PRESENTER'S GUIDE

"WORKPLACE SECURITY"

Part of the General Safety Series

Quality Safety and Health Products, for Today... and Tomorrow

OUTLINE OF MAJOR PROGRAM POINTS

OUTLINE OF MAJOR PROGRAM POINTS

The following outline summarizes the major points of information presented in the program. The outline can be used to review the program before conducting a classroom session, as well as in preparing to lead a class discussion about the program.

- **We hear about it almost every day... somewhere something bad has happened in a workplace.**
  - An employee has been shot by an angry coworker or an estranged spouse.
  - A bomb has been set off and people have been injured.
  - A truckload of valuable product is missing.
  - A company's computer system has been hacked and the credit card information of millions of customers has been stolen.

- **These things don't just happen "somewhere else".**
  - They can occur in our own city or town… even our own company.
  - Having a good workplace security program in place can often prevent these situations from occurring.

- **The first step in creating and implementing a Workplace Security Program is to form a plan.**
  - To do that you will need to assemble a team that will work to identify the types of security issues your facility may face, and what can be done to protect the company from harm.

- **The team should include people from all of the company's operating departments.**
  - If possible local law enforcement personnel should be included as well.

- **Having multiple perspectives regarding what is of value in your facility, and where your facility's vulnerabilities are, is important.**
    - Law enforcement can provide an “outside view”, as well as insights based on what they have seen at other facilities in the area.

- **Once your team is assembled, the first thing that they should do is create three lists.**
    - The first list should catalog anything of value that someone might want to steal from your facility.
    - The second list should identify your facility's points of vulnerability that could "open the door" for an unlawful entry.
    - The third list should contain any type of security issue that your facility could be subject to.

- **All of this is influenced by the type of business that you're in.**
    - A jewelry store will need to pay particular attention to their merchandise, including how easy it is for someone to get their hands on it.
    - A bank has the same type of concern regarding its “product”… the money that is on site.
    - Hospitals and other medical facilities must not only guard materials that are used there, such as drugs, but also their staff and patients who might be subject to an attack.
    - Manufacturing locations may have valuable raw materials or high priced finished products
    - Warehouses can contain all types of desirable merchandise.

- **Your facility's normal "entrances" are an obvious vulnerability, but not necessarily the only “location” issue.**
    - There could well be other ways someone could gain access, such as through loading docks, fire exits or even windows.
    - If employees work outside the facility or in isolated areas, they could be at risk as well.

- **How you control access to your facility is one of the most important aspects of your Security Plan.**
    - Restricting access goes a long way toward preventing theft and property damage, isolating sensitive work areas, and most importantly, protecting employees from harm.

- **"Physical security" addresses all of these things, often by using some type of "protective barrier".**
    - So it’s imperative that your company determine which types of barriers are already in place, if any upgrades are required and what additional measures may be needed.

- **For almost all facilities doors are the primary security measure for controlling access and prohibiting unauthorized entry.**

- **As well as being visually pleasing, the solid glass doors that are used in many entrances offer a clear view of anyone who approaches or enters your building.**
    - But they can also be vulnerable to being smashed.
    - Changing the glass in entryways and windows to "security glass", or adding "strengthening film" to current glass, can fortify these access points.

- **Other exterior doors that are out of plain sight or lead to areas where large quantities of raw materials or finished goods are stored may need to be beefed up as well.**
  - You might want to install more secure doors in places such as telephone and server closets, utility rooms and designated "safe rooms" as well.

- **Steel and solid wood doors are especially suited to protecting a workplace.**
  - Unlike hollow wooden doors they won't crack, and they can be more difficult to break down.
  - Many steel doors are also drill-proof, chemical-resistant, bulletproof and fire resistant, which helps to protect against break-ins and arson.

- **But strong doors by themselves are only half the answer.**
  - They won’t stop unwanted entry to your building if they have a faulty or easily manipulated lock.

- **For years, traditional locks and keys were the standards for workplace security.**
  - But most "keyed" locks can easily be picked, or drilled out. And lost or stolen keys can be copied.
  - At the least this can result in costly lock replacements.
  - At worst it can lead to an unauthorized entry, which is why many facilities have gone to "keycard" or "keypad" systems.

- **People often think "physical security" mainly consists of physical barriers.**
  - But strong doors, locks and bullet proof glass are not the only forms of physical security that can be used in a workplace.
  - These days, facilities are supplementing traditional physical security measures with increased exterior lighting, surveillance systems and alarms.

- **According to the U.S. Department of Justice, the third most common place for crimes to occur is a parking lot.**
  - This is not just theft and vandalism.
  - Nearly 1,400 violent crimes like assault and robbery are committed in parking lots each day.

- **At the very least, all of your building's exterior lighting should be checked to verify that it is functioning properly.**
  - Any needed repairs should be scheduled immediately.
  - New lights should be installed in any areas that need it.

- **If your workplace is like most, it is often vacant at night, which makes it more likely to be burglarized then, than during daytime working hours.**
  - Adding surveillance cameras (both indoor and outdoor) to your building, and posting signs as to their existence, can act as a deterrent… as well as aid law enforcement in their investigations.

- **There are also a variety of alarms that can help to defend your facility against all types of security risks.**
    - Intrusion alarms can discourage unlawful entry by letting burglars know that they have been noticed, and notifying local law enforcement that a break-in is occurring at your building.
    - Employee activated "duress alarms", like the systems used in banks, can help to prevent violence in your facility by silently calling for help during robberies or active shooter incidents.

- **Many of these alarms can be integrated into your building's fire control system, door access controls and surveillance cameras.**
    - Tech-based systems can also include apps or other software that allow you to monitor things from devices such as tablets and smartphones.

- **Today, it seems like you can accomplish almost anything with technology. Thanks to computers and the internet, your company can:**
    - Communicate with customers and business partners around the world via e-mail and video conferencing.
    - Manage payroll, expenses and payments with online banking.
    - Keep an accurate inventory of products.
    - Train and educate employees with online learning courses.

- **While this technology opens up a whole new world of opportunities for your business, it can also leave you open to the threat of "cybercrimes".**
    - Thieves are no longer just interested in stealing your company's physical assets.
    - They want your digital information as well… from customer data to banking records.

- **Although cybersecurity can be a very large and complex topic, there are three easy-to-follow guidelines that can go a long way toward helping to protect your company's digital information.**
  - Use "strong" passwords.
  - Don't open suspicious e-mails, attachments or links.
  - Never use public WIFI without a Virtual Private Network (VPN).

- **Using "strong passwords" is one of the simplest, yet most effective forms of cybersecurity.**
  - Passwords should be at least 16 characters long and include both upper and lower case letters, numbers and symbols.
  - The more complex and random that the password is, the more difficult it will be for hackers to crack.

- **You should avoid using your children's names, birthdays, pets' names, or any other personal information for your password.**
  - Hackers will often search your social media pages or company bios to find and try those.

- **Using sequential numbers or letters in your password is also a "no-no".**
  - When hackers are trying to determine password patterns, they often key in sequential numbers and letters first.

- **You should also create a different password for every computer or account that you access.**
  - If a hacker does manage to steal one of your passwords, they will quickly test it on all of your accounts to see what it will unlock.
  - To stay ahead of cybercriminals, you should change your passwords every month.

- **Even if you create very secure passwords, you aren't out of the cybersecurity woods yet. You also have to watch out for "phishing"**
    - "Phishing" occurs when cybercriminals impersonate the e-mail account of a source that you trust, such as a friend, coworker, or customer.
    - Using this "look-alike" address they will send an e-mail containing attachments or links that release computer viruses.

- **There are some quick checks you can use to help determine if an e-mail might be harmful.**
    - Does the e-mail contain spelling errors or oddly worded phrases?
    - Is the sender requesting some confidential information, such as a credit card or social security number?
    - Does the e-mail read *"Here is that file you wanted"* even though you never requested one (it's likely that the attachment contains a virus or worse)?
    - Does the e-mail instruct you to click on an embedded website or other link (that link could take you to a site that allows a hacker to gain access to your computer)?

- **The best way to deal with a questionable e-mail is not to open it at all.**
    - If you think it might be legitimate call the sender.
    - If it is a potential hack, your call will also alert them to a potential attack on their own account.

- **The communication systems that you use with your computer can present their own risks.**
    - If you're working at home, in a hotel or in a coffee shop, your personal router or public WIFI may not be secure enough to prevent hackers from accessing your accounts.

- **One way to guard against this is to use a Virtual Private Network (VPN).**
  - This will provide an encrypted connection between your location and your company's computer network.
  - Using VPN's will allow you to safely and securely share information from anywhere you are.

- **Strengthening your physical and cybersecurity can help to prevent intruders from gaining access to your facility and company data.**
  - But what can you do if someone does make it through the door?

- **The place to start is by stationing an employee in your reception area.**
  - This not only creates a "psychological barrier" for anyone who approaches, it also helps prevent visitors from going further into the building on their own.

- **When someone enters, the "receptionist" should ask them to sign into a physical or digital "log-book".**
  - The visitor should provide their name, the reason for their visit, the name of the person they are there to see, and note the date and time.

- **For scheduled visits, the visitor should then be issued a badge.**
  - The person they have come to see should be notified of their arrival.
  - The receptionist should wait with the visitor until someone arrives to escort them to their destination.
  - If the visitor doesn't have an appointment, the person they want to see should be called to determine if they want to go ahead and meet.

- **You should never allow visitors to wander around your building unaccompanied.**
    - If there are multiple visitors at the same time, the receptionist should ask other staff members for help.

- **The front desk should never be left unattended while a visitor is escorted to their destination and a visitor should never be left unsupervised.**
    - If a backup person is unavailable, the front door should be locked and someone should monitor the entrance or set up to listen for the doorbell.

- **Enforcing a policy that designates your main entrance as the only access point for both your employees and visitors can help reduce the risk of unauthorized entry as well.**
    - Employees should be told that if they violate the company's entrance policy they will receive a warning, and that repeated violations will result in further disciplinary action.

- **Other exterior doors should not be operable from the outside and have "evacuation bars" inside.**
    - If a door needs to be left open or can't be closed due to a faulty lock, it should never be left unattended.

- **If keycards, codes or physical keys are lost or stolen this should be reported to your department supervisor immediately.**
    - This will allow them to quickly deactivate the cards, reprogram codes or replace the locks and issue new keys.

- **Making sure that security devices are working properly is also important.**
    - At least once a month, department supervisors should inspect all locks or key devices in their area for damage.

- **In the event a visitor somehow does gain access through an exterior door, someone should approach them from a safe distance and ask them to leave immediately, or come to the main entrance to log in.**
    - If there are any concerns about the visitor's intentions they should be followed from a safe distance to confirm that they exit while someone calls the authorities.

- **There was a time when it seemed like violence only occurred in businesses that handle cash, like banks and convenience stores… or places that served alcohol, such as bars and nightclubs.**
    - Today the sad truth is that violence can occur in any workplace, for a variety of reasons.
    - Planning for how to deal with an incident should be part of every facility's Security Plan.

- **There a number of things your company can do to effectively deal with workplace violence and help to minimize harm if it does occur, such as:**
    - Making sure all employees understand the "run, hide, fight" principle.
    - Developing communication techniques that employees can use to alert each other of potential incidents.
    - Establishing evacuation routes for safely and quickly exiting the facility.
    - Setting up secure rooms or areas where any employees who are unable to evacuate the building can safely wait until the event is over and everything is secure.

- **If a workplace violence event appears to be developing, employees and the authorities need to know about it immediately.**
    - Having emergency communication methods in place can help people to alert each other to the possible danger and take swift action.

- **A "Phone Tree" arrangement can quickly and effectively get a brief emergency message out to everyone in your facility.**
    - Text messages are often best, since they are "silent" and don't run the risk of being heard by perpetrators.

- **There should be a primary "point person" in each department whose responsibility is to notify several other designated coworkers of the emergency situation.**
    - These other employees then alert the rest of the department of the situation.

- **Additionally, an emergency contact list for local police, fire and ambulance groups should be posted at every desk, workspace and common area in your building, so that anyone in the facility can contact the authorities if necessary.**
    - For rapid dialing, emergency numbers should be preset on internal phones, and employees should add them to their cell phones as well.

- **If a workplace violence event seems unavoidable, everyone should vacate the building ASAP.**
    - This is where clearly defined evacuation routes will help people make an organized and quick exit.

- **Using your building's floor plans, maps should be created with arrows that clearly show the nearest evacuation routes and exits for each area... as well as exterior meeting places where employees should gather.**
    - In addition to being posted in each work area, every employee should be provided with a copy of their map so that they can familiarize themselves with their evacuation routes, exits and meeting places.

- **If someone is unable to exit the building, they should immediately take shelter in a "safe room" or area until the threat is over, and the building is declared secure by the authorities.**

- **If your building doesn't currently include any "safe areas", employees should use a windowless room with a sturdy, solid-core or steel door.**
  - If a windowless room is unavailable, the windows of the room should be covered if possible.
  - Employees should get low to the ground and hide somewhere that is away from the windows and doors.

*** * * SUMMARY * * ***

- **The first step in creating a Workplace Security Program is to form a plan.**

- **The key to any Security Program is identifying a facility's security issues and vulnerabilities.**

- **Controlling access to your facility is one of the most important aspects of your Security Plan.**

- **Safeguarding your company's information can be as vital as safeguarding your facility itself.**

- **Even if your facility is physically secure, it's important to monitor potential access points and visitors.**

- **Employees need to be trained regarding what to do if a workplace violence event occurs and where and how to evacuate the facility.**

- **While workplace security is more complex today that it ever used to be, you can help your company implement a comprehensive Workplace Security Program… so that you and your coworkers can go home safe at the end of every day.**