

— Gaye S. Farris

Responding to the Hurricanes of 2005

Although the U.S. Geological Survey is not considered a first responder, it regularly provides science and technology to assist first responders after national disasters such as earthquakes, volcanic eruptions, and hurricanes. Nowhere did the USGS do that more effectively than in the wake of Hurricanes Katrina and Rita. Additionally, USGS became a first responder itself when the urgent call for boats came during Hurricane Katrina, the costliest hurricane to ever hit the United States.

Technology Assistance for 911 and 1-800 Calls

As calls for boat rescues and humanitarian aid began pouring in, so did requests to use USGS technology. Flooding in the New Orleans area reached 13 feet in some neighborhoods, making rescue based on street addresses useless. Street signs were covered, often only roof tops of houses were visible, and most responders were from areas far outside the city and thus not familiar with neighborhoods.

The Louisiana Department of Wildlife and Fisheries and the Louisiana State Police asked the USGS National Wetlands Research Center to use its technology to convert street addresses to latitude and longitude coordinates. Other users of the data included the Louisiana Office of Homeland Security and Emergency Preparedness, Federal Emergency Management Agency, Centers for Disease Control and Prevention, and Louisiana Geological Survey.

After USGS staff determined the coordinates, they added them to a layer of a geographic information system (GIS) and produced paper maps for helicopter and boat rescuers to locate stranded citizens. The information was derived from both 911 calls and a 1-800 emergency number the Department of Wildlife and Fisheries had established. The USGS used a street dataset in the GIS to approximate the street address coordinates.

Emergency responders without Global (GPS) Positioning System equipment requested maps with geographic coordinates overlain on grids of street addresses on aerial photography. Responders with GPS requested coordinate data in a digital form that could be sent directly to their equipment.

In the three weeks following Hurricane Katrina, 23,087 emergency calls were placed, but 7,487 lacked street addresses; additional ones had nonspecific descriptors that could not be processed by geoaddressing software. Consequently, about 9,000 calls were successfully converted to latitudes and longitudes for Katrina. To perform this work, USGS personnel worked 24/7 in shifts at the Office of Emergency Preparedness in Baton Rouge. Others also worked around the clock at the New Orleans Saints football team's practice headquarters coordinating these data with urban search and rescue teams; often they slept on the playing field.

(Continued on next page)

By the time Hurricane Rita hit southwestern Louisiana on Sept. 23, 2005, with a 14 foot storm surge, USGS scientists had outfitted their mobile spatial data unit and were able to travel to hard-hit Cameron, La., to geoaddress more calls. By Sept. 27, they had created coordinates for 128 calls or about half the calls received. Details on the 911 conversions are being published by the USGS. *(1)*

Other Emergency Responses: Mapping and Data

Because the USGS National Wetlands Research Center had worked closely with many State and Federal agencies in providing geospatial analyses, especially for monitoring and projecting coastal land loss, the Louisiana Office of Homeland Security and Emergency Preparedness and other agencies called on it to further assist in Katrina disaster recovery.

Staff from FEMA requested maps of flooding and water levels, levee breeches, pumping stations, roads, debris location, human remains, and satellite and aerial imagery for key personnel from the FEMA Incident Support Team and others. Partners helping with geospatial activities included the U.S. Army Corps of Engineers, U.S. Department of Agriculture (USDA), and USDA Forest Service. The center also used its Data and Information Management Systems to deliver aerial photography and maps to emergency responders. *(2)*

In the aftermath of Hurricane Rita, with its 14-foot surge and flooding that extended inland 15-20 miles, hazardous debris was scattered throughout the area. Debris included industrial equipment, gas and diesel tanks supporting the oil industry, and household hazardous material. The USGS National Wetlands Research Center supported FEMA personnel from Oct. 30 to Nov. 26, 2005 by analyzing aerial photography to help in surveying damage and locating, identifying, and removing hazardous waste. *(3)*

Becoming a First Responder

Hurricane Katrina made landfall at 6:20 a.m. on Aug. 29, 2005, southeast of New Orleans as a strong category 3 storm, but with gusts up to 140 miles per hour. Because of the catastrophic flooding of 80 percent of New Orleans, Louisiana state agencies called on USGS to use their expertise in boating and their knowledge of the New Orleans area to rescue hundreds of citizens stranded on roofs and porches.

Amid rumors of violence in New Orleans, USGS scientists in Louisiana left their offices at the National Wetlands Research Center in Lafayette each morning before dawn, pulling boats and emergency supplies of water. The USGS personnel teamed up with the U.S. Fish and Wildlife Service, the Louisiana Department of Wildlife and Fisheries, the National Guard, the Phoenix Fire Department, and other volunteer responders, directly rescuing almost 600 people by using boats, and indirectly 1,900 more by helping them off tug boats or helicopters.

Meanwhile, other USGS scientists and staff were also busy back at their offices, donating water, food, and blood. They volunteered at night at the evacuation shelter in Lafayette, the Cajundome, a sports arena that housed almost 20,000 evacuees during the 2005 hurricane season. They opened their homes and offices to displaced family, friends, scientists, and even journalists who could find no place to stay in a state with ravaged communication networks and infrastructure. Phones were unreliable and sometimes just did not work for weeks. Internet connections often failed.

Summary of USGS Responses to the Hurricanes of 2005

In addition to the work the Louisiana USGS science centers performed, a summary will soon be published of how USGS nationwide responded scientifically to Hurricanes Dennis, Katrina, Rita, and Wilma. *Science and the Storms: The USGS Response to the Hurricanes of 2005* should be available in print and online in early fall of 2007. *(4)*

Planning for Future Emergency Response

Science Response Vehicle

Applying lessons learned about the needs of first responders, the USGS National Wetlands Research Center is maintaining a Science Response Vehicle, which was first used after Hurricanes Katrina and Rita. The vehicle, capable of rapid deployment in response to natural disasters throughout the United States, is equipped with computers, software, and plotters to provide spatial analyses. Spatial analysis technologies available in the vehicle enable scientists to:

- Evaluate land use, recovery, and restoration
- Develop maps and imagery of critical infrastructure for first-responder assessments
- Model biological impacts of natural hazards (hurricanes, earthquakes, and wildfires)
- Help in emergency response and humanitarian search and rescue operations (e.g.. mapping of 911 calls)
- Provide rapid scientific monitoring and assessments of biological, geological, hydrological, and geographical resources
- Transfer critical monitoring data.

Additionally, the vehicle provides:

A scientific base for sample collection and field processing

- Critical Internet communications through an onboard satellite dish
- Capability for serving as a GPS-base station
- Satellite voice and data communications
- Television reception for weather and emergency information
- Living quarters for scientists.

Technology to Analyze Wetland Loss

The USGS National Wetlands Research Center continues to use its technology and databases to provide information for coastal restoration. Such information includes several critical studies documenting that Louisiana lost 217 square miles of coastal land after Hurricanes Katrina and Rita. *(5)*

Hurricane Data on the Web

The USGS National Wetlands Research Center also continues to provide hurricane data and imagery from several different sources at the Web sites below:

- Hurricane Information Center is part of the LaCoast Web site managed by USGS and sponsored by the Coastal Wetlands Planning, Protection and Restoration Act task force. It contains geospatial data, monitoring and assessment information, photography, emergency response activities, studies, posters, presentations, and hurricane summaries. http://www.lacoast.gov/hurricane/index.htm
- Hurricanes: Powerful Agents Shaping the Coast is part of the National Biological Information Infrastructure's Central Southwest Gulf Coast Information Node. It provides a user-friendly method for locating topical information from multiple agencies and resources. Categories include the relationship between hurricanes and climate, data resources, economic impact, environmental impact, flooding and storm surge, health and safety, land loss, maps and images, and response and recovery. A special section focuses on hurricanes that have had a significant impact on the Gulf Coast. http://www.nbii.gov/portal/community/Communities/Geographic_Perspectives/Central_Southwest_&_Gulf_Coast/Ecosystems/Gulf_of_Mexico/Gulf_Coast_Hurricanes/
- Hurricane Research at NWRC gives examples of the National Wetlands Research Center's wide-ranging hurricane efforts and the hurricane work it has done dating back to that of Hurricane Andrew in 1992. www.nwrc.usgs.gov

Drills and Workshops

Currently, the National Wetlands Research Center - working with other USGS coastal partners and local, state, and federal agencies - is involved in drills and planning for hurricanes and other disasters in which its technology, particularly its SRV and its databases, can be of immediate assistance to first responders.

(Continued on next page)

The National Wetlands Research Center continues to sponsor its own hurricane drills and participate in others such as the 2007 Spills of National Significance and the State of Texas drill. The center also hosts data workshops related to search and rescue:

- Hurricane Season Geospatial/Imagery Data Availability: Data Mining, an annual two-day workshop presents various available geospatial/imagery data sets related to Hurricanes Katrina and Rita. This year's (July 2007) included proposed and planned geospatial/imagery data sets collected by various agencies.
- Louisiana Coordinate Reference/Grid Systems: Emergency Response Workshop, a one-day workshop in April--sponsored by the Louisiana GIS Council, Louisiana Department of Transportation and Development, Louisiana Department of Environmental Quality and USGS/Louisiana National Spatial Data Infrastructure Partnership Office--provided a forum to coordinate reference/grid systems for emergency response events in Louisiana.
- Unmanned Airborne Vehicle (UAV) Imagery for Domestic Emergency Response and Natural Resource Survey: Deployment, Operations, and Applications, a workshop held December 2006, provided a forum for evaluating the deployment, processing, and applications of UAV platforms and imagery data for first responders' search and rescue and various natural resource damage assessments.

The Research Science Continues

Concurrently with the development of emergency response process and information, the USGS National Wetlands Research Center continues long-term research conducted by the its cadre of biologists and geographers to assist in coastal restoration.

Gaye S. Farris (gaye_farris@usgs.gov) is Information Branch Chief at the USGS National Wetlands Research Center. She is the center's publishing liaison and manages public affairs, outreach and education, the center's library, information technology, and the center's publication approval process.

---

(1) *Conzelmann, C.P., Sleavin, W., Couvillion, B., in press, Using geospatial technology to proccess 911 calls after Hurricanes Katrina and Rita, in Farris, G.S., Smith, G.J., Crane, M.P., Demas, Robbins, L.L., and Lavoie, D.L., eds., Science and the storms—the USGS response to the hurricanes of 2005: U.S. Geological Survey Circular 1306.*

(2) Wilson, S., and Cretini, C., in press, Data access and dissemination for emergency response and long-term recovery efforts related to hurricanes Katrina and Rita, in Farris, G.S., Smith, G.J., Crane, M.P., Demas, Robbins, L.L., and Lavoie, D.L., eds., Science and the storms—the USGS response to the hurricanes of 2005: U.S. Geological Survey Circular 1306.

(3) Hartley, S., in press, USGS Humanitarian and geospatial response for search and rescue after Hurricanes Katrina and Rita, in Farris, G.S., Smith, G.J., Crane, M.P., Demas, Robbins, L.L., and Lavoie, D.L., eds., Science and the storms—the USGS response to the hurricanes of 2005: U.S. Geological Survey Circular 1306.

(4) Farris, G.S., Smith, G.J., Crane, M.P., Demas, Robbins, L.L., and Lavoie, D.L., eds., in press, Science and the storms—the USGS response to the hurricanes of 2005: U.S. Geological Survey Circular 1306.

(5) Barras, J.A., 2006, Land area changes in coastal Louisiana after the 2005 hurricanes-- a series of three maps: U.S. Geological Survey Open-File Report 2006-1274, accessed July 31, 2007 at http://pubs.usgs.gov/of/2006/1274.

Barras, J.A., 2007, Satellite images and aerial photographs of the effects of Hurricanes Katrina and Rita on coastal Louisiana: U.S. Geological Survey Data Series 281, accessed July 31, 2007 at http://pubs.usgs.gov/ds/2007/281.

Barras, J. A., in press, Land area changes in coastal Louisiana after Hurricanes Katrina and Rita, in press, in Farris, G.S., Smith, G.J., Crane, M.P., Demas, Robbins, L.L., and Lavoie, D.L., eds., Science and the storms—the USGS response to the hurricanes of 2005: U.S. Geological Survey Circular 1306.

Hurricane Katrina: The Houston Response—What Made it Work

— LCDR Joseph J. Leonard, Jr., United State Coast Guard
— Fire Marshal Mike Montgomery, Harris County Fire Marshal
— Chief Robert W. Royall, Jr., Harris County Fire Marshal's Office
— Lieutenant Gary Scheibe, Houston Police Department

Hurricane Katrina directly impacted the States of Louisiana, Mississippi, and Alabama in August 2005, but indirectly affected almost every other state before the end of September. The devastation was unprecedented and required a massive response at the federal, state, local, and private sector levels.

A lot has been written since Katrina made landfall on what went wrong at all levels of the response. Less has been written about things that went right. We were somewhat successful in our response activities in the Houston area for several reasons, but the most important being we were not in the immediate impact area and had some time to react.

In the span of 23 days, the Houston Megashelter Operations Area Command sheltered more than 44,000 displaced citizens while directing another 105,000 to other shelters within the State of Texas after initial Inprocessing and medical triage. We did this with the assistance of many organizations that provided about 8,000 responders and another 80,000 volunteers. Without these organizations and these dedicated professionals and volunteers, we would not have had the same level of success that we experienced.

We learned many lessons the hard way, but we hope that other entities faced with similar crises in the future may learn from our experiences. Some of the best practices we will look at include unified command, pre-established relationships, agency representatives, local infrastructure, contingency plans, and how to try expect the unexpected.

Unified Command

We recognized early into the response that this was not going to be an event that was going to be managed by a single organization; in fact, we were rather certain that this would require a much wider array of organizations that any of us had ever conceived. The response community in this area, comprising representatives from federal, state, local, and private sector entities, had already embraced the National Incident Management System (NIMS) and had practiced unified command on multiple occasions, including severe weather response during Tropical Storm Allison, oil spills, hazardous materials incidents, and ship fires. In fact, most of the senior Area Command staff had served for years on an ad-hoc interagency NIMS Incident Command System (ICS) training team, further aiding the rapid establishment of an effective incident management team.

NIMS is an "all risk, all hazards" approach and goes a long way toward enhancing an effective direction and control functions. All agencies that have a direct role in an emergency response are required to complete specific NIMS training in order to maintain homeland security grant funding. Other organizations have internal NIMS compliance requirements in place and it is optional for those in the private sector. Nonetheless, a lot of organizations that are not required to follow NIMS are doing so as they recognize that most of the other responders with whom they will be working use it.

(Continued on next page)

This training is available online, from trainers working for agencies that are using it, as well as from several qualified service providers. Contingency planners and training officers should determine your specific compliance requirements and which source is best for your individual organization. Like any other skill, you have to use it or you will lose it. Follow your initial training with additional classes, drills, and exercises.

Successful unified command is best described as an effective partnership amongst key agencies involved in the response. While there may be a large number of participating organizations, the actual number of participants within the unified command should be kept small, generally no more than five. In our case, we had representatives from the U.S. Department of Homeland Security, Harris County, and the City of Houston. Other agencies had representative in many of the critical command and general staff positions, either at the area command level or within the various incident command systems that were established under the area command.

Pre-Established Relationships

All of the principal organizations comprising the unified command had worked together in the past, giving a general feeling of comfort amongst the key participants. This was the key to our success.

At 2:00 a.m., in the middle of a disaster is not the time of day to meet your fellow responders for the first time. If you want to succeed in emergency response, you should know your fellow responders well before an incident takes place.

You should know their personal and organizational capabilities and limitations, what types of incidents they feel comfortable with and where there is doubt, how comfortable they are making decisions and even how they take their coffee.

We had a lot of Type-A personalities present in the command post but egos were left at the door. This was not the time for interagency rivalry. Regardless of rank or organization, each member of the command team assumed his or her assigned role, becoming a single incident management team that provided the best services possible to the displaced citizens we were serving.

It was these previously established relationships that enabled the Area Command to stand up so rapidly and effectively. We were already familiar with one another, had a comprehensive understanding of each others' capabilities and limitations, and knew everyone could make decisions in a timely manner.

Agency Representatives

NIMS teaches that Agency Representatives are usually the senior participants from their responding agencies and that they work through the Liaison Officer (or directly for command) unless assigned elsewhere within the response organization. They must be well versed in their organizational capabilities and limitations. These Agency Representatives MUST have the authority to make decisions and commitments from their respective organizations.

Agency Representatives must be familiar with NIMS and understand where they fit in to the overall picture, as well as what is expected of them. If they cannot meet these requirements, they need to ensure that there is communication between the Liaison Officer (or command) and their Agency Administrator to overcome any obstacles. This may require the assignment of a more capable Agency Representative with decision-making authority.

We realized that everything did not work perfectly during our operation in Houston in August and September of 2005. But one thing was very clear: we had fewer command and control issues with those organizations that provided effective and able Agency Representatives. We struggled with those organizations that did not embrace the critical NIMS concepts and those that sent representatives without the authority and control to make decisions and commitments for their organizations.

Local Infrastructure

When responding to a major incident, it's really helpful to know and understand your local infrastructure and how it can best be put to use for your advantage. There is a lot of talk these days about "interoperability." Interoperability involves a lot more than shared radio frequencies. Knowing where you can obtain additional resources, logistical support, or facilities, in a timely manner can mean the difference between an effective response and one where the emergency is still in charge.

Knowing your road and rail network, your communications capabilities and limitations (such cell phone and radio dead zones), water supplies, and hospital surge capabilities before an incident can help with operational and logistical planning.

A comprehensive understanding of your contingency plans can pay big dividends when trying to better understand how you can best utilize your local infrastructure to your advantage.

Contingency Plans

Know your plans. You should not be reading your plans for the first time after the incident has occurred. You should be familiar with your plans, resource and logistical support requirements and communications instructions necessary to initiate and continue with effective response operations.

The best way to do this is to take an active role in their development. In that fashion, you gain the knowledge of how and why the plan was put together, and you are more familiar with your vulnerabilities or resource shortfalls.

Plans are not effective until they have been tested and validated. That is why we have exercises. In these exercises (which may be tabletop, command post, or full scale), we get to see if the plan will work and if not, where we need to fix the plan so that it will work the way we need it to.

No one had a plan for a megashelter operation, but we had to begin our activities with the plans we had. Both the American Red Cross and the Salvation Army had mass care plans. Local government plans existed for communications, mutual aid, and facility sharing. We took these and multiplied their requirements many times over while ensuring that we had the logistical support to manage such an endeavor. In addition, we still had to make certain that the third largest county and fourth largest city in the United States were not so stripped of resources that they could not provide essential services to the regular populations. Local (city and county) and state mutual aid agreements were instrumental in providing most of the resources needed to implement effective operations.

Expect the Unexpected

Hurricane Katrina was tabbed as one of the largest hurricanes to ever reach the Gulf Coast. Beginning with the initial trickle of evacuees into Reliant City, the unified command staff began to ask "What if . . . ?" What if the number of evacuees is more than expected? What if an NFL team has its home opening game scheduled for the same stadium complex that was acting as a shelter? What if the shelter location is too small for the numbers on the way? What if somebody decides that cruise ships are an effective shelter location? What if another Category-5 hurricane enters the Gulf of Mexico and takes dead aim at Houston?

We instituted briefings after each of two daily shift changes, in accordance with the standardized "Planning P," as set down in NIMS operations. Following the evening briefing, the command staff would get together and discuss contingency plans for these and many other possible events. The result of those informal discussions was a series of contingency plans that could be put into place as needed. Before the Reliant City megashelter closed its doors 23 days after it opened, every one of those plans was tested and used.

The success of those efforts was due to ongoing planning and discussions about possible emergencies within the disaster. When each occurred, it was a relatively simple matter to put the right contingency plan in action.

(Continued on next page)

Conclusion

Hurricane Katrina was a worst-case scenario—the kind that we hope only comes around once in a career. In emergency response, we recognize that there is no organization with all the resources necessary to guarantee success; we need to reach out to other agencies and work together to mitigate the incident, ideally in an effective and efficient manner. Effective in that we minimize the overall impact of the event on the population and efficient in that we minimize the cost necessary to ensure success. Understanding the intricacies of unified command, having effective pre-established relationships with other emergency responders, effectively using Agency Representatives, being aware of local infrastructure, validated contingency plans, and asking "What if…?" were some of our keys to success.

While not all-encompassing for every type and kind of incident, some of the NIMS best practices can help most organizations in their day-to-day response activities. As a direct result of the lessons learned during the mega-shelter operations, this area is better prepared for similar disasters should they ever occur in the future.

Lieutenant Commander Joseph J. Leonard, Jr. is the Chief, Response Department, US Coast Guard Marine Safety Unit Galveston. Fire Marshal Mike Montgomery is the Fire Marshal and Emergency Management Coordinator for Harris County, Texas. Chief Robert W. Royall, Jr. is Chief of Emergency Operations for the Harris County Fire Marshal's Office. Lieutenant Gary Sheibe is with the Houston Police Department and serves in the Mayor's Homeland Security Office. The authors served as part of the Area Command during the Hurricane Katrina Megashelter Operations in Houston.

Dear Readers

Threat risk assessments. Electrical grids. Hurricane Katrina.

Disaster recovery touches everyone. In this issue we take a look at some lessons learned and tools used following Hurricane Katrina that devastated the US Gulf Coast in 2005. We also explore threat risk assessments – the basics and how they can be useful to you, introduce you to DHS' National Cyber Security Division (October is, after all, National Cyber Security Awareness Month) and disaster recovery components of NERC reliability standards (electricity). If you don't think that the latter is important, remember August 14, 2003, when a massive multi-state power outage effectively took out a large portion of the northeastern United States. If you were there, you probably have a whole new appreciation for electricity and air conditioning.

Thank you to our editorial review team:

Dan Biby – Dan has more than 18 years experience in business continuity planning, serves on the InfraGard Oklahoma Members Alliance board, and has authored articles and a reference book (Disaster Dictionary) on the subject.

Ray Hornung – Ray is a business continuity planner with the National Marrow Donor Program in Minneapolis, MN.

We are looking for experts in food and agriculture security to review articles for the next issue. If you are interested, please contact the editor at editor@infragardmembers.org

As always, The Gardian is your publication. We welcome any comments or suggestions.

Thank you.

Editorial Board

Please report any InfraGard membership information changes (i.e., email address, mailing address, etc.) to infragardhelpdesk@infragard.org.

Contact Us

Web
For more information or to join InfraGard, please go to: www.infragardmembers.org

Email
ManagingDirector@infragardmembers.org

To receive future editions of the Gardian, please subscribe by sending a message to Subscribe@infragardmembers.org