Is your Business at Risk?
Terrorism in the Workplace
Housekeeping

• Exits
• Rally points
• Cell phones
• Facilities
Free OSHA 8-Hour Emergency Response Awareness Annual Refresher

Tuesday, September 26, 2017
8:15 am - 4:30 pm

OVERVIEW: This 8-hour program meets the requirements of Hazardous Waste Site Worker Refresher Training 29 CFR 1910.120(e)(8) & Emergency Responder Refresher Training 29 CFR 1910.120(d)

DOWNLOAD THE FLYER HERE
Agenda

- Threats/Tactical actions
- Vulnerability assessment
- Prevention/Protection/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 riguer in the emergency response community.
  - Domestic and international groups would harm and have harmed the US for a variety of reasons.
5 Common Threats Small Businesses Face

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

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...
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. Leaking your small business uninsured 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 [Official name] 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.
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.
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
Private Sector CI/KR Impact

• Private-sector CI/KR 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 CI/KR protection programs.
• Reporting CI/KR status using established mechanisms for inclusion in the national common operating picture (COP).
• Developing and coordinating CI/KR 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 CI/KR and prioritizing related protection and restoration activities.
CRITICAL INFRASTRUCTURE AND KEY RESOURCES

Critical infrastructure are the assets, systems, and networks, whether physical or virtual, 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.

Sharing Information with the Private Sector
Critical Infrastructure Sector Partnerships

Because the private sector owns and operates a vast majority of the nation's critical infrastructure, partnerships between the public and private sectors that foster integrated, collaborative engagement and interaction are essential to maintaining critical infrastructure security and resilience. These partnerships create an environment to share critical threat information, risk mitigation, and other vital information and resources.

The Department of Homeland Security, National Protection and Programs Directorate's Office of Infrastructure Protection (IP) leads the coordinated national effort with public- and private-sector critical infrastructure partners to enhance the security and resilience of the nation's critical infrastructure.

Sector Partnership Structure

Critical Infrastructure Partnership Advisory Council
National Protection and Programs Directorate

NPPD’s vision is a safe, secure, and resilient infrastructure where the American way of life can thrive. NPPD leads the national effort to protect and enhance the resilience of the nation’s physical and cyber infrastructure.

- View NPPD at a Glance (PDF - 2 pages, 1 MB)
- View the National Protection and Programs Directorate Organizational Chart (PDF - 1 page, 65.39 KB)
- Learn more about the National Infrastructure Protection Plan (NIPP)

NPPD Vision and Mission
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 critical infrastructure and key resources of the United States and its territories and possessions during actual or potential domestic incidents. The annex details processes to ensure coordination and integration of CIKR-related activities among a wide array of public and private incident managers and CIKR security partners within immediate incident areas as well as at the regional 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 the National Response Framework (NRF) coordinating structures and the 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)
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/micro-actor/homegrown violent extremist (HVE)

* Defined in US Code Title 18 Section 2331
Special Interest-Single Issue

• Earth Liberation Front

• Animal Liberation Front

• Stop Huntingdon Animal Cruelty (SHAC)

• Anti-abortion groups
S.H.A.C. Group

• Targeted both Huntingdon Life Sciences and their suppliers.
• Performed tests on animals.
• S.H.A.C. ceased their activities in 2014.

Photo credit:https://en.wikipedia.org/w/index.php?curid=22000454
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 the 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 leaderless resistance terrorism

• Aka: HVE
  • Homegrown Violent Extremist
Current Threat

• U.S. Department of Justice has issued an awareness brief addressing online radicalization.
• All current surveillance efforts are geared towards detecting and preventing potential recruits to promote violent extremism.
• Once someone expresses interest, they are directed to more private areas to continue indoctrination.

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. 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.
Current Threat

• January 26, 2016
• Milwaukee man arrested after buying guns & silencers.
  • Target was a Masonic temple.
  • Wanted to kill 30 people.
• Goal to incite more attacks.
  • “I am telling you, if this hit is executed, it will be known all over the world.”

Photo credit: Twitter.com
Current Threat

• The “Right Wing” Domestic threat is still very real.

• Nearly 100 plots/actions have occurred and disrupted the 1995 Murrah Building bombing.

• Most contemplated deaths of large numbers of human beings.
  • 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
Infrastructure Target

• Three rectangular steel tanks with a height of 152 feet, and a span of 80 feet. The tanks were in Elk Grove, California.
• Each tank held 12 million gallons of liquid propane.
• Dubbed "the largest liquid propane storage tank in the world".
Current Threat:

- Kansas Militia's bombing plot 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
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 avionics technician arrested
  - Wichita airport
  - Van with VBIED weapon of choice
  - Motivated by foreign terrorist organizations

Source: Associated Press/Homeland 1
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.)
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/
Insider Attack

• June 11, 2017

• Afghan soldier opens fire on American troops
  • Second insider attack this year
    • In March, three soldiers were wounded when an Afghan soldier opened fire within the confines of a U.S. Special Operations base in Helmand Province.

• Three killed

• Attacker also killed

Multiple sources: The Washington Post, BBC, ABC News, Aljazeera
Current Threat

- Cyber attacks could compromise infrastructure.

- Targets include:
  - Power grids
  - Wastewater treatment plants
  - Oil/gas pipelines
  - Planes
  - Medical devices

http://www.hospira.com
THE PERSISTENT TERROR THREAT TO THE UNITED STATES

In the past 12 months...

39 HOMEGROWN JIHADIST CASES in 20 STATES for...

☐ PLOTS TO ATTACK
☐ OVERSEAS TRAVEL
☐ FINANCIAL SUPPORT
☐ LYING TO AUTHORITIES
☐ WEAPONS CHARGES

HOMELAND SECURITY COMMITTEE

TERROR THREAT SNAPSHOT
MAY 2017
ISIS-LINKED PLOTS AGAINST THE WEST SINCE 2013

199

21

OF THESE, 63 CASES RESULTED IN ATTEMPTED OR SUCCESSFUL ATTACKS

14 TIMES MORE TIMESヒの内訳は以下の通り。

44 TIMES

AVG.

AVG.

HOMEGROWN JIHADIST CASES IN AMERICA SINCE 9/11

= 209 TOTAL

HOMELAND.HOUSE.GOV
Religious Dates

• Ramadan, 30 day period of fasting and reflection for Muslims has been called upon by ISIL for its followers to wage “all-out war” on the “infidels” of the West.

• Same request was made in 2016; results:
  • The final global body count after the month-long rampage was 421 dead and 729 wounded.
Religious Dates

- Suicide explosion at church in Alexandria, Egypt, 32 dead
- Ice cream shop targeted in Baghdad, 29 killed
- Rush hour truck bomb in Kabul claims 90+ lives
- London Bridge attack with vehicle and knives
- Police Officer attacked with hammer outside Notre Dame Cathedral in Paris
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.

http://arstechnica.com/
Bank System Cyber Hack

• May 1, 2016
• 81M stolen from Bangladesh’s Central Bank.
• Hackers broke into the “Rolls-Royce of payment networks”.
  • SWIFT- Society for Worldwide Interbank Financial Telecommunication.
• May 13, 2016 another heist occurred, same system, bank/amount not named.
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”

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

IC³.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, steering wheel, transmission, brakes all able to be manipulated.
- Car ended up in a ditch.
- 471,000 vehicles

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.

Sources: The Associated Press & The News & Observer
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
- Hacktists
- 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. Garshwin, the Central Intelligence Agency’s National Intelligence Officer for Science and Technology, 21 June 2011. These include national governments, terrorists, industrial spies, organized crime groups, hacktists, 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 lower-level nuisance web page delacetions to espionage and serious disruption with less 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, destruction of infrastructure to attack the U.S. economy, full-scale attacks on the infrastructure.
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 rejacking policy within the industry.
May 04, 2017
Alert Number
1-050417-PSA

Questions regarding this PSA should be directed to your local FBI Field Office.

Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE
E-MAIL ACCOUNT COMPROMISE
THE 5 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to Business E-mail Compromise (BEC) PSAs 1-012215-PSA, 1-082715-PSA and 1-061416-PSA, all of which are posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data as of December 31, 2016.

DEFINITION
Business E-mail Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The E-mail Account Compromise (EAC) component of BEC targets individuals that perform wire transfer payments.

The techniques used in the BEC/EAC scam have become increasingly similar, prompting the IC3 to begin tracking these scams as a single crime type in 2017.

The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim’s normal business practices. The scam has evolved to include the compromising of legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfer of funds.
International Cyber Hack

- May 12, 2017- 0324 hours
- WannaCry ransomware attack
- 150 countries, >200,000 people victimized as of 05.17.17
  - 40 hospitals in UK affected
- National Security Agency developed tool dumped on line by a group calling itself the Shadow Brokers

Source: USA TODAY TALKING TECH
International Cyber Hack

• “Kill switch” found by a 22 year old British self taught computer worker
  • Other variations observed on May 14

• Microsoft issued patch for vulnerability on March 14, 2017

• Prevention: Install/allow patches for installed software
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 1,441 attacks worldwide in 2016, causing 14,356 fatalities*.

• 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.

Tactical Actions

• Although too numerous to describe in total during this session’s time frame, several actual events are described throughout the rest of the Program.

• 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.
• San Jose
• 17 transformers burn down around
  • Attempted to drain cooling oil, causing failure.
• 911 fibrates
• Perpetra

Photo credit: Jim Wilson, NY Times

Source: http://www.wnd.com/
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

### 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
Planning and Response to an Active Shooter:
An Interagency Security Committee Policy and Best Practices Guide

November 2015
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

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

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.
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

Preventing 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 recommends that public and private organizations develops plans to prevent terrorist attacks, regular occurrences of natural disasters demonstrate the importance of being prepared for any emergency. While recognizing that each situation is unique, your organization can be better prepared if it plans ahead, 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 worldwide and regional disasters. You should plan in advance to manage any emergency. Be prepared to assess the situation, make sound decisions, and take immediate action to take care of yourself, your customers, and your business property.

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 assessment should be based on its own experience and the risk-based methodology of the Continuity Management Guide. The Continuity Management Guide describes the risk assessment methodology.

Every Business Should Have A Plan.

FEMA
Federal Emergency Management Agency
Washington, DC 20575

www.ready.gov
## Risk Assessment Table

<table>
<thead>
<tr>
<th>(1) Asset or Operation at Risk</th>
<th>(2) Hazard</th>
<th>(3) Scenario (Location, Timing, Magnitude)</th>
<th>(4) Opportunities for Prevention or Mitigation</th>
<th>(5) Probability (L, M, H)</th>
<th>Impacts with Existing Mitigation (L, M, H)</th>
<th>(11) Overall Hazard Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

- Water, 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.
- Food, at least a three-day supply of non-perishable food.
- Battery-powered radio and extra batteries.
- Flashlight and extra batteries.
- First Aid kit.
- Whistle to signal for help.
- Dust or filter masks, readily available in hardware stores, which are rated based on how small a particle they filter.
- Moist towelettes for sanitation.
- Wrench or pliers to turn off utilities.
- Can opener for food (if kit contains canned food).
- Plastic sheeting and duct tape to "seal the room".
- Garbage bags and plastic ties for personal sanitation.

• Shelter in place
• No notice emergency
• Quickly develop an escape route
• Using the Risk Assessment tool to require your employees to re-examine what level of preparedness

• Require your employees to re-examine what level of preparedness

• Require your employees to re-examine what level of preparedness
### Business Continuity Resource Requirements

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

**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 Continuity Plan

Business Impact Analysis
• Develop questionnaire
• Conduct workshop to instruct business function and process managers how to complete the BIA
• Receive completed BIA questionnaire forms
• Review BIA questionnaires
• Conduct follow-up interviews to validate information and fill any information gaps

Recovery Strategies
• Identify and document resource requirements based on BIAs
• Conduct gap analysis to determine gaps between recovery requirements and current capabilities
• Explore recovery strategy options
• Select recovery strategies with management approval
• Implement strategies

Plan Development
• Develop plan framework
• Organize recovery teams
• Develop Relocation Plans
• Write business continuity and IT disaster recovery procedures
• Document manual workarounds
• Assemble plan; validate; gain management approval

Testing & Exercises
• Develop testing, exercise and maintenance requirements
• Conduct training for business continuity team
• Conduct orientation exercises
• Conduct testing and document test results
• Update BCP to incorporate lessons learned from testing and exercises

Business Continuity Planning Process Diagram - Text Version

When business is disrupted, it can cost money. Lost revenues plus extra expenses means reduced profits. Insurance does not cover all costs and cannot replace customers that defect to the competition. A business continuity plan to continue business is essential. Development of a business continuity plan includes four steps:

• Conduct a business impact analysis to identify time-sensitive or critical business functions and processes and the resources that support them.
• Identify, document, and implement to recover critical business functions and processes.
Prepare My Business for an Emergency

Businesses can do much to prepare for the impact of the many hazards they face in today’s world including natural hazards, human-caused hazards or technology related hazards.

- Natural hazards could be a flood, hurricane, tornado, earthquake or a widespread serious illness such as the H1N1 flu virus pandemic.
- Human-caused hazards include accidents, acts of violence by people and acts of terrorism.
- Examples of technology-related hazards are the failure or malfunction of systems, equipment or software.

DHS sponsors a resource called “Ready Business” to assist businesses in developing a preparedness program by providing tools to create a plan that addresses the impact of many hazards. The direction recommended is to adopt a standard for Disaster/Emergency Management and Business Continuity Programs called an “all hazards approach.”
Start and grow your business.

Whether you’re already up and running or just getting started, we can help. Come take a look how.

LET'S GO
SBA Offers Ten Cybersecurity Tips

• Protect against viruses, spyware, and other malicious code
• Secure your networks
• Establish security practices and policies to protect sensitive information
• Educate employees about cyberthreats and hold them accountable

https://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips
SBA Offers Ten Cybersecurity Tips

• Require employees to use strong passwords and to change them often
• Employ best practices on payment cards
• Make backup copies of important business data and information
SBA Offers Ten Cybersecurity Tips

• Control physical access to computers and network components
• Create a mobile device action plan
• Protect all pages on your public-facing websites, not just the checkout and sign-up pages
Managing a Business

- Running a Business
- Leading Your Business
- Growing Your Business
- Business Law & Regulations
- Business Guides by Industry
- Exporting
- Closing Down Your Business

Cybersecurity

- Introduction to Cybersecurity
- Protect Against Ransomware
- Top Ten Cybersecurity Tips
- Top Tools and Resources for Small Business Owners
- Social Media Cyber-Vandalism Toolkit
- Additional Cybersecurity Resources

Top Ten Cybersecurity Tips

Please read this advisory in order to protect your small business from ransomware. The following tips will also help secure your small business:

1. Protect against viruses, spyware, and other malicious code
   Make sure each of your business's computers are equipped with antivirus software and antispyware and update regularly. Such software is readily available online from a variety of vendors. All software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install updates automatically.

2. Secure your networks
   Safeguard your Internet connection by using a firewall and encrypting information. If you have a Wi-Fi network, make sure it is secure and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

3. Establish security practices and policies to protect sensitive information
   Establish policies on how employees should handle and protect personally identifiable information and other sensitive data. Clearly outline the consequences of violating your business's cybersecurity policies.

4. Educate employees about cybersecurity and hold them accountable
   Educate your employees about online threats and how to protect your business’s data, including safe use of social networking sites. Depending on the nature of your business, employees might be introducing competitors to sensitive details about your firm’s internal business. Employees should be informed about how to post online in a way that does not reveal any trade secrets to the public or competing businesses. Hold employees accountable to the business's Internet security policies and procedures.

5. Require employees to use strong passwords and to change them often
   Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Title</th>
<th>Description</th>
<th>View Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEATURED</td>
<td>SBA's All Small Mentor-Protégé Program</td>
<td>This tutorial is designed to help you answer the question, &quot;Is SBA's All Small Mentor-Protégé Program a good fit for my business?&quot; You will be provided relevant details to inform the answer to...</td>
<td>GO TO COURSE</td>
</tr>
<tr>
<td>FEATURED</td>
<td>Taking Your High-Tech Product to Market</td>
<td>Your product or service is on the cutting edge of technology, a game changer. Now you need to find the best way to get your breakthrough to market. This course will introduce you to the product...</td>
<td>GO TO COURSE</td>
</tr>
<tr>
<td>FEATURED</td>
<td>Understanding Your Customer</td>
<td>Knowing your customer is a vital part of effectively selling your product or service. This course will introduce you to tools and resources that will help you understand your customer and increase...</td>
<td>GO TO COURSE</td>
</tr>
<tr>
<td></td>
<td>ANC Business Guide: 8(a) Business Development Program</td>
<td>This module is designed to inform and educate ANCs (Alaska Native Corporations) about the 8(a) Program.</td>
<td>GO TO COURSE</td>
</tr>
</tbody>
</table>
Cybersecurity for Small Businesses

This self-paced training exercise provides an introduction to securing information in a small business. Topics include: defining cybersecurity, explaining the importance of securing information through best cybersecurity practices, identifying types of information that should be secured, identifying the types of cyber threats, defining risk management, and listing best practices for guarding against cyber threats.

Duration: 00:30:00

Text-based accessible version

BEGIN COURSE

System Requirements:
Acrobat Reader, Adobe Flash Player
Due to Flash limitations, some courses will only play in iOS tablets or mobile devices with additional software installation

Other Courses You May Like

Get Local Assistance
Counseling, mentoring, and training from an SBA District Office, SCORE Business Mentor, Small Business Development Center or Women's Business Center in your area.
DHS Chemical Facility Preparedness Program (CFATS)

• The Chemical Facility Anti-Terrorism Standards (CFATS) program identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with these chemicals.

• 16 page Appendix of chemicals of interest.

• Concern of sabotage, theft, release.

DHS Chemical Facility Anti-Terrorism Standards (CFATS)
http://www.dhs.gov/chemical-facility-anti-terrorism-standards
Local Assets for Preparation/Response

- Fire
- Police
- EMS
- Public Health
- Public Works
- Emergency Management

Photo credit: http://www.rand.org/
Summary

All types of businesses need to be prepared for interruptions.

Natural causes, deliberate acts, attacks from within and industrial espionage are areas of vulnerability.

Performing a risk assessment and mitigation plan may contribute to continuity of operations and/or rapid recovery and return to production.
Summary

- A variety of resources are available:
- FEMA
- DHS
- SBA all offer guidance on preparation and response.

Questions?
Evaluation Information

Bob Zalewski

bzalewski@nhcosh.org