Massachusetts General Hospital
POLICE, SECURITY and OUTSIDE SERVICES

(A)LL (P)OINTS (B)ULLETIN

March 2012

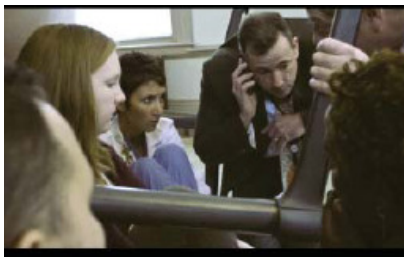
The mission of the MGH Police, Security and Outside Services Department is to competently deliver protective and supportive services to the MGH Community in order to provide a welcoming, accessible and safe environment.

Code Silver: Preparing for the Unthinkable

Matt Thomas, CNY Operations Supervisor, Special Police Officer

Senseless acts of violence tend to stay in our memories. I'm sure, for instance, we all remember the senseless killings at Columbine High School, Edgewater Technologies in Wakefield, Virginia Tech University, and more recently, Johns Hopkins Hospital. These incidents are classified by the US Department of Homeland Security (DHS) as 'active shooter' incidents.

It is sobering to think about defending ourselves against an active shooter. In truth, the likelihood of being involved in an active-shooter incident is as remote as being struck by lightning. But the safety and welfare of our patients and staff is the highest priority at MGH, so it makes sense to think about it, plan for it, and educate our workforce to minimize casualties should the worst-case scenario occur.



After benchmarking with DHS, outside law enforcement, and other hospitals, a procedure was developed by MGH senior leadership, Police, Security and Outside Services, Emergency Management, and Human Resources for how to respond in the event of an active shooter incident. The response is called: Code Silver.

A three-phase roll-out plan is being implemented to train employees on what to do during a Code Silver alert. Phase I consists of training managers and supervisors; Phase II consists of training MGH employees via a video on HealthStream; and Phase III consists of a Code Silver drill to be conducted in collaboration with the Boston Police Department.

Since September, more than 100 manager/supervisor training sessions have been conducted, and Police, Security and Outside Services is finalizing the Code Silver training video.

The primary components of the Code Silver training are the four levels of response to an encounter with an active shooter:

- Get out
- Hide out
- Call out
- Take out

Getting out, or evacuating, is the first option. If there's a safe escape route, leave the premises. Have an escape route in mind; leave all belongings behind; assist others if possible. Follow the instructions of law enforcement, and do not attempt to move the wounded.

Hiding out is the second option. If evacuation is not possible, find a place to hide. The best hiding places provide protection but don't trap or restrict your ability to move. Block or lock the door if possible, hide behind large objects, and remain quiet.

Calling for help is the third option. If evacuation and hiding are not possible, remain calm and call 911. If you can't speak, leave the phone line open to allow the dispatcher to hear what's happening.

IN THIS ISSUE

Taking the shooter out is the fourth option and should only be attempted as a last resort (if your life is in imminent danger). Then and only then, attempt to disrupt or incapacitate the shooter. Make a plan, commit to the plan, and do whatever it takes to carry out your plan.

The Code Silver training video will be available on HealthStream later this month for all clinical staff.

For more information, review the Code Silver policy in Trove. Department training can be scheduled by calling Police, Security and Outside Services at 4-3030.

Information Security is Everyone's Responsibility

Kevin Lavoie, CNY Operations, Security Officer Level II

If your work deals with information about business assets, patients or employees, then you need to be thinking about the confidentiality and integrity of those assets. In reality, we ALL share that responsibility… information security is **EVERYONE'S** responsibility!

Any desktop computer, laptop computer or server could be used to host viruses, Trojan and other malicious programs. We all should be aware of the security issues related to our daily use of computers. Here are some basic steps and precautions that you, as a computer user, can take to help secure your computer and to protect the integrity of information stored on it.

1. Beginning with physical security, some basic recommendations are to turn your system off at night and during the weekends, don't stay logged in to your system or e-mail while you are not there and use locking screen savers if you need to leave your system on and unattended for any prolonged length of time (a locking screen saver is built-in to Windows). An unattended, unlocked system allows anyone to walk up to your computer and access files and information (and potentially your e-mail) stored on your computer when you are not there.

2. Any computer that is connected to a network and "always on" may be vulnerable to intrusions. There are readily available tools on the Internet that allow other people to scan your system for well-known vulnerabilities. You may want to consider installing a personal firewall on your system to prevent intrusions. This is already done for your MGH computer. Install anti-virus software and update virus definition files on a regular basis. The largest threat on the Internet is the propagation of viruses and malicious programs through e-mail. You should ensure that attachments are not automatically opened and/or executed and ensure that all attachments are scanned for viruses prior to opening them. Turn off unnecessary services such as file sharing. If you have to enable these services, enable password protection.

3. Make routine backups of your most critical data and information. Test your backups to ensure that you can recover the information should you need to. Backups are like insurance--you never know when you'll need it, but you'll be glad you have it in a crisis. Protect passwords, select a "strong" password, change them regularly and don't use the same passwords for different accounts. Don't tape passwords to your monitor, or hide them under the keyboard or mouse (those are the first places people look). Choose passwords that are difficult to guess. Don't use your first or last name, user ID, SSN, telephone number, birth date, or dictionary words (most password cracking programs will test against these items). Choose passwords that are at least 8 characters in length and use a combination of upper, lower and special characters.

These are some precautions that you can take to secure your computer systems and the integrity of the information contained within. If we all do our part, although we may not be able to eliminate attacks, we can certainly impede the efforts of those who threaten the integrity of our systems.

Credit Card Fraud: Still a Hot Topic

Jim Harrop, Communications Officer, Special Police Officer

Credit card fraud is a term relating to the theft or fraud that is committed by using a credit card or any similar payment sources to deprive one of their goods or services. The purpose is to obtain these goods or services without paying, or to obtain unauthorized funds from an account that does not belong to the holder. Credit card fraud is closely tied to identity theft.

Each year the cost of credit card fraud continues to rise and the number is staggering. Each year credit card fraud averages approximately 750 million dollars in lost revenue and legal bills for businesses and the consumer affected by the fraud.

Credit card fraud starts with the actual physical theft of a card and the cardholders can mitigate against this fraud risk by checking their accounts frequently as well as set up alerts that can warn you against large or multiple purchases.

When a credit card is lost or stolen, the card will remain usable until the cardholder notifies the bank or the issuing company that the card has been lost or stolen. Most credit companies have a toll free numbers to assist their holders with prompt reporting. Still, it is possible for a thief to make unauthorized purchases on a card until it is canceled.

A security measure that has been put in place on credit cards is the rear signature strip located on the back of cards. Since there are many thieves that can forge a signature, it is beneficial for you to write "**PLEASE VERIFY ID**" which causes the merchant to ask the individual for identification to verify if the card user matches the identification given.

So the moral of the story to prevent credit card fraud is to:
-- Report stolen or missing cards **immediately**
-- Monitor your credit report quarterly
-- Place "**PLEASE VERIFY ID**" on the signature strip
-- Make sure all transactions are appropriately marked and accounted for on your statements
-- Utilize alert text or email messages to monitor transactions

Safety to a "T"

Dan McCarthy, CNY Operations, Security Officer Level II

Have you noticed less elbow room on your MBTA bus or train lately? It's not your imagination. This past fall, the MBTA announced that its ridership had reached nearly 1.35 million users on an average weekday, the highest amounts in the agency's forty-seven year history. Unfortunately, along with this increase came a dramatic rise in T-related crimes. Statistically, comparing reported crimes to the number of users, the system is still a relatively safe alternative to driving into work. The most common crimes reported include pick-pocketing, thefts of bikes and thefts of electronic devices. Keeping this in mind, there are still a few things you can do to try to ensure that you get to and from work hassle free.

1. Plan Your Route Ahead of Time: The T scheduling system can get pretty confusing if you are trying to coordinate bus and subway trips. It helps to have your exact route planned out before you even step out the door. This way you will know where you need to be, when you need to be there, how long you will have to wait, etc. One of the biggest dangers of public transportation is looking like you don't know what you are doing, or where you are going. This could make you a vulnerable target. Today, it is easier than ever to manage your commute due to the proliferation of mobile applications for our hand-held electronic devices. There are more than two dozen "apps" available that provide up to the minute T bus, subway and commuter rail information, most in 'real time'. Just go to www.mbta.com, and click on 'Rider Tools', then 'App Showcase" to find out how to download an application. Your long wait for a bus or train could be over!

2. Dress for Success: When we dressed for our job interview, we dressed to impress; when we dress for a night out after work, we dress to look good; but when you dress to ride the rails, you don't want to look too good. This means avoiding expensive coats, clothing, watches, jewelry, rings, necklaces, etc. If you are going someplace fancy, bring separate clothes in a bag or wear a nondescript outer layer. This is one time when standing out in the crowd is not a good idea. You don't want to invite trouble!

3. Stay Awake and Alert: Reading the Metro or playing Angry Birds can be great ways to pass the time on a bus or train, but they also take your attention away from your surroundings and make you an easier target for thieves. This especially goes for those of us who have the tendency to fall asleep. Dozing off on a crowded bus or train full of strangers can be very dangerous unless you have someone with you to watch over you and your stuff. Also, avoid listening to really loud music when wearing headphones while riding the T. This may distract you and could also make you a potential target.

4. Pay Attention to Those Around You: You can tell a lot about a situation just by getting a feel for your surroundings. Be aware of fellow passengers who seem suspicious, argumentative, or talkative. One method criminals use is to divert your attention somewhere while an accomplice steals your belongings.

By following these suggestions, you should be able to enjoy an uneventful commute. The T's safety slogan is "See Something? Say Something!" So remember, if trouble does occur, don't be afraid to notify the bus or subway driver right away. Also, add the Transit Police telephone number, 617-222-1212, to your cell phones contact list for quick dialing.

Look Both Ways Before Crossing the Street…

Ron Ruggiero, Main Campus Operations, Security Officer

Since I have been a traffic officer at MGH, I have seen many scary moments for pedestrians. Directing traffic in front of one of the busiest hospitals in the world is no simple task. There are multiple crosswalks, thousands of cars, tens of thousands of pedestrians, and ***one*** traffic officer. Over time I have seen a lot of people cross the street, and though it is a task we all do many times each day, many of us have not thought about it since the first grade!

Pedestrians do have the right of way; however just because this is the case does not mean that you will get it. Many of our pedestrians are also patients, and they are often nervous, overwhelmed and distracted with their emotions. Drivers naturally have other things on their mind and their focus might not be you standing in the crosswalk. When using a cross-walk, imagine that a stop sign is in front of you, the pedestrian. Stop on the curb and wait for the approaching vehicle to see you. Make eye contact with the driver and wait for them to signal you to cross.

When a traffic officer is directing traffic, wait until the officer tells you that it is safe to cross. The streets surrounding the hospital get very busy. Although the pedestrians have the right of way, the officer needs to sometimes keep the traffic flowing to keep a clear path for incoming emergency vehicles. It may take a few extra seconds, but wait for the officer to inform you that it is safe to cross. Running out in between cars does not only pose a danger to you, but to the driver of the vehicle who has to swerve to avoid you. It poses a severe safety hazard to others as well.

We hear a lot of publicity regarding texting and driving, which is very unsafe. Every day I see many people walking and texting. Though this is not against the law, it puts you in an unsafe position by being unaware of your surroundings. If you need to read or send that important text, stop for a minute and then continue to where you are going.

Again, because you are in a crosswalk, it does not make vehicles stop. At times we are all in a hurry, but take a moment and cross safely so you can arrive at where you are going.

Get in the Game!

Ken Sutton, CNY Operations, Security Officer

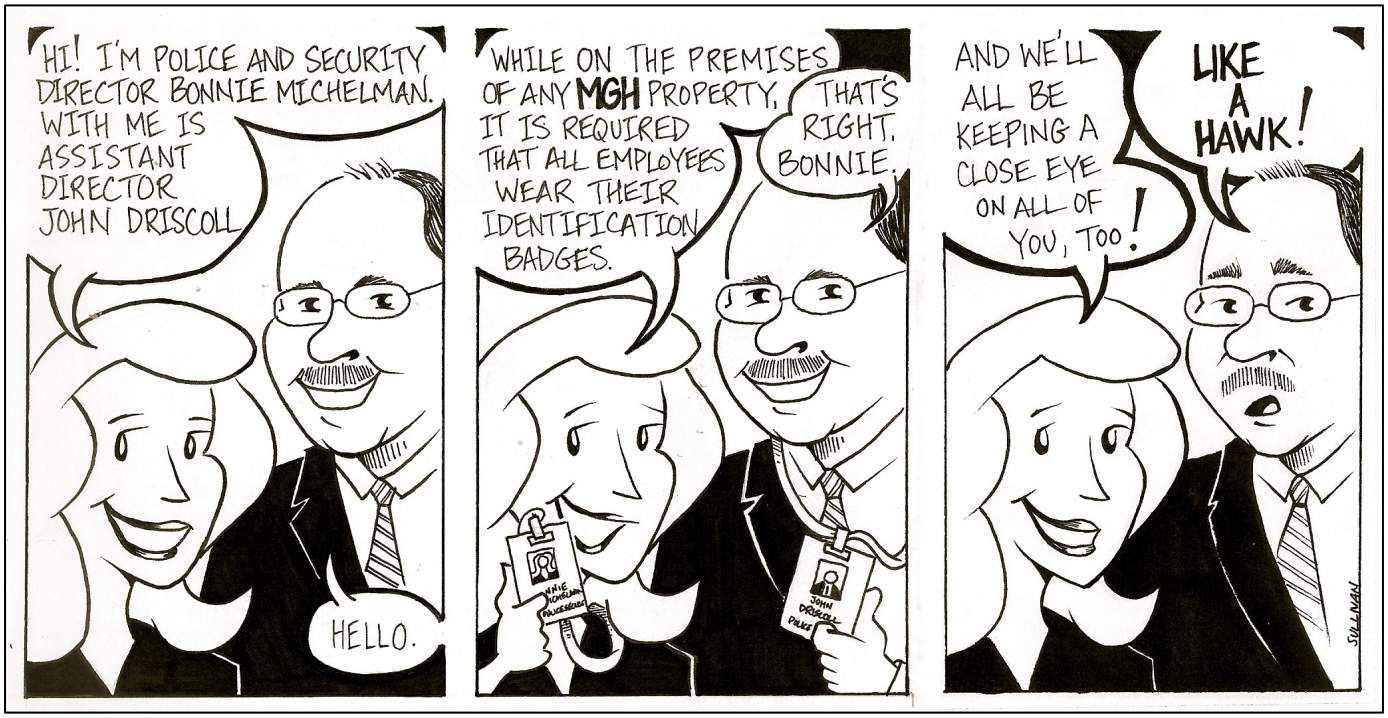
In basketball it is called the "Sixth Man." In football, it's called the "Twelfth Man." In baseball it is referred to as the "Tenth Man." All three of these terms refer to the efforts of fans to help their team. The presence of fans can have a profound impact on how the teams perform. Therefore these loyal fans often create loud distracting noises to confuse the opposing teams and cheer emphatically for their own team in order to help them be successful. Some fans will go to any length to help their team win, feeling as if they are a part of the game. They are a great advantage in helping their team protect its home turf. At times such fans can seem like extra players as they make opposing teams feel unwelcome. Whatever the game, be it basketball, football, baseball or just the game of life, everyone can get involved and have a profound effect on its outcome.

Massachusetts General Hospital is our home team, yet it consists of many smaller teams working together in order to make us all successful. The MGH Police, Security and Outside Services team is here to protect our home turf. Although security is no game, the concept of teamwork is still the same! We can all contribute or "Get in the Game." Every patient, visitor and employee who calls security for any critical issues serves as adjunct members of our security team! Everyone who sees or hears anything pertinent to the safety and security of the MGH community and reports it, are demonstrating that they are a valuable member and loyal fan of our security team as well as the larger hospital team! On behalf of the entire MGH Police, Security and Outside Services team we want to thank everyone and let you know that we appreciate your efforts in helping keep our community safe and secure.

So please in a word… "Continue!" Please continue to call security before situations escalate. Continue to make some noise for your team and question anyone in your work area who doesn't belong there or seems out of place. Continue to let the opposition feel uncomfortable and unwelcome. Continue to call for security standbys. Continue to wear and display your MGH identification badge, thereby showing your team spirit. Most of all, continue to make sure your team keeps the home court or home field advantage in your own way. Continue to make a difference and… **"GET IN THE GAME!"**

"On the Lookout"

David Sullivan, CNY Operations, Security Officer



LETTERS TO THE EDITORS

CAROLYN WHITE
cwhite7@partners.org
617-724-7833

MASSACHUSETTS GENERAL HOSPITAL
Police, Security & Outside Services

MATT THOMAS
mdthomas@partners.org
617-643-0806