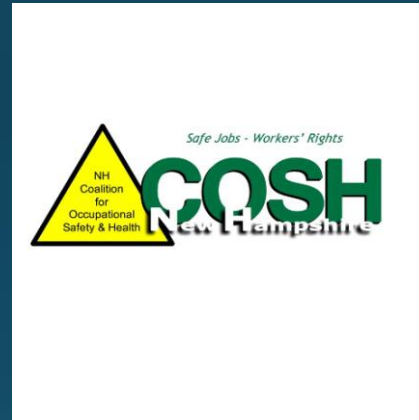


## December 2016 G. I. Roundtable



## Preparation, Planning, Mitigation for All Hazard Events

# Housekeeping

- Exits
- Rally points
- Cell phones
- Facilities



# Agenda

- Threats
- Vulnerability assessment
- Information sources



# Business Threats

- Insurance companies list threats to businesses ranging from property losses through electronic data breaches.
- Threat assessment has transcended from the traditional view to encompass both environmental and deliberate causes.
  - The term “all-hazards” is now considered de rigueur in the emergency response community.
  - Domestic and international groups would harm and have harmed the US for a variety of reasons.





Oct 22nd

## 5 Common Threats Small Businesses Face

BY ADMIN | SMALL BUSINESS, WORKERS COMPENSATION | NO COMMENTS »



GUEST POST BY ALYSSA DELLACAMERA | EATON & BERUBE

Today's guest post is brought to you by Alyssa DellaCamera from [Eaton & Berube Insurance Agency](#), an independent insurance agency located in New Hampshire. Learn about the common threats small businesses face and strategies to manage them.

As many small business owners understand, owning your own company offers many rewards, but with these rewards come certain risks. To protect your business from the exposures it faces, it's crucial to identify these threats and develop a [risk management plan](#). The following list of common threats to small businesses will help you identify the risks your company may face, as well as provide you with strategies to manage them:

### 1. Property Losses

For many small business owners, commercial property represents one of your largest assets. To protect your business from a potentially devastating property loss, it's important to ensure that you have adequate coverage. Taking an inventory of your property can help you

### Subscribe by E-mail

Enter email address...

GO

### Connect With Acadia



### What's Popular

- What do I need to consider about boarding horses on my hobby farm? 97 views
- 5 Common Threats Small Businesses Face 77 views
- Top 5 Reasons Why You Should Consider Insurance as a Career 64 views

### Archives

- November 2016 (1)
- October 2016 (2)
- September 2016 (1)
- August 2016 (6)
- July 2016 (5)
- June 2016 (1)

### Categories

- Automobile (15)
- Construction (4)
- Cyber Security (2)
- Farm & Agriculture (11)
- General Liability (34)
- Insurance Careers (1)



## Top 10 Threats to Small Businesses

Simple strategies small business owners can take to identify and manage top risks, provided by Van Meter Insurance

Optimism is the fuel that drives the entrepreneurial spirit, so it isn't surprising that most small business owners consider themselves optimists. Too much optimism, however, can get a small business owner into trouble. A business plan built solely on the "best case scenario" is like a house of cards—one gust of wind (or fire or wrongful termination lawsuit) and the entire business can come crashing down. That's why smart business owners temper their innate optimism with a healthy dose of reality. In other words, they learn to manage risk.

The first step in implementing a comprehensive risk management plan is identifying potential risks. To help

you get started, we have provided a list of the top 10 threats facing small business owners. As you read through the list, consider the unique risks facing your business and ask yourself whether those risks are being managed effectively.

### 1. Protecting your Property

Property holdings are often a small business owner's largest asset. Therefore, for the long-term security of your small business, it is vital that you evaluate potential threats to your property and develop a plan to manage those threats. Begin by taking a complete inventory of all your assets to determine how a loss might affect your business and how much coverage you need. Property coverage can come in many forms to suit your specific needs, but a typical policy will provide the replacement cost value for your building and the actual cash value for your business property.

You have a lot weighing on your budget already, but don't make the mistake of planning for the "best case scenario" when it comes to your property coverage. Leaving your small business underinsured is a risk too great to take.

### 2. Business Interruption

The U.S. Department of Labor estimates that more than 40 percent of businesses never reopen following a disaster such as a fire or flood. Is your business prepared to weather the storm if disaster strikes? If a fire causes the [C\_Officialname] facility to be temporarily unusable, what would you do? Ideally, you would move to a temporary location while your permanent place of business is being repaired, but traditional Property Insurance does not cover this move or the loss of income while the permanent business location is being repaired. Ill-prepared businesses are often forced to completely shut down operations during repair, which can do irreparable damage to their brand and leave employees without work for extended periods of time. To mitigate this risk, consider adding Business Interruption coverage to your Property Insurance policy. This invaluable, though often

# Critical Infrastructure/Key Resources

- **Presidential Policy Directive 21 enumerated 16 Sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.**

# CI/KR Sectors

- Chemical:
  - Sector-Specific Agency: Department of Homeland Security
- Commercial Facilities:
  - Sector-Specific Agency: Department of Homeland Security
- Communications:
  - Sector-Specific Agency: Department of Homeland Security



# CI/KR Sectors

- Critical Manufacturing: Sector-Specific Agency: Department of Homeland Security
- Dams:  
Sector-Specific Agency: Department of Homeland Security
- Defense Industrial Base:  
Sector-Specific Agency: Department of Defense
- Emergency Services:  
Sector-Specific Agency: Department of Homeland Security

# CI/KR Sectors

- Energy:  
Sector-Specific Agency: Department of Energy
- Financial Services:  
Sector-Specific Agency: Department of the Treasury
- Food and Agriculture:  
Co-Sector-Specific Agencies: U.S. Department of Agriculture and Department of Health and Human Services

# CI/KR Sectors

- Government Facilities:  
Co-Sector-Specific Agencies: Department of Homeland Security and General Services Administration
- Healthcare and Public Health:  
Sector-Specific Agency: Department of Health and Human Services
- Information Technology:  
Sector-Specific Agency: Department of Homeland Security

# CI/KR Sectors

- Nuclear Reactors, Materials, and Waste:  
Sector-Specific Agency: Department of Homeland Security
- Transportation Systems:  
Co-Sector-Specific Agencies: Department of Homeland Security and Department of Transportation
- Water and Wastewater Systems:  
Sector-Specific Agency: Environmental Protection Agency



# SSA Definition

- The term "Sector-Specific Agency" (SSA) means the Federal department or agency designated under this directive to be responsible for:
  - Providing institutional knowledge
  - And specialized expertise as well as
  - Leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

# Private Sector CI/KR Impact

- **Private-sector CIKR owners and operators are responsible at the corporate and individual facility levels for risk and incident management planning, security, and preparedness investments.**
- **Other activities that form part of business and continuity of operations planning activities include:**
  - **Developing and revising business continuity and emergency management plans to address direct effects of incidents and critical dependencies and interdependencies at sector, enterprise, and facility levels.**
  - **Building increased resiliency, backup capabilities, and redundancy into business processes and systems.**

# Private Sector CI/KR Impact

- Maintaining coordination with incident management, information-sharing, and CIKR protection programs.
- Reporting CIKR status using established mechanisms for inclusion in the national common operating picture (COP).
- Developing and coordinating CIKR protective and emergency-response actions, plans, and programs.

# Private Sector CI/KR Impact

- **Guarding against insider threats.**
- **Providing technical expertise to DHS, SSAs, ESFs, and other Federal, State, tribal, and local entities.**
- **Identifying CIKR and prioritizing related protection and restoration activities.**

**IS-821.A: Critical Infrastructure Support Annex**





## Critical Infrastructure and Key Resources Support Annex

The Critical Infrastructure and Key Resources (CIKR) Support Annex describes policies, roles and responsibilities, and the concept of operations for assessing, prioritizing, protecting, and restoring infrastructure and key resources of the United States and its territories and possessions during actual or potential incidents. The annex details processes to ensure coordination and integration of CIKR-related activities among public and private incident managers and CIKR security partners within immediate incident areas as well as state and national levels. Specifically, the annex does the following:

- Describes roles and responsibilities for CIKR preparedness, protection, response, recovery, restoration, and continuity of operations relative to [National Response Framework](#) (NRF) coordinating structures and [National Incident Management System](#) (NIMS) guiding principles.
- Establishes a concept of operations for incident-related CIKR preparedness, protection, response, recovery, and restoration.
- Outlines incident-related actions (including preresponse and postresponse) to expedite information sharing and analysis of actual or potential impacts to CIKR and facilitate requests for assistance and information from public- and private-sector partners.

Read the [Critical Infrastructure and Key Resources Support Annex](#) - (PDF - 36 pages, 357 KB)

Last Published Date: August 26, 2015

# Terrorism Threat

- **Terrorism is defined by the FBI as; “The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”**

# Major Terrorism Categories

- **International\***
- **Domestic\***
- **Single Issue-Special Interest**
- **Lone wolf/microactor/homegrown violent extremist (HVE)**

**\* Defined in US Code Title 18 Section 2331**

# Potential Attack Targets

- Business
- Government
- Maritime
- Military
- First responders
- Private citizens & property
  - Public venues
  - Schools/Universities
- Religious institutions
- Transportation
- Symbolic





# The Hierarchy of the WMD Threat

- Cyber attack
- Explosives
- Biological toxins
- Industrial chemicals
- Biological pathogens
- Radiological isotopes
- Military chemical agents
- Nuclear weapons



# Al-Qaeda Business Tactic

- **Operation Hemorrhage**
  - Inflict heavy economic damage
  - Use low cost operations
  - Smaller, more frequent attacks
  - “Strategy of a thousand cuts”
    - **Object is to bleed the enemy to death.**
- **First successful on September 03, 2010.**
  - A UPS cargo plane exploded after takeoff from Dubai International Airport.



# Package Bombs

- Addressed to infamous people involved in the Crusades and Spanish Inquisition.
- One of the synagogues allegedly has gay/lesbian members.



# Hydroelectric Plant IED Attack

- July 21, 2010- Northern Russia
- Perpetrators killed two security guards to gain entry.
  - Detained & assaulted & detained to employees.
- Placed up to five IED's, four of which detonated.
  - One rendered safe.

# Hydroelectric Plant IED Attack

- Two of the plant's three generators destroyed.
  - Fire took three and a half hours to extinguish.
- Attack at a police station in a nearby town one hour prior may have been distracter/diversion event.



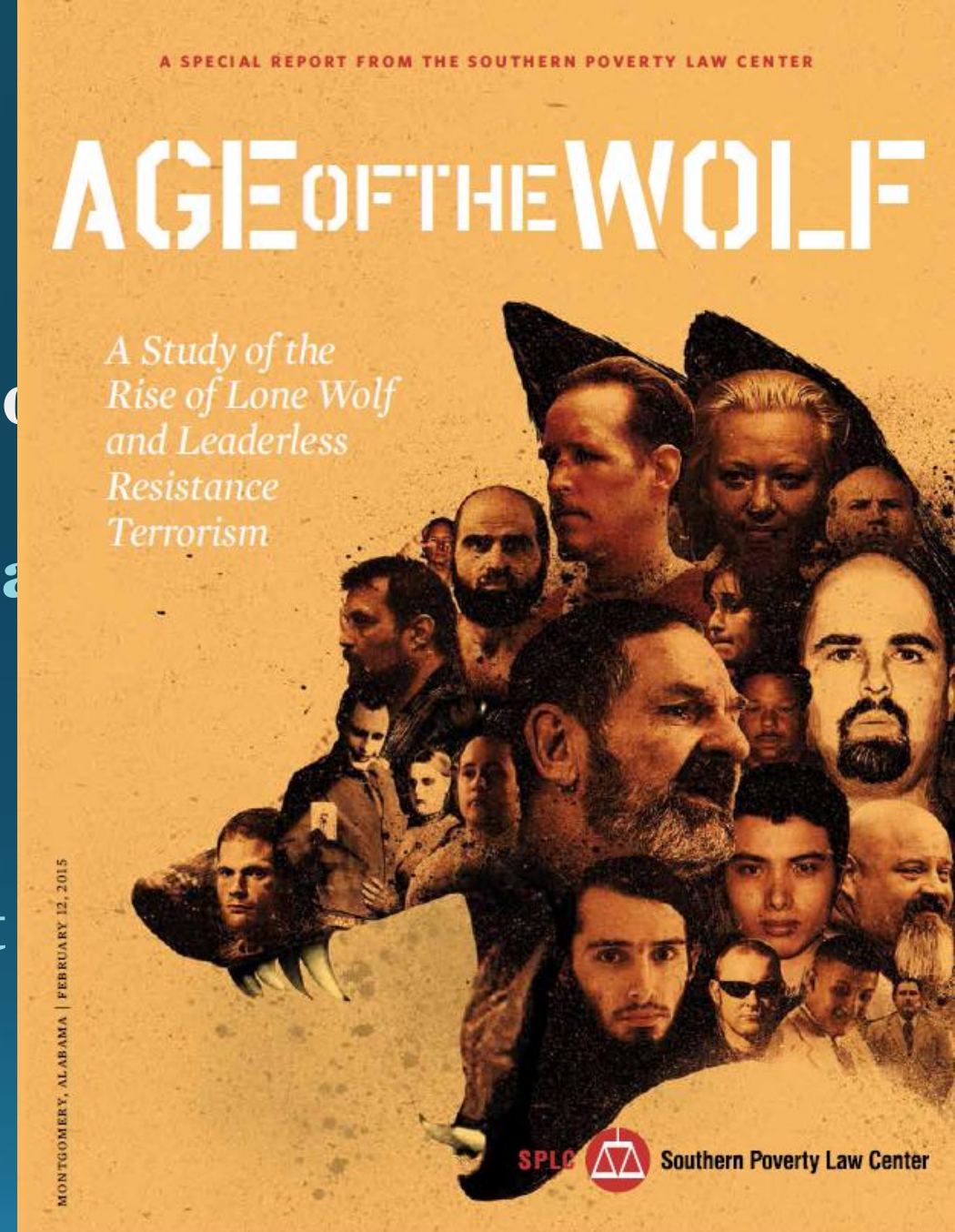
# Current Threat

- **Due to the proliferation of available radicalization material, the threat has evolved from spectacular events such as the Murrah Building and WTC attacks to smaller events carried out by individuals or smaller groups.**
- **This type of activity is difficult to track, investigate, and prevent.**
- **Magazines, books, Internet information contribute to self radicalization.**



# Current Threat

- “The Age of the Wolf”- Southern Poverty Law Center
  - 44 page document
  - Describes the rise of lone wolf and resistance terrorism
- Aka: HVE
  - Homegrown Violent Extremist





# DABIQ

14 ISSUE

1437 RAJAB

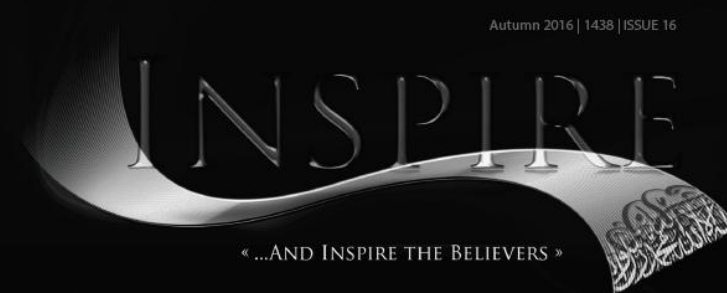


The Murtadd  
Brotherhood

oliferat

material av

ars now tak



Autumn 2016 | 1438 | ISSUE 16

الملاحم  
Al-Malahem Media

« ...AND INSPIRE THE BELIEVERS »

september

the 9/17

OPERATIONS

SPECIAL ISSUE

# Current T

- U.S. Department of Justice addressing online radicalization
- All current social media platforms have policies to prevent users from converting to extremist groups
- Once someone is radicalized, they are more private

## AWARENESS BRIEF

### Online Radicalization to Violent Extremism



#### Defining Online Radicalization

Online radicalization to violence is the process by which an individual is introduced to an ideological message and belief system that encourages movement from mainstream beliefs toward extreme views, primarily through the use of online media, including social networks such as Facebook, Twitter, and YouTube.<sup>1</sup> A result of radical interpretations of mainstream religious or political doctrines, these extreme views tend to justify, promote, incite, or support violence to achieve any number of social, religious, or political changes.

In many cases, online radicalization does not occur after viewing one video or reading one online post but happens gradually. The factors that influence a specific individual can change for him or her depending on the time or circumstance. Moreover, while the factors that influence radicalization differ from person to person, so too does the radicalization process itself. Individuals can move back and forth between stages or remain static while factors and levels interact and influence one another.

Generally, as individuals immerse themselves in online extremist content, they begin to develop a skewed sense of reality in which

their views no longer seem radical. Online interactions with like-minded individuals can substitute for an individual's physical community and create an online social environment similar to that of a gang in which deviant behavior and violence are the norm. Consumers of online extremist content can also develop or increase feelings of superiority, moral outrage, desensitization to violence, and willingness to commit acts of violence in furtherance of a particular cause.

#### How Extremists Use the Internet to Recruit and Radicalize

People and organizations worldwide have embraced the Internet because of its ease and convenience. Individuals and organizations use the Internet to share photos and videos, post news and press releases, raise money, and communicate with others. As access to the Internet continues to spread, more people own Internet-enabled devices, and as the use of social media proliferates, people are spending more time online, consuming content from a variety of sources and creating virtual communities.



**COPS**  
Community Oriented Policing Services  
U.S. Department of Justice



age brief

to recruit

directed to  
ination.

# Ohio Incident-11.28.16

- **Student expressed concern regarding lack of a place to pray on campus during entry interview.**
- **Drove car into fellow students then attacked with knife.**
- **Motive?**
- **Was it politically/socially motivated?**
- **This may be counted as a terrorist incident.**

# Threat Assessment Matrix

- **Technical feasibility**
  - **Capacity to obtain/produce material**
- **Operational practicability**
  - **Feasibility of delivering/employing material**
- **Behavioral resolve**
  - **Psychological assessment of likelihood of perpetration**



# Current Threat

- January 26, 2016
- Milwaukee man arrested after attack on police officers & silencers.
  - Target was a Masonic temple
  - Wanted to kill 30 people
- Goal to incite more attacks.
  - “I am telling you, if this is not known all over the world

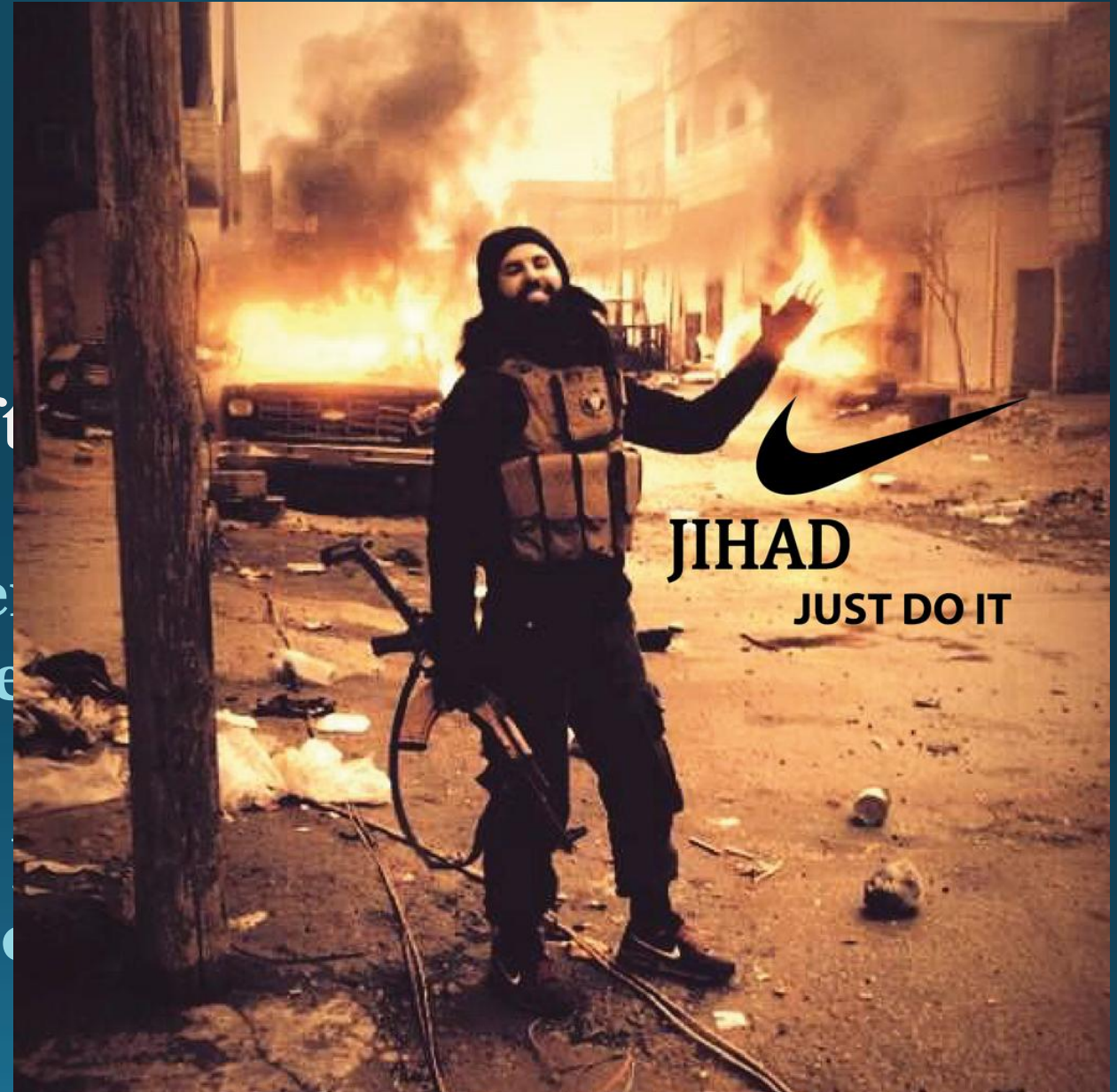


Photo credit: Twitter.com

# Current Threat

- The “Right Wing” Domestic threat is still
- Nearly 100 plots/actions have occurred and disrupted the 1995 Murrah Building bombing
- Most contemplated deaths of large numbers
  - In one case, as many as 30,000.



Source: “Terror from the Right” Special Report, SPLC



# Current Threat

- **Right Wing plans included bombing:**
  - Government buildings
  - Banks
  - Refineries
  - Utilities
  - Clinics
  - Synagogues
  - Mosques
  - Memorials
  - Bridges



Photo credit: <http://www.motherjones.com>



Photo credit: <http://www.bcbridges.org>

# Infra

- Three wing in Elk
- Ea
- Dubb tank f



<http://www.panoramio.com/photo/18929943>

ight  
e tanks  
propane.  
the



# Current T



Photo credit:  
Sedgwick County  
Sheriff's Office via AP

**AP** Associated Press

Story credit:  
<http://www.businessinsider.com/>  
and AP

- Kansas Militia disrupted.
- Three men planned to detonate four car bombs at an apartment complex where over 100 Somalis resided and that contained a mosque the day after the 2016 Election.  
Population around 27K



# Current Threat

- **Cyber attacks could compromise infrastructure.**
- **Targets include:**
  - **Power grids**
  - **Wastewater treatment plants**
  - **Oil/gas pipelines**
  - **Planes**
  - **Medical devices**



<http://www.hospira.com>

# Power Grid Cyber Attack

- **January 4, 2016-Ukraine**
- **First known hacker caused power outage perpetrated.**
  - **December 23, 2015 date of attack.**
- **Electrical substations disconnected.**
  - **Hundreds of thousands of homes without electricity.**

# Current Threat



- **Cyberterrorist goals:**
  - **Destroy, incapacitate, exploit critical infrastructure**
  - **Threaten national security**
  - **Cause mass casualties**
  - **Weaken the U.S. economy**
  - **Damage public morale/confidence**
- **May use phishing schemes to generate funds/gather sensitive information.**



## Cyber Security Starts with “You”



Photo By: © 2007 Jupiterimages Corporation

**IS YOUR COMPUTER LOCKED?**

**LOCK IT WHEN YOU LEAVE IT!**

**Keep your data safe and secure.**



**Multi-State  
Information Sharing and Analysis Center (MS-ISAC)**  
<http://www.msisac.org>



**IC<sup>3</sup>.gov Federal  
Website for  
filing formal  
reports of cyber  
attacks, &  
information  
source.**

# Cyber Attack

- **March 18, 2010**
- **Omar Ramos-Lopez, 20, fired from auto dealership in Texas.**
  - **Used a former colleagues password to hack into dealerships website.**
  - **Caused cars to be disabled, set off car horns, ordered \$130,000.00 in GPS equipment.**

# Cyber Hack

- July 21, 2015
- Jeep Cherokee
  - Air conditioning
  - Brakes all
  - Car ended
- 471,000 vehicles



mission,


Photo credit: Andy Greenberg/WIRED

<http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

# Energy Sector Cyber Attacks

- **Duke Energy**
  - Country's largest electricity Company
  - Manages three of the 16 types of infrastructure critical to human life
- **Computer system under constant attack**
  - A dozen times in the last decade foreign hackers have gained enough remote access to control the operations networks that keep the lights on.

Firefox Cyber Threat Source Descriptio...  
https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions  
Official website of the Department of Homeland Security

 **ICS-CERT**  
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME ABOUT ICSJWG INFORMATION PRODUCTS TRAINING FAQ

**Control Systems**

- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

**Cyber Threat Source Descriptions**

Cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. To protect against these threats, it is necessary to create a secure cyber-barrier around the Industrial Control System (ICS). Though other threats exist, including natural disasters, environmental, mechanical failure, and inadvertent actions of an authorized user, this discussion will focus on the deliberate threats mentioned above.

- [National Governments](#)
- [Terrorists](#)
- [Industrial Spies and Organized Crime Groups](#)
- [Hacktivists](#)
- [Hackers](#)
- [GAO Threat Table](#)

For the purpose of this discussion, deliberate threats will be categorized consistent with the remarks in the Statement for the Record to the Joint Economic Committee by Lawrence K. Gershwin, the Central Intelligence Agency's National Intelligence Officer for Science and Technology, 21 June 2001. These include: national governments, terrorists, industrial spies, organized crime groups, hacktivists, and hackers. Activities could include espionage, hacking, identity theft, crime, and terrorism.

**National Governments**

National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm US interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Among the array of cyber threats, as seen today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to U.S. critical infrastructures.

The tradecraft needed to effectively employ technology and tools remains an important limiting factor, particularly against more difficult targets such as classified networks or critical infrastructures. For the next 5 to 10 years, only nation states appear to have the discipline, commitment, and resources to fully develop capabilities to attack critical infrastructures.

Their goal is to weaken, disrupt or destroy the U.S. Their sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack the US economy, full scale attack of the infrastructure.

10:45 AM  
8/13/2015



11.23.16

# Another Cyber Twist

- Malware covertly turns PCs into eavesdropping devices.
- Headphones, earphones, and speakers can be reprogrammed from output to input.
- Countermeasures include:
  - Completely disabling audio hardware,
  - Using an HD audio driver to alert when microphones are being accessed,
  - Establishing a strict rejack policy within the industry.



# Current Threat Summary

- Domestic and international actors still pose a real threat to perpetrate an attack within the U.S.
- On-line radicalization of singular individuals/small groups are difficult to identify & track.
  - Teenagers, young children, females, and families are now more prevalent in terrorism activities.
- Continued publication of terror-based magazines provides motivation and direction for home grown violent extremists (HVE).

# Current Threat Summary

- There were 11,774 attacks worldwide in 2015, causing 28,328 fatalities\*.
  - **Constant vigilance is required to identify suspicious activity.**
- Attacks that are well planned involve target selection, surveillance, practice runs, and possibly testing security measures.
- Employers/employees should take note of and report through established procedures, any activity that may fit into any phase of attack planning.

\* Source: National Consortium for the Study of Terrorism and Responses to Terrorism

# Tactical Actions

- Although too numerous to describe in total during this Roundtable time frame, two attacks, one international, one domestic are detailed in the following slides.
- The Counter-Terrorism discipline is ever evolving; as we do better at prevention, those who would cause harm explore ways to circumvent our efforts.
- Constant vigilance, situational awareness, and communication are three methods of protection businesses can employ to deter an attack.

# Tactical Actions

- January, 2015
- 80% (140 million people) of Pakistan blacked out due to a terrorist bombing of the power grid.
  - Two transmission sites hit.
  - Two nuclear plants also knocked offline.
- Perpetrators may have found a critical focal point of the system.

# US Tactical Action

- San Jose, CA.
- 17 transformers riddled with bullets
  - Attempt to drain cooling towers
- 911 fiber optic lines also cut
- Perpetrators have never been identified



Photo credit: Jim Wilson, NY Times



# Armed Assault Tactic

- From sharp edged items through and including multiple types of explosives and firearms, the armed assault has become a tool in the terrorist toolbox.
- There is information available for preparation and response to such an event.

# On Scene Active Shooter Actions

## HOW TO RESPOND

WHEN AN ACTIVE SHOOTER IS IN YOUR VICINITY

### 1. EVACUATE

- Have an escape route and plan in mind
- Leave your belongings behind
- Keep your hands visible

### 2. HIDE OUT

- Hide in an area out of the shooter's view
- Block entry to your hiding place and lock the doors
- Silence your cell phone and/or pager

### 3. TAKE ACTION

- As a last resort and only when your life is in imminent danger
- Attempt to incapacitate the shooter
- Act with physical aggression and throw items at the active shooter

**CALL 911 WHEN IT IS SAFE TO DO SO**

## HOW TO RESPOND

WHEN LAW ENFORCEMENT ARRIVES

- Remain calm and follow instructions
- Put down any items in your hands (i.e., bags, jackets)
- Raise hands and spread fingers
- Keep hands visible at all times
- Avoid quick movements toward officers such as holding on to them for safety
- Avoid pointing, screaming or yelling
- Do not stop to ask officers for help or direction when evacuating

## INFORMATION

YOU SHOULD PROVIDE TO LAW ENFORCEMENT OR 911 OPERATOR

- Location of the active shooter
- Number of shooters
- Physical description of shooters
- Number and type of weapons held by shooters
- Number of potential victims at the location

## COPING

WITH AN

- Be aware of your surroundings as much as possible
- Take no action that could compromise the facility
- If you are in a secure area, stay there
- Attempt to evacuate as a last resort

Contact your supervisor for human resources information regarding active shooter response

CA  
IS



# Planning and Response to an Active Shooter:

## An Interagency Security Committee Policy and Best Practices Guide

November 2015



Interagency  
Security  
Committee

ing or  
ed and  
ne use

N

lves

ed to

### When law enforcement arrives:

- Remain calm and follow instructions
- Drop items in your hands (e.g., bags, jackets)
- Raise hands and spread fingers
- Keep hands visible at all times
- Avoid quick movements toward officers, such as holding on to them for safety
- Avoid pointing, screaming or yelling
- Do not ask questions when evacuating

### Information to provide to 911 operations:

- Location of the active shooter
- Number of shooters
- Physical description of shooters
- Number and type of weapons shooter has
- Number of potential victims at location

### For questions or additional assistance contact:

Your local law enforcement authorities or FBI Field office :



Department of Homeland Security  
3801 Nebraska Ave, NW  
Washington, DC 20528

## ACTIVE SHOOTER EVENTS

When an Active Shooter is in your vicinity, you must be prepared both mentally and physically to deal with the situation.



### You have three options:

#### 1 RUN

- Have an escape route and plan in mind
- Leave your belongings behind
- Evacuate regardless of whether others agree to follow
- Help others escape, if possible
- Do not attempt to move the wounded
- Prevent others from entering an area where the active shooter may be
- Keep your hands visible
- Call 911 when you are safe

#### 2 HIDE

- Hide in an area out of the shooter's view
- Lock door or block entry to your hiding place
- Silence your cell phone (including vibrate mode) and remain quiet

#### 3 FIGHT

- Fight as a last resort and only when your life is in imminent danger
- Attempt to incapacitate the shooter
- Act with as much physical aggression as possible
- Improvise weapons or throw items at the active shooter
- Commit to your actions . . . your life depends on it

The first officers to arrive on scene will not stop to help the injured. Expect rescue teams to follow initial officers. These rescue teams will treat and remove injured.

Once you have reached a safe location, you will likely be held in that area by law enforcement until the situation is under control, and all witnesses have been identified and questioned. Do not leave the area until law enforcement authorities have instructed you to do so.

# Insider Vulnerability

- **The insider threat may involve harm to physical facilities, personnel.**
- **It could also involve non-violent actions, centered round sensitive security information, trade secrets, business continuity plans, etc.**
- **Ensuring employees are trained to the level of knowledge commensurate with their duties is one method to protect valuable assets.**



# **(U//FOUO) Insider Threats**

- **(U//FOUO) Terrorism Insider Threat Indicators: The following indicators of insider threats can reflect criminal activity unrelated to terrorism or legitimate terrorism-related activities.**
  - **The presence of multiple indicators especially in combination with other situational information—should raise concerns about a terrorist insider threat.**

# **(U) Potential Indicators of the Insider Threat:**

- **(U) Attempts to gain information from employees on topics outside a questioner's area of responsibility.**
- **(U) Repeated attempts to enter restricted areas without proper credentials.**
- **(U) Unauthorized copying of sensitive files—particularly blueprints of buildings or critical systems, such as security and fire suppression systems.**
- **(U) Threats made by disgruntled employees.**

# **(U) Potential Indicators of the Insider Threat:**

- **(U) Improper use of information technology systems or repeated attempts to access restricted information.**
- **(U) Requests for irregular work schedules or attempts to be left alone in a facility.**
- **(U) Patterns of inaccurate statements or making excuses for irregular behavior.**
- **(U) Off-duty employees on the property—possibly accompanied by unknown or unauthorized individuals.**

# Insider Attack Averted

- June 8, 2015
  - Former
- Wichita air
  - Van with
- Motivated by an individual with violent jihadist



choice  
with an  
supporting

# Insider Threat

- **British Airways worker faces terror charge.**
  - **Computer specialist allegedly was plotting suicide bombings.**
    - **Including one he planned to carry out himself.**
- **Rajib Karim, 30, Bangladesh native,**
  - **Deliberately took job to further terrorist conspiracy.**
  - **Would volunteer to join flight crew if employees strike. (Which they did.)**

**boston.com**

**AP** Associated Press

**BRITISH AIRWAYS**

**March 12, 2010**



# Insider Attack

- **August 26, 2015**
- **Two NATO soldiers killed by two men wearing Afghan security force uniforms.**
- **Third “insider attack” this year.**
  - **An Army Major was killed by an insider in August of 2014.**
  - **Highest ranked US Officer to be slain in combat since the Vietnam War in 1970.**

<http://nypost.com/>

# Vulnerability & Risk Assessment

- There is much information available to businesses in assessing their risk and determining the most cost effective solutions to mitigate that risk.
- This next Program segment explores some of those resources.



# Let's Start with FEMA

- <https://www.ready.gov/business>
- Quadfold Brochure and 12 page Booklet

*Ready Business* was developed in consultation with the following organizations:

The 9/11 Public Discourse Project, ASIS International, Business Executives for National Security, The Business Roundtable, International Safety Equipment Association, International Security Management Association, National Association of Manufacturers, National Federation of Independent Business, Occupational Safety and Health Administration, Small Business Administration, Society for Human Resource Management, U.S. Chamber of Commerce.

These recommendations reflect the Emergency Preparedness and Business Continuity Standard (NFPA 1600) developed by the National Fire Protection Association and endorsed by the American National Standards Institute, the 9/11 Commission and the U.S. Department of Homeland Security.

This common sense framework is designed to launch a process of learning about business preparedness. For more information go to:

[www.ready.gov](http://www.ready.gov)



[www.ready.gov](http://www.ready.gov)



**FEMA**

Federal Emergency Management Agency  
Washington, DC 20472

## Preparing Makes Good Business Sense.

How quickly your company can get back to business after a terrorist attack or tornado, a fire or flood often depends on emergency planning done today. While the U.S. Department of Homeland Security is working hard to prevent terrorist attacks, the regular occurrence of natural disasters demonstrates the importance of being prepared for any emergency. While recognizing that each situation is unique, your organization can be better prepared if it plans carefully, puts emergency procedures in place, and practices for all kinds of emergencies. This guide outlines common sense measures business owners and managers can take to start getting ready. A commitment to planning today will help support employees, customers, the community, the local economy and even the country. It also protects your business investment and gives your company a better chance for survival.

**Every business should have a plan. Get ready now.**

## Plan to Stay in Business

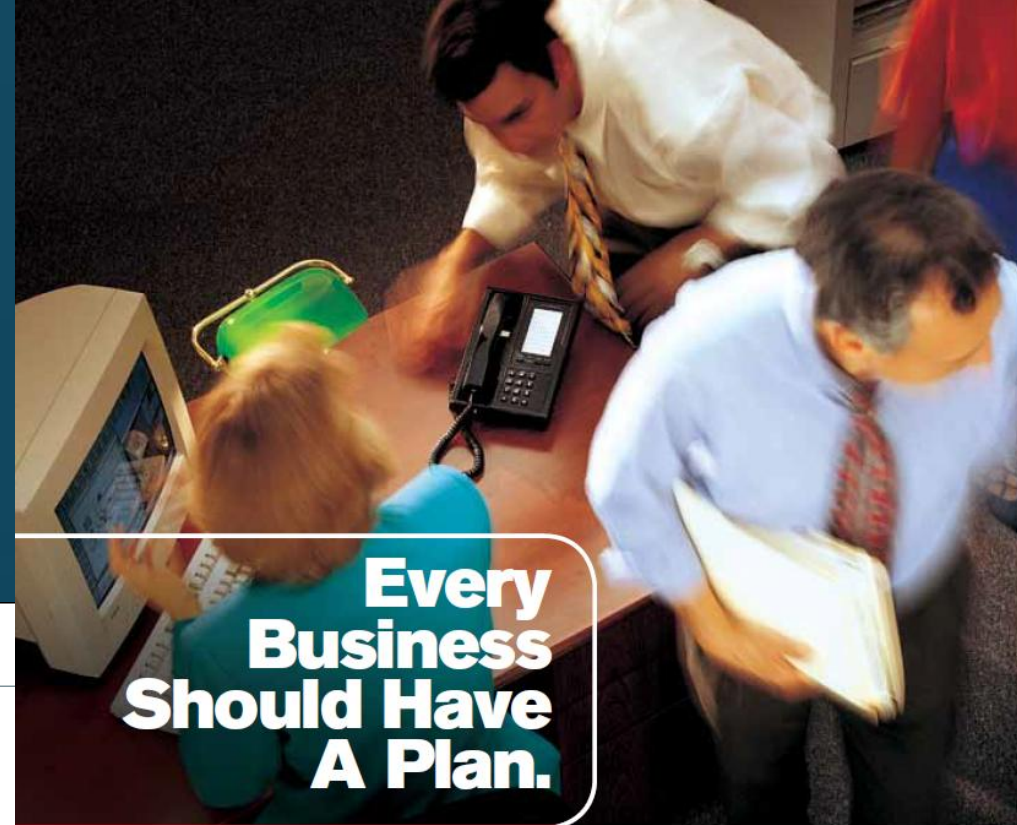
Business continuity planning must account for both man-made and natural disasters. You should plan in advance to manage any emergency. Be prepared to assess the situation, use common sense and available resources to take care of yourself, your co-workers and your business' recovery.

**Continuity Planning:** Risk assessment can be a sophisticated area of expertise that ranges from self-assessment to an extensive engineering study. Your organization's risk needs will vary according to the specific industry, size, scope and location of your individual company. Start by reviewing your business process flow chart, if one exists, to identify operations critical to survival and recovery. Carefully assess your internal and external functions to determine which staff, materials, procedures and equipment are absolutely necessary to keep the business operating. You should also establish procedures for succession of management.

Include co-workers from all levels in planning and as active members of the emergency management team. Make a list of your most important customers and proactively plan ways to serve them during and after a disaster. Also identify key suppliers, shippers, resources and other businesses you must interact with on a daily basis. A disaster that shuts down a key supplier can be devastating to your business.

Plan what you will do if your building, plant or store is not accessible. Talk with your staff or co-workers and frequently review and practice what you intend to do during and after an emergency. Just as your business changes over time, so do your preparedness needs. Review and update your plans at least annually and inform your employees of the changes.

**Emergency Planning for Employees:** Your employees and co-workers are your business' most valuable asset. Two-way communication is central before, during and after a disaster. Include emergency information in newsletters, on your company intranet, in periodic employee emails and/or other communication tools. Designate an



**FEMA**

(1) Asset or Operation at Risk	(2) Hazard	(3) Senario (Location, Timing, Magitude)	(4) Oportunities for Prevention or Mitigation	(5) Probability (L, M, H)	Impacts with Existing Mitigation (L, M, H)					(11) Overall Hazard Rating
					(6) People	(7) Property	(8) Operations	(9) Environment	(10) Entity	



# FEMA 428

- **Primer for Schools, 305 pages.**
- **First Chapter on asset value, threat/hazard/vulnerability, and risk.**
- **May be helpful in finding correlating weaknesses.**

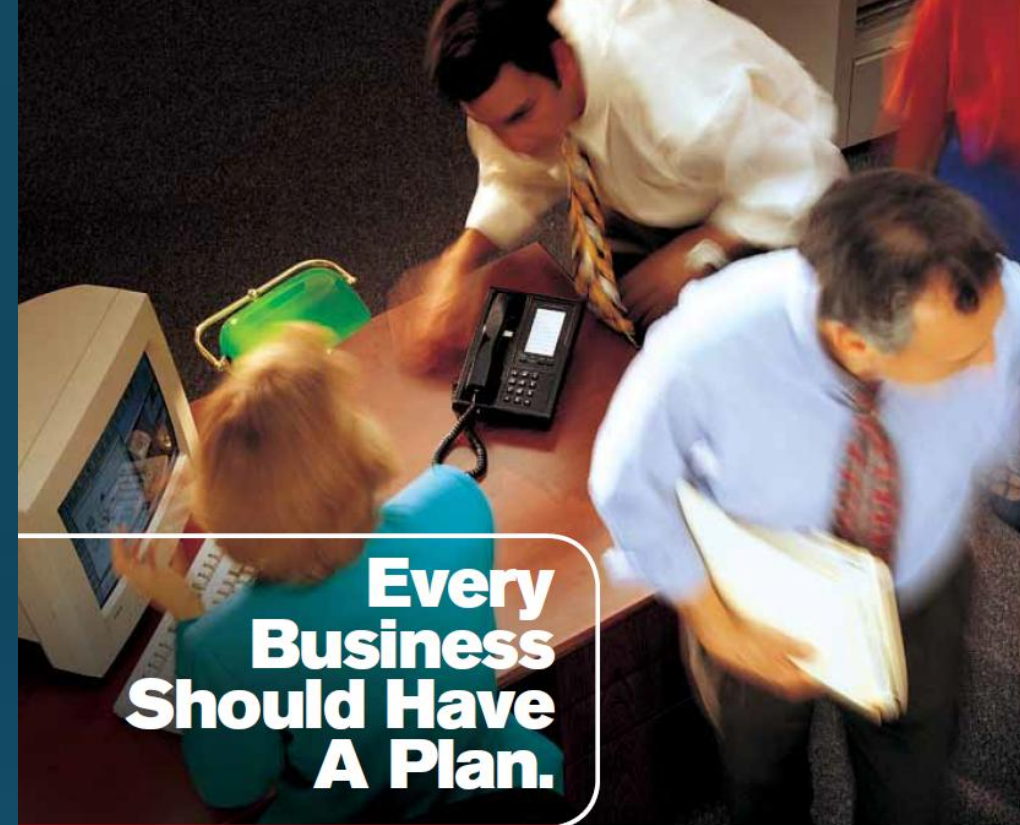
**T**his chapter presents methodologies for architects, engineers, school administrators, and state and local officials working in the building sciences field to identify the most effective mitigation measures to achieve a desired level of protection against terrorist attacks. These methodologies will help designers define asset value and evaluate vulnerability assessment information for the purpose of integrating threat/hazard into a design basis. Architects and engineers will be able to identify the best and most cost-effective terrorism mitigation measures for each building's unique security needs. Mitigation measures are conceived by the design professional and are best incorporated into the building architecture, building systems, and operational parameters, with consideration for life-cycle costs. The methodologies described in this chapter can be used for new buildings during the design process, as well as for existing buildings undergoing renovation. A key tool in the assessment process is provided for the designer in the last section of this chapter, the Building Vulnerability Assessment Checklist.

In order to create a safe school environment, many factors must be considered. Figure 1-1 depicts the assessment process presented in this primer to help each school identify the best and most cost-effective terrorism mitigation measures for its own unique security needs. Section 1.1 identifies the value of a school's assets (e.g., people, buildings, equipment, and processes) that need to be protected, recognizing that students, faculty, and staff will always be a school's most vital asset requiring protection. Section 1.2 describes how to conduct a threat/hazard assessment to identify and define the threats and hazards that could cause harm to a school. Section 1.3 discusses how to perform a vulnerability assessment to identify school weaknesses that might be exploited by a terrorist or aggressor. Combining the results of the asset value, threat, and vulnerability assessments in Sections 1.1 through 1.3, the next step in the assessment process is to perform a risk assessment (Section 1.4) to determine to what degree a school's assets are vulnerable



# Business Booklet

- 24 point document to assist with preparation, planning, response and recovery for both acts of nature and deliberate events.
- Addresses the all hazards concept.



**Every  
Business  
Should Have  
A Plan.**



**FEMA**

# Emergency

- Shelter in place
- No notice emergency
- Quickly develop a plan and train employees to respond
- Using the Risk Assessment, determine what level of preparation is required

### Emergency Supplies

Talk to your co-workers about what emergency supplies the company can feasibly provide, if any, and which ones individuals should consider keeping on hand. Recommended emergency supplies include the following:

<input type="checkbox"/>	<b>Water</b> , amounts for portable kits will vary. Individuals should determine what amount they are able to both store comfortably and to transport to other locations. If it is feasible, store one gallon of water per person per day, for drinking and sanitation
<input type="checkbox"/>	<b>Food</b> , at least a three-day supply of non-perishable food
<input type="checkbox"/>	<b>Battery-powered radio and extra batteries</b>
<input type="checkbox"/>	<b>Flashlight and extra batteries</b>
<input type="checkbox"/>	<b>First Aid kit</b>
<input type="checkbox"/>	<b>Whistle</b> to signal for help
<input type="checkbox"/>	<b>Dust or filter masks</b> , readily available in hardware stores, which are rated based on how small a particle they filter
<input type="checkbox"/>	<b>Moist towelettes</b> for sanitation
<input type="checkbox"/>	<b>Wrench or pliers</b> to turn off utilities
<input type="checkbox"/>	<b>Can opener</b> for food (if kit contains canned food)
<input type="checkbox"/>	<b>Plastic sheeting and duct tape</b> to "seal the room"
<input type="checkbox"/>	<b>Garbage bags and plastic ties</b> for personal sanitation

require your  
od of time.  
what level of

## Business Continuity Resource Requirements

Resource Category	Resource Details	Normal Quantity				
			24 hours	72 hours	1 week	Later (specify)
Managers						
Staff	Primary site, relocation site and recovery site					
Office space						
Office equipment	Furniture, phone, fax, copiers					
Office technology	Desktops and laptops (with software), printers with connectivity; wireless devices (with email access)					
Vital records, data, information	Location, backups, and media type					
Production Facilities	Owned, leased, or reciprocal agreement					
Production machinery & Equipment	Especially custom equipment with long replacement time					
Dies, patterns, molds, etc. for machinery & equipment						
Raw Materials	Single or sole source suppliers and possible alternates					
Third party services						

**Instructions:** Identify resources required to restore business operations following a disaster. Estimate the resources needed in the days and weeks following the disaster. Also review information technology disaster recovery plan for restoration of hardware and software.

# Business Emergency Plan

- Seven page document.
- Covers business continuity and disaster preparedness planning.
- Contains space for cybersecurity measures.
- Annual review prompt also included in the Plan.

## Business Continuity and Disaster Preparedness Plan

### ☐ PLAN TO STAY IN BUSINESS

If this location is not accessible we will operate from location below:

Business Name

Business Name

Address

Address

City, State, Zip Code

City, State, Zip Code

Telephone Number

Telephone Number

The following person is our primary crisis manager and will serve as the company spokesperson in an emergency.

If the person is unable to manage the crisis, the person below will succeed in management:

Primary Emergency Contact

Secondary Emergency Contact

Telephone Number

Telephone Number

Alternative Number

Alternative Number

E-mail

E-mail

### ☐ EMERGENCY CONTACT INFORMATION

Dial 9-1-1 in an Emergency

Non-Emergency Police/Fire

Insurance Provider

- Company disaster
- During reassess
- Identify their si concern
- Bought staff to minute

### SMALL BUSINESS CASE STUDY

Equity Technologies Corporation knows what it means to be prepared. Located in Mobile, Alabama, the company has long had plans and procedures in place to counter the threat posed by hurricanes and other severe weather. For instance, Equity Technologies promotes family and individual preparedness and has set up a means of communicating with employees when dangerous weather threatens. Employees carry laminated cards with contact information for supervisors and a voice recorded call-in number with updates about the company's status.

But it was the risk of Y2K related disturbances that motivated Equity Technologies to get serious about its disaster preparedness and business continuity plans. "We are a small company which does business around the world. To be competitive my clients must feel confident that we are ready for anything," said Equity Technologies Corporation's President and CEO Cathy Anderson-Giles. "It wasn't hard to put together a plan, you just have to make it a priority."

First the company identified workers to serve as key contacts for the 72-employee operation. These key contacts then established safety and security teams which analyzed Equity Technologies Corporation's entire emergency process.

The teams realized that communication between the company and the outside world was the single most important operational factor in an emergency. As a result, Equity Technologies purchased generators to power the phone system during utility outages and trained co-workers to set them up within seven minutes. Not only does the company have emergency plans and procedures in place, it has made a commitment to review the plans and tools each year at the start of the hurricane season. "We have the annual review on our corporate calendar," said Anderson-Giles. "Being prepared means being ready for any kind of emergency, be it hurricane, utility disruption or man-made disaster."





## Overview

The growth of network-connected devices, systems and services comprising the Internet of Things (IoT)<sup>1</sup> creates immense opportunities and benefits for our society. Internet-connected devices enable seamless connections among people, networks, and physical services. Network-connected devices are becoming ubiquitous in, and even essential to, many aspects of day-to-day life, from fitness trackers, pacemakers, and cars, to the control systems that deliver water and power to our homes. While the benefits of the IoT are undeniable, so too is the reality that security is not keeping up with the pace of innovation.

## Prioritizing Security

As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats. Our increasing national dependence on network-connected technologies has grown faster than the means to secure it.

These non-binding [strategic principles](#) are designed to enhance security of the IoT across a range of design, manufacturing, and deployment activities, and include relevant suggested practices for implementation. It is a first step to motivate and frame conversations about positive measures for IoT security among IoT developers, manufacturers, service providers, and the users who purchase and deploy the devices, services and systems.

### STRATEGIC PRINCIPLES FOR SECURING THE IOT

- Incorporate Security at the Design Phase
- Promote Security Updates and Vulnerability Management
- Build on Recognized Security Practices
- Prioritize Security Measures According to Potential Impact
- Promote Transparency across IoT
- Connect Carefully and Deliberately

<sup>1</sup> In this context, the term IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems.

# STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)

Version 1.0  
November 15, 2016



# DHS Chemical Facility Preparedness Program (CFATS)

- Section 550 of the DHS Appropriations Act of 2007 grants the Department the authority to regulate chemical facilities that “present high levels of security risk.” Under this authority, in April 2007, the Department promulgated the Chemical Facilities Anti-Terrorism Standards (CFATS) regulation.

# DHS Chemical Facility Preparedness Program (CFATS)

- Facilities that may be required to comply with at least some provisions of the CFATS regulation will largely fall into the following categories:
- Chemical manufacturing, storage and distribution;
- Energy and utilities;
- Agriculture and food;
- Paints and coatings;
- Explosives;
- Mining;
- Electronics;
- Plastics; and
- Healthcare.

# **DHS Chemical Facility Preparedness Program (CFATS)**

- **Three chemical security issues identified in the CFATS Program:**
- **Sabotage, theft or diversion, release**
- **16 page Appendix lists of chemicals of interest.**

**DHS Chemical Facility Anti-Terrorism Standards  
(CFATS)**

**<http://www.dhs.gov/chemical-facility-anti-terrorism-standards>**

# Active Shooter Guide

- **No one wants to have their place of business involved in this type of event.**
- **With the increase in micro-actors, self radicalized individuals, and people acting as a result of perceived wrongs these types of events have increased in frequency.**
- **One preparatory document has been published by the Interagency Security Committee, part of DHS.**

<https://www.dhs.gov/interagency-security-committee>



# Interagen

- On October 5, 1995, the bombing of the President Clinton Library and the Interagency Security Committee continuing government facilities.
- Prior to 1995, standards did not exist for government facilities.



## Planning and Response to an Active Shooter:

An Interagency Security Committee  
Policy and Best Practices Guide

November 2015



Interagency  
Security  
Committee

ee

Oklahoma City  
building,  
1997, creating  
to address  
deral

standards did  
not exist

# Local Assets

- Fire
- Police
- EMS
- Public Health
- Public Works
- Emergency Management
- City-Town Manager-Mayor



Photo credit: <http://www.rand.org/>

# Summary

- **Homegrown violent extremists pose a significant threat.**
  - **Women, children now frequently involved.**
- **Attack patterns occurring in multiples, both in vicinity of each other and at separate locations.**
  - **First attack may be diversion or to draw resources to area for follow on actions.**