

PEPtalk

1st Quarter 2009



A Networking Organization of Professionals Involved In Planning For Emergencies And Disasters. www.pepkc.org

Presidents Corner

I am very proud to say that we have had a very successful PEP Year thus far. Over the last three months PEP has continued to help foster a sense of preparedness that goes far beyond the surface. In November, we hosted a fantastic presentation on Earthquake Preparedness. For that session, I would like to thank Steve Hannah for suggesting the topic and delivering a fantastic speaker.

By January, we were able to have Tom Munoz and Jayme Rick talk about Designing an Effective Emergency Operations Center (EOC). Their perspective and unique experience at Sprint were an added value to our general membership.

I also am excited to announce that PEP is currently working with a group of students from Johnson County Community College on an overhaul of the PEP web site. The work on the PEP web site is serving as a class project for these students and is an excellent example of PEP's far reaching presence in the community. The project should be completed in the next few weeks and rolled out in the late spring. As an organization, we are also appreciative of Johnson County Government's cooperation in letting PEP continue to host their web site for free. I would like to thank Nick Crossley for his continue help and support related to the PEP web site.

Moreover, because PEP is so well respected as a leading public-private organization, I was asked to provide the key note address at the Partners for Emergency Preparedness Conference this April. I will be highlighting the strengths of PEP as an organization and community partner. I am proud to be representing this organization and to speak to the great things it has accomplished through unmatched public-private partnership.

I would also like to encourage everyone to note in the newsletter the information about the upcoming election process as well as a reminder about the code of ethics as members. These are important items that need the full support of the membership.

We have two more great general sessions coming up in March and May as well as the KC Metro BC/DR Conference in July. Go ahead and mark your calendars....we'll see you there!

Adam Crowe
PEP President

PEP Meetings

March 19, 2009

PEP General Session
Severe Weather
Swiss RE • RSVF

April 9, 2009

PEP Board of Directors
Swiss RE

May 14, 2009

PEP Board of Directors
Swiss RE

May 21, 2009

PEP General Session
Virtual Workplace
Recovery
TBD

June 11, 2009

PEP Board of Directors
Swiss RE

Inside PEPtalk

[In the Crosshairs / Page 2-3](#)

[How to Design An Effective EOC / KC Metro BC/DR Conference / Page 4](#)

[Choosing Secure Passwords / Page 5](#)

[PEP Code of Ethics / PEP Annual Election / Page 6](#)

[Business Continuity Conferences and Training 2009 / Page 7](#)

[Directory of Officers & Directors / Call for PEPtalk Articles / Page 8](#)

IN THE CROSSHAIRS by Will Gunther

Reprinted with permission from the November 2008 issue of Risk Management Magazine.
Copyright 2008 Risk and Insurance Management Society, Inc. All rights reserved.

In June of this year, Wesley Neal Higdon was sent home from his job at the Atlantis Plastics plant in Henderson, Kentucky following a dispute with a co-worker. Higdon got a gun from his house, returned to work and fatally shot five co-workers, including his supervisor and the co-worker he had originally argued with. He injured another co-worker before finally turning the gun on himself.

Even more tragic than the lives lost at Atlantis Plastics is the fact that workplace shootings like this occur again and again. Predicting who will become the next shooter is extremely difficult as the warning signs often emerge only after the fact, as was the case with Higdon. But there are proven methods to prevent or limit the impact of a shooting once it has begun that can save lives and protect a company's fortunes.

In terms of security, there are a few simple methods that can thwart a potential workplace violence incident. Whether a shooting is the result of a dispute or domestic violence, the shooter has usually been to the workplace on several occasions. They will know where the guards are, where the person they are looking for is usually located, and where key personnel offices are. Expensive security measures and metal detectors will not deter the emotional shooter.

Some strategies that can stop the crisis before it starts combine simple procedures and existing security technology. The first is to provide the receptionist with a coded phrase such as "Mr. X is here to see you as soon as humanly possible" that will allow security to be alerted without alerting the shooter that he or she has been identified. This is important because a shooter will usually start shooting from the moment that he or she is identified or feels threatened. The receptionist might also be instructed to use the public address system to announce that a caller is holding on line eight or another fictitious number beyond the number of lines that actually exist.

Another effective measure is to move the guard away from the metal detector. Companies that have metal detectors often post a security guard near the detector so they can observe what items a visitor removes before entering. The problem is that this forces the shooter to interact with the guard immediately and possibly begin shooting. Stationing guards away from the metal detector and allowing them to observe visitors on a monitor is far more effective. Now the shooter must go through the metal detector or attempt to engage the armed guard from a greater distance. This allows the guard and the employees more time to react. In most active shooter situations, the shooter has planned the attack and has visualized how things will unfold many times. Once the shooter is confronted in a way that is unexpected, however, he or she becomes reactive and their plan starts to unravel. If a shooting event cannot be prevented, this is the next best way to limit casualties.

Shooter on the Premises So what can be done about an active shooter? The main priority is to minimize the shooter's ability to create mass casualties. The best way to achieve this is to isolate him or her from the workers and create an environment that assists the police and medical staff to respond quickly enough that the shooter is on the defensive in the shortest amount of time possible.

The first part of the plan is to move into the first available room and lock the door. If the door does not lock or if there is a window near the door lock, furniture should be placed against the door. The lights should be turned out and the blinds drawn shut in order to limit visibility from outside the room. Everyone should move away from the door so the shooter cannot shoot through the door and create more injuries. *Continued on page 3*

In The Crosshairs, continued...

Every room should contain the following simple items: luminous (glow-in-the-dark) tape, a grease pencil, a detailed diagram of the building, gauze or other material designed to stop bleeding, a thermal blanket and a flashlight. These items should be placed in the same spot in every room so the staff can easily find the items they need.

The luminous tape can be used to create a code for law enforcement that is visible during the day or night. The company security manager should work with local law enforcement to make sure the police understand the codes. By using codes such as a "T" to indicate everyone in the room is unharmed, or a "V" to indicate there are injured in the room, police can then determine the priority for evacuation. These symbols can speed the time for police response exponentially because there is information flow between the victims and law enforcement from the minute law enforcement arrives on scene.

In most cases, the initial information to law enforcement is overwhelming and confusing. Often the police do not know how many gunmen are inside or if there are hostages. This slows the process for response because police have to wait for additional forces and gather better intelligence; meanwhile, the shooter is continuing the rampage inside. If police can see the luminous tape on the windows, they can assume that the shooter is probably not in that room. This will allow them to immediately react and bring the victims out of those rooms. The sooner the police can reach victims, the sooner they can debrief them, determine the situation and respond. This alone can save lives.

The grease pencil is important for various reasons. First and foremost, it can be used to write a cellular phone number on the window. This will allow emergency or law enforcement personnel to contact the victim inside. Phone numbers transcend most languages, making this an effective tool in any part of the world. If luminous tape codes and other measures do not work, everyone understands the implied request to call the phone number written on the window. When a victim is able to provide law enforcement with timely information, law enforcement officials can react faster to the situation and limit the casualties.

The grease pencil can also be used to write the number of casualties and how many victims are critical. This allows the police to move directly to the rooms with critically injured first. It also allows medical personnel to contact the victims inside to assess their condition and make preparations for treatment. In many cases, medical personnel can provide simple life-sustaining advice by phone to those attempting to render first aid until medical professionals are able to reach the victims.

Having a detailed diagram of the building in every room allows victims with cell phones to explain their exact location to law enforcement as well. Not only does this aid in rescuing wounded victims but it can also help police determine the shooter's location. For example, the victim can describe where they are and that they can hear gunshots from their location. This will allow victims to report locations in such a way that outside personnel understand. For example, "I am on the third floor of the north side of the building, three rooms from the eastern edge of the building."

The gauze can be utilized to stop or slow the bleeding of injured victims. Even the plastic on the gauze package can be used to seal a sucking chest wound (lung injury) caused by gunshots. The exact techniques for this can be taught by the corporate health personnel and are not invasive. This means the liability is minimal and the lifesaving factor is greatly increased.

The thermal blanket can also help sustain those victims that succumb to shock due to their injuries and the flashlight can be used while treating the wounded or even as another form of signaling device, if necessary.

In summary, a simple and effective plan can greatly increase the speed at which police can respond and place the shooter in the defensive mode much sooner, which in turn decreases the time victims must wait for medical treatment. These techniques not only save lives but greatly decrease any financial losses to the company stemming from possible liability claims. Fewer casualties mean fewer cases brought against the company and the fact that a detailed, quality plan was in place demonstrates the depth of a company's concern for its employees.

Will Gunther is a risk management and disaster preparedness consultant and a former military special operations member with 20 years of experience in crisis situations, personnel evacuations and intelligence. He has authored several articles on preparedness and security issues and has worked on projects for various U.S. government organizations, large corporations and small businesses.

How To Design An Effective EOC

At our January 2009 General Session, Tom Munoz and Jayme Rick from Sprint provided an informative presentation on designing an Emergency Operations Centers (EOCs). In case you missed it, here's a summary of their presentation.

An EOC is the physical location from which response teams and municipal, county, state and federal officials provide direction and exercise control in an emergency or disaster.

The EOC serves as the central place for

- Providing direction and control of the incident
- Developing an assessment of the situation
- Directing coordination of resources
- Establishing priorities of the response and recovery
- Enforcing existing policies or creating ad hoc policies
- Gathering information
- Disseminating information



Keep personnel to include in the EOC include HR, Facilities, Security, Information Technology and Public Relations. Since each business has different drivers (e.g. regulatory environment), there is no single list of players. Every business will be different.

The type of EOC you choose depends on your organization. They may vary from a multi-purpose conference room to a dedicated facility to a mobile vehicle.

Matt May, of the Johnson County Emergency Management Agency can give you a virtual tour of the of their EOC on YouTube: <http://www.youtube.com/watch?v=gPoizlhAEOQ>

KC Metro BC/DR Conference • July 16, 2009

Calling all PEP members to mark your calendar for the second annual "KC Metro BC/DR Conference" scheduled on July 16th, at the Johnson County Emergency Management and Homeland Security Offices at 111 South Cherry, Olathe Kansas. Last year we had over 100 attendees, with (7) presentations and another (5) vendor booths represented. This year we are looking at using the same format with at least (6) presentations and multiple vendor booths. Presentations by SunGard, CoSentry, Bick Group, ARMA, American Micro, Dialogic, and Riverbed Technologies were given last year, and this year we look to set up a new list of participants. If you are interested in providing material for a table or booth, please contact Dennis Largent at dlargent@cosentry.com. What an exciting turn-out we had last year, and we are asking our members to invite their friends, work associates, and other businesses to this event. More information will be coming to you in the next few months as we finalize our plans.

Creating The Secure Password • Part 1 By Jeff Blackmon, CBCP, CISSP

Choosing a secure password has always been an interesting topic for me. Like it or not, all of us need to use passwords for our online bank accounts, credit cards, insurance and a multitude of other services. So just how secure do you think your self-produced passwords really are? Over the years I have tried multiple formats and schemes in hopes of producing the near unbreakable password. And in my own mind, I thought I was doing rather well at it.

All of that changed when I ran across a very good Bruce Schneier Crypto-gram news letter. <http://www.schneier.com/crypto-gram.html>. The newsletter describes the processes used by AccessData's Password Recovery Toolkit (PRTK) to discover so called secure passwords. This product is used for offline guessing such as encrypted PKZip or PGP files, not online web access passwords. After reading the newsletter, I discovered that all except one of my passwords would have been uncovered by PRTK. So much for being near unbreakable! So let's run through some of the processes that they use to discover the undiscoverable.

Lets begin with taking a quick look at the brute force attack of a five character password that can use the characters of a – z, and A – Z. This gives us 52 different characters to use in our make believe password. A total of more than 525 or 380 million possible passwords can be generated from this list of characters. That may sound like a lot of passwords, but with a 3-GHz Pentium 4 processor, anywhere from 350,000 to 1,000,000 passwords can be tested per second. Therefore, in this case, it will take an hour or so to break the password. Not good. But today's passwords can be much larger than that. If we change the above make believe password to be a length of 20, then our number of possible passwords to check becomes 5220 or 2.08×10^{34} . The same Pentium processor above will need up to 1.89×10^{21} years to complete the search. I am not waiting around for that one to complete. Much of the time will be spent testing improbable passwords such as 'ZRduoIlDeTmmNlolytgN', and not looking for the more probable passwords.

Access Data's PRTK has other means than just the popular brute force approach to determine hidden passwords. PRTK tries to approach the task in a much more organized manner. Instead of testing for each and every possibility, it looks for the more probable passwords. Brute force attacks are out, and dictionary attacks are in.

PRTK starts with using a dictionary of the 1,000 or so common passwords such as 'PW', 'password', '12345', 'letmein' and others. Then it will try adding a common suffix such as '1', '4u', 'abc' or '!' to the different common password list. According

to Access Data, this password guessing routine can uncover 24% of the hidden passwords. This statement says something about our lax ways in creating our passwords.

PRTK then starts a search process using 5,000 common words from the dictionary, 10,000 common names, 100,000 not so common words from the dictionary, and 10,000 phonetic patterns. If the password is not discovered by the above search, then appendages are applied to the above patterns and tested again. The appendages may include two-digit combinations, three-digit combinations, dates from 1900 to current, single symbols and two-symbol combinations. This testing process can uncover up to 65% of the hidden passwords. However, this process may take a month or two.

You may be one of the lucky ones if your password has held up so far. But wait, PRTK is still not done yet. All of the above would be considered a blind attack on your password. That is, no personal data is included in the search criteria. The PRTK program has a feature where the searcher can load personal information to be used as search keys. Information such as spouse's name, children's names, pet's names, house number, street name, ZIP code, phone number, car license plate number, birth dates, and the list goes on. All of that can be used as search criteria along with the common appendages. This process gives the PRTK program the ability to test probable passwords and not try to test all passwords.

The result is that today's software packages can perform a password search in a reasonable time. Instead of taking the 1.89×10^{21} years to do a brute force password search, intelligent software packages can bring the search time down to a few days, and with up to a 65% success ratio.

After reading this article, I have to believe that most passwords used today would not hold up well to these types of password cracking utilities. Try your own passwords and see how they would hold up to the above process. I will tell you that all except one of my passwords would probably be uncovered with the above software package.

Now that I have shot down the belief that most of us are using good passwords, you may be asking what does it take to create a secure password? Well, that information will be part of the next PEP newsletter. So stay tuned for more to come!

*Jeff Blackmon, CBCP, CISSP is a long time PEP member.
mailto: jdblackmon@sbcglobal.net*



National Poison Prevention Week • March 15-21
Poison Prevention Week Council

Earthquake Preparedness Month • In April
State of California

Page 6

Partnership for Emergency Planning • PEP Code of Ethics

The following Code of Ethics adopted by the Partnership for Emergency Planning (PEP) shall govern the conduct of all members, member representatives and invited guests.

All members and guest attendees involved with any PEP activities shall:

- Conduct themselves and their activities in a professional business manner.
- Abide by the bylaws and policies of PEP.
- Keep confidential anything of a sensitive and/or proprietary nature mentioned in PEP meetings, at PEP activities or written in PEP minutes or other PEP documents or PEP communications.
- Properly register at all PEP meetings and activities.
- Not engage in sales activities or solicitation.
- Not conduct any other activity contrary to the purposes and objectives of PEP.
- Not distribute any materials or post displays of any kind at PEP activities without the prior approval of the PEP Board of Directors or their designated representative.
- Not use the PEP name other than in the conduct of PEP business, as determined by the Board of Directors.
- Be prohibited from the use of the PEP general membership list, mailing list or any subsets thereof, except for PEP business. Membership lists are not to be furnished to non-members without the written permission of the PEP Board of Directors. Members who fail to observe this policy will be subject to loss of membership.
- Restrict the use of PEP proprietary documents to the use(s) defined by the policies and procedures of the PEP Board of Directors.
- Not publicly disclose verbal or written information pertaining to PEP business without prior written approval of the Board of Directors.

PEP Annual Election

The PEP Annual Election process is underway. The Nominating Committee is accepting nominations for President-Elect, Treasurer, Secretary, and Board Director positions. Any member in good standing can nominate someone for these positions.

Nominations should be sent to one of the following members of the Nominating Committee:

President, Adam Crowe, adam.crowe@jocogov.org
President-Elect, Sarah Keever, sekever@dstsystems.com
Past President, Linda Linhoff, Linda_Linhoff@swissre.com

The Nominating Committee will review the nominations to ensure they are in good standing. The Board will provide an approved list of nominees via ballot to the general membership. Once distributed, the ballot can be submitted electronically or via U.S. Mail.

Business Continuity Conferences 2009

DRJ Spring Conference • Orlando, Florida • March 29 to April 1, 2009
http://www.drj.com/index.php?option=com_content&task=view&id=2269&Itemid=697

Contingency Insights • Phoenix, Arizona • April 27-29, 2009
<http://www.contingencyinsights.com/Conference.html>

Gartner BCP/DR Conference • Chicago, Illinois • April 27 to 29, 2009
<http://www.gartner.com/us/bizcon>

CPM 2009 West • Las Vegas, Nevada • May 12 to 14, 2009
<http://www.contingencyplanning.com/mcv/events/west/>

NFPA Conference and Expo • Chicago, Illinois • June 8 to 11, 2009
<http://nfpa.typepad.com/conference/>

ASIS 2009 International Conference • Anaheim, California • September 21 to 24, 2009
<http://www.asisonline.org/education/programs/anaheim/default.htm>

International Association of Emergency Manager (IAEM) • Orlando, Florida • October 31 to November 5, 2009
<http://www.iaem.com/events/annual/intro.htm>

Public and Private Sector Training (BCP and FEMA)

FEMA Independent Study Courses training you can download with on-line exam
<http://training.fema.gov/IS/crslist.asp>

State Emergency Management Agency training in various Missouri locations
<http://training.dps.mo.gov/>

Mid America Regional Council (MARC) in-person training in Kansas City, Missouri
<http://www.marc.org/emergency/emergencytrainingprograms.htm>

Association of Contingency Planners search for a local chapter
<https://www.acp-international.com/chapter.taf>

Independent Groups list of groups by state
<http://www.drj.com/groups/drj6.html>

Webinars

Strohl webinars sponsored webinars
<http://www.strohl.com/Events/Webinars/default.asp>

3N Global (formerly known as National Notification Network)
<http://www.3nonline.com/webinars>

Disaster Recovery Journal sponsored webinars
http://www.drj.com/index.php?option=com_content&task=blogsection&id=21&Itemid=382

Contingency Insights sponsored webinars
http://www.contingencyinsights.com/Resources/Virtual_Seminars.html

PEP Directory of Officers & Directors

Officers

President, Adam Crowe, CEM, MPA
Assistant Director • Community Preparedness
Johnson County Emergency Management & Homeland Security
111 South Cherry St., Suite 100
Olathe, KS 66061-3441
913-715-1003 office
913-791-5002 fax
816-260-1695 mobile
E-mail: Adam.Crowe@jocogov.org

President Elect, Sarah Keever, CBCP
Senior Business Continuity Analyst
DST Systems, Inc.
816 Broadway, 1st Floor
Kansas City, MO 64105
816-843-9197 office
816-935-0210 mobile
E-mail: sekever@dstsystems.com

Past President, Linda Linhoff, CBCP
Swiss Re • 5200 Metcalf
Overland Park, KS 66202
913-676-3131 office
913-207-1920 mobile
E-mail: Linda_Linhoff@swissre.com

Secretary, Linda DeTienne, CFM, CFMJ
National Catastrophe Restoration, Inc.
8065 Flint
Lenexa, KS 66214
316-636-5700 office
316-761-0014 mobile
E-mail: detienne@ncricat.com

Treasurer, Tom Munoz, MBCP
Sprint • 6100 Sprint Pkwy
Mailstop: KSOPHK0110 - 1A753
Overland Park, KS 66251-6113
913-315-5570 office
913-485-9774 mobile
E-mail: Thomas.2.Munoz@sprint.com

Hospitality Coordinator, Dennis Largent
CoSentry, 10801 N. Amity Ave.
Kansas City, MO 64153
816-891-5911 office
913-221-1341 mobile
E-mail: dlargent@cosentry.com

Web Master, Nick Crossley, CEM, ABCP
Director
Johnson County Emergency Management & Homeland Security
111 South Cherry St., Suite 100
Olathe, KS 66061-3441
913-715-1007 office
913-485-1465 mobile
E-mail: ncrossley@jocogov.org

Newsletter, Jim Baird
U.S. Central Federal Credit Union
9701 Renner Blvd., Suite 100
Lenexa, KS 66219
913-227-6510 office
E-mail: jbaird@uscentral.org

Board of Directors

Historian, Bill Latteman, CBCP
Argus Health Systems, 1300 Washington St.
KC, MO 64105
816-435-5405 office
816-510-4305 mobile
E-mail: Bill.Latteman@argusHealth.com

Ronn Hennessy, CBCP
American Century Investments
4500 Main
Kansas City, MO 64111-7709
816-340-3834 office
E-mail: ronn_hennessy@americancentury.com

Steven Hannah, MBA, CBCP, CISA, CISSP,
CHS Level III
Waddell & Reed, 6300 Lamar Avenue
Shawnee Mission, KS 66201-9217
913-236-1484 office
816-914-7912 mobile
E-mail: Shannah@waddell.com

Alisa Pacer, CBCP
Johnson County Community College
Police Dept.
Emergency Preparedness Manager
12345 College Blvd.
Overland Park, KS 66210-1299
913-469-7622 office
E-mail: apacer@jccc.edu

Call for Newsletter Articles

The partnership for Emergency Planning Board of Directors would like to invite all members to submit articles for publication in the quarterly PEP Newsletter. This newsletter is circulated to over 200 PEP members representing over 100 companies and government agencies in the Kansas City Metro area.

You can submit articles from other publications (with author permission) or write about a recent exercise, lessons learned in continuity/disaster planning, or other general areas of interest to private and public continuity and emergency managers.

The articles should be 250-500 words in length and submitted via email. You may also include a short profile of yourself and company that will be included with the article.

If you are interested in submitting an article or would like more information, please contact Jim Baird via e-mail at jbaird@uscentral.org.