Executive summary

While it’s impossible to predict when or where an emergency may occur, planning ahead is critical to your operations and your employees. By working together, drawing upon resources such as the Homeland Security Information Network (HSIN), public and private sector entities can improve emergency preparedness and get back to business as usual, more quickly and efficiently.

Contents

HSIN: A ‘focal point’ for sharing critical information ........ 2
Preparing for effective response ......................... 2
The Boston Marathon bombing ....................... 3
HSIN R3 ........................................ 4
Public-private partnerships in emergency preparedness .......... 4
Financial institutions ............... 5
Building financial resiliency planning into emergency preparedness .......... 6
A famous and cleverly worded quote from Benjamin Franklin might say it best: “By failing to prepare, you are preparing to fail.” While these words were intended to make a statement on individual success, they are also particularly relevant for government agencies that need to be prepared for sometimes impossible situations.

In a post-9/11 world, there is no longer any doubt that disaster preparedness must be an essential part of any normal, business planning. Preparedness and mitigation costs have to be a part of your day-to-day operations; otherwise, you run the real risk of losing productivity, profits and your employees when an unforeseen incident strikes. The increased prevalence and power of major, natural disasters where we haven’t seen them before, combined with increased recognition of the threats of global pandemics and terrorism, are driving both business and government to work together in new, and innovative, ways to build relationships, share information, and train to respond to, and recover from, major incidents, well before they occur. An essential part of such preparedness efforts between the public and private sectors is information sharing, and the U.S. Department of Homeland Security’s Homeland Security Information Network (HSIN R3) is an essential and leading part of public-private cooperation, coordination and collaboration.

HSIN: A ‘focal point’ for sharing critical information

One of the recommendations of the 9/11 Commission was the creation of the HSIN, a national, secure and trusted Web-based portal for critical information-sharing and collaboration among federal, state and local government entities, as well as the private sector engaged in homeland security. Operated by the U.S. Department of Homeland Security (DHS), HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging and document sharing.

HSIN allows partners to work together instantly, regardless of their location, to communicate, collaborate and coordinate. Users can securely share information within their communities or reach out to others as needed. Prior to its creation, each individual entity would need to separately contact other entities one at a time, wasting critical time and resources. Now, entities have one place to go.

HSIN is “the nation’s focal point for the sharing of sensitive but unclassified (SBU) information across the entire homeland security enterprise,” says Michael Brody, policy outreach and communications manager for HSIN at the Department of Homeland Security. “Our job is to make sure that homeland security professionals nationwide, as well as corporate security officers, get the unclassified information they need to be prepared for major incidents, to be aware of major intelligence alerts, and to help manage major events and incidents when and if they occur.”

Preparing for effective response

But HSIN isn’t just an information source during emergencies. It’s a way for professionals in the public and private sectors to establish relationships with each other well before an incident occurs, so they are adequately prepared to respond to a disaster in a coordinated way.
“The most important lesson that we learned from 9/11 is that the way we prevent incidents like that from happening again, and the way that we ensure that we respond effectively to such incidents, is to share information and build critical relationships before something happens,” says Brody. “Any emergency manager will tell you that the time to start building relationships for preparedness activities is not 12 hours into an incident, it’s 12 months before an incident may occur. The network is a major facilitator of just that.”

By registering and joining HSIN, emergency response managers get the information they need from DHS, as well as the state and local government, to be prepared. The network is a key component of ensuring that individuals know ahead of time where to go to get the information they need once something happens or is impending.

After an entity registers with HSIN, DHS identifies and validates its identity to ensure it receives the appropriate information. Registering on HSIN, Brody says, is as easy as registering to access an individual’s financial accounts or health records.

HSIN has been used over the past few years in a number of major incidents and operations, ranging from the Boston Marathon bombing to special events like the Super Bowl.

**The Boston Marathon bombing**

The April 2013 Boston bombing is probably one of the best and most recent examples of how HSIN works.

According to Brody, more than 100 intelligence analysts nationwide used the network within 12 hours of the incident to get the latest alerts and notifications. Similar information was being disbursed through critical infrastructure communities. HSIN created a webinar to ensure that responders had the latest information to distinguish fact from fiction about the response and the investigation.

“We did a lot of work ahead of time with all sorts of Homeland Security partners to make sure they had the resources they needed to quickly set up an information site,” Brody says. “We had already developed relationships with law enforcement across the country so that they were able to get a webinar going to ensure that we had the very latest awareness of what was true and wasn’t true about the response and the investigation in Boston.

“The reason that the information was able to flow so efficiently and quickly was because those communities were already well established on our network,” Brody says. “People that provide information to those networks knew how to get it posted, and people who are members of those communities knew where to go and what to look for. So preparedness is essential. When something happens, you don’t have time to ask, ‘What do I do?’ You need to know ahead of time.”
HSIN R3

Homeland Security recently released an update to the network, called HSIN R3. The updated HSIN is a more secure, advanced and reliable platform. It contains an entirely new suite of improved features and enhanced functionality. DHS is working on having simplified access to any number of sources of information, as well as a much wider variety of users.

DHS says the rollout of HSIN R3 is an excellent time for entities to familiarize themselves with the network if they haven't already, in order to be part of a much more advanced and expanded network of users.

The network currently has more than 40,000 registered users, but DHS wants to increase that number. While there is strong awareness of the network within many of the critical infrastructure sectors, such as law enforcement, DHS is looking to enrich and increase its involvement in such areas as fire services, immigration and border security, and cyber security.

Donna Roy, HSIN program manager at DHS, wants more entities involved in critical infrastructure security to register with the network.

“It’s never too early to be prepared for the next disaster,” she says. “Some of our advisers in law enforcement have this analogy: You use your radio every day, and you are so used to using it that when it goes off during a fire, you don’t have to think about how to use it. We want our partners to use HSIN in a way that it becomes so familiar that, in a disaster, they know where to go and what to do to find the information they need, so that they can better respond.”

Public-private partnerships in emergency preparedness

Not surprisingly, most registered HSIN users are state- and local-level security and response professionals. But, about a quarter of them work in the private sector. According to DHS, more than 80% of critical infrastructure in the U.S. is owned by the private sector.

That is why it’s essential that representatives of public and private entities involved in the homeland security mission engage each other in order to be ready to work together to create a coordinated response in the event of an emergency. DHS says HSIN is a great way for them to do that.

“One of the key functions of government is to ensure that the owners of businesses have the knowledge that they need to know what threat they or their employees may be facing,” Brody says. “HSIN is a great way to build those relationships and to collaborate in real time, in a secure place, with all the key owners of critical infrastructure in your community that you need to be able to liaise with.”

On its own, the private sector has been able to build a system of resilient continuity resources that it shares with its public sector partners in order to drive effective policies. That has led to increased cooperation between the two spheres.
Cooperation between the public and private sectors in preparing for emergencies has shifted “180 degrees, from segregation to full integration,” in recent years, says Jeff Dell, senior business continuity consultant at Bank of America Merrill Lynch. And an enormous amount of progress is being made each day.

“The linkage between the public and private sectors is critical,” he says. “Where we have improved relationships between government and the private sector, we have a much higher effectiveness in planning, response and recovery.”

Financial institutions

In particular, because they have so many relationships and fundamental connections with entities in both the private and public sectors already, banks play a key role as a liaison between local government responders and the private sector in both preparedness and emergency response.

Because banks receive information directly from emergency responders, they are able to leverage that information to make informed business decisions and to pass this information on to their commercial and business clients. This is critical, as these local clients can often provide aid in the response and relief effort.

Utilizing local private sector resources provides two benefits: It makes the response quicker and more efficient, and speeds the recovery process by helping businesses and the local population get back on their feet quicker.

Initially, the consensus thinking was to bring in out-of-region resources to aid in the response effort, Dell says. But then the bank started to explore the flow of commerce at “a very fundamental level” to see how it could be used to help in a disaster situation.

“We really want to encourage the government agencies responding to consider leveraging the resources within the impacted community before they bring in someone from out of the region,” he says. The victims themselves may have businesses that could provide goods and services to support the victims and survivors of the disaster, everything from batteries to cots, but particularly perishable items, like food.

Not only does involving local businesses in the effort improve efficiencies, but it keeps commerce flowing and businesses open and operating, he notes. And getting back to “business as usual” should be a top priority in any disaster situation, not just for practical reasons, but also for its psychological benefits on the affected community.

“We want to help our client businesses where possible, and governments picked up on this. They think this is a great idea and they are moving the dial,” Dell says. “They’re making the effort to leverage local commerce.”

Being part of the response and relief effort provides an “extra level of incentive” for private sector businesses to increase their own emergency preparedness. “If you have a continuity plan, and you’re able to answer the phone when FEMA calls during a disaster, you can directly support the response and recovery effort in your own community,” Dell says. “If they are prepared to the degree that FEMA or the local government is requesting, we can keep that client in business longer.”
The bank is working with its clients in both public and private sectors to help build awareness and best practices. But while public-private partnerships are improving in emergency preparedness and resiliency planning, more work needs to be done to include nonprofit organizations and nongovernment agencies in the loop. These entities, which include churches, food banks, soup kitchens, missions and the like, are neither public nor private agencies, but are often on the front lines of helping people who need it the most during an emergency.

Building financial resiliency planning into emergency preparedness

Banks play a larger role in financial resiliency planning. There are dozens of items in the financial area that private and public sector entities must consider and have “at their fingertips” in the event of a disaster, so they can support themselves — as well as their employees, customers and communities that depend on them — and get back up to business-as-usual status as quickly as possible.

Banks can help officials in both the public and private sectors understand what steps they need to take to be prepared, as far as their financial needs and business continuity plans are concerned. Importantly, an effective preparedness plan must align with each party’s capabilities. The first step in the process is becoming aware of what those needs are and how the banks can help respond.

While first responders are generally well prepared and have the equipment and experience to deal with a disaster, many public and private entity officials don’t always think about the business side of an emergency, such as how they will be able to sustain themselves and function for many days, if not weeks, if they can’t return to their offices.

In August 2004, the central Gulf Coast of Florida was hit by Hurricane Charley. While there may be a common belief that hurricanes hitting Florida are relatively routine, in fact, such storms don’t hit that part of the state very often, so the area was perhaps not as prepared as one might think, shared Sherry Burd, a Public Sector Banking senior client manager at Bank of America Merrill Lynch.

However, governments and businesses learned lessons regarding disaster preparedness from that storm and have, together with their banks, built those lessons into their financial resiliency planning, Burd said.

People in the path of a hurricane have the relative luxury of two or three days to prepare, compared to two or three minutes in the event of a tornado. But whether it is two days or two minutes, entities need to have the necessary plans already in place, so there is no time wasted thinking about what to do when an emergency strikes.

“In the case of a disaster, we don’t always think as clearly as when we’re sitting at our desk and we know our account numbers off the top of our head,” Thompson says.

At the onset of hurricane season, the bank provides its clients with a disaster preparedness document to help them create a contingency plan to have at their fingertips should a disaster occur. This document includes a schematic of all their account structures and the financial services for emergency preparedness

Banks offer a variety of products and services that can prove vital in a disaster situation:

- Emergency cash delivery via armored courier using existing relationship
- Mobile banking centers
- Telephone wires
- Mobile ATMs
- Payroll direct deposits
- Payroll card alternatives, such as prepaid cards
- Ability to send payroll file to the bank in advance with an effective payroll date
- Purchasing cards
- Small Business Administration loans after the disaster
treasury services at their disposal. It reminds them to update the telephone numbers of critical contacts at the bank should they need to get in touch with them, as well as the other information they need to be prepared, such as having enough cash on hand and making sure they have everything they need with them should they be required to evacuate.

Perhaps just as critical as putting these emergency procedures in place is testing them regularly. The goal, as Donna Roy of DHS notes, is that people shouldn’t have to spend time thinking about what to do in an emergency; the response should be automatic.

As such, Bank of America Merrill Lynch encourages its clients to perform a live, emergency payroll run within 30 days of receiving the disaster preparedness document, preferably from a remote location on a laptop computer. To do that, they will need security passwords and telephone numbers, as well as PIN numbers, in case they need to dial in and conduct a telephone wire transfer.

In advance of an actual hurricane, the bank urges clients to order large sums of cash to have on hand—not just for its own uses, but to hand out to its first responders should they need to purchase food or water in the community. It also encourages them to establish a relationship with an armored courier, because that might be the only way to get cash from the vault. However, they must handle the cash prudently. Ordering too much cash can be just as dangerous as having too little, especially if the word gets out to more than just a select few leaders. One of the vital lessons from Hurricane Charley was the importance of using purchasing cards to supplement or replace the use of cash.

The bank recommends that entities develop a hierarchy of critical employees and first responders who would have purchasing cards in an emergency. Likewise, they might need to release the spending limits on the cards and open the network of merchant codes where the cards can be used. For example, while in normal circumstances the entity might reasonably block purchases made with the cards at liquor stores, this might be the only place to buy ice in an emergency.

“Being trained to be prepared should a disaster hit is a huge best practice,” says Thompson. “It gives our clients peace of mind and us, too, knowing that our clients are well prepared.”

The client manager at your bank may have materials that provide a checklist on necessary preparations. Here are some preparations that public and private entities need to make before a disaster strikes:

• Create a business continuity plan.

• Order enough cash to have on hand, at least 48 hours in advance.

• Acquire an emergency line of credit.

• Be able to meet payrolls in the event there’s no building for employees to go to.

• Help employees pay for emergency needs.

• Create a telephone “call tree” for your employees.

• Back up computers to access online reports.
• Cross-train employees on payroll issuance; have backup personnel to perform this function.

• Distribute extra cash among several key employees, rather than having it with one person.

• Identify key banking centers for deposits and employee check-cashing.

• Know where alternative banking centers are located, so staff can be directed to them in the event of closures.

• Ensure all passwords and critical phone numbers are on hand; employees should have copies of this information at home, not just at the workplace.

• Prepare contingencies in the event of extended disruption of power or communications connectivity, especially as it relates to cyber security.

• Make sure vendors continue to get paid on time.

• Identify contingency locations.