

Microsoft Course Player - Internet Explorer

https://library.skillport.com/courseware/Content/ria/RIA_V3_1_1123/index_tablet.html?lang=en&AICC_URL=https%3A%2F%2Fsamhouston.csod.com%2FLMS%2Fscorm%2Faicc.aspx&AICC_SID=AICCneerjf9ecYYuQIF_YbqMstc-0cxz-kgV

< Menu

Table of Contents

Workplace Safety, Security, and Privacy

Exit

Workplace Safety, Security, and Privacy

1 Hour 12 Minutes

Employee Safety

27 Minutes

Employee Health

17 Minutes

Workplace Security

17 Minutes

Workplace Privacy

11 Minutes

Course Test

Employee Safety

Topic Type: Instruction

Approximate Duration: 27 minutes

You have not taken a test for this topic.

This topic covers the following points:

[Course overview](#)

[Employee safety](#)


[Review](#)

Learning Objectives:

After completing this topic, you should be able to:

- sequence the steps for conducting a workplace risk assessment
- differentiate between the strategic roles of management, HR, and safety committees
- sequence the steps in the accident investigation procedure
- identify and describe workplace illnesses and disorders

Skip Topic



<< Previous Topic

< Back

Next >

Next Topic >>

Course Transcript

Risk Management: Workplace Safety, Security, and Privacy

Workplace Safety, Security, and Privacy

[1. Employee Safety](#)

[2. Employee Health](#)

[3. Workplace Security](#)

[4. Workplace Privacy](#)

Employee Safety

Learning Objectives

After completing this topic, you should be able to

- *sequence the steps for conducting a workplace risk assessment*
- *differentiate between the strategic roles of management, HR, and safety committees*
- *sequence the steps in the accident investigation procedure*
- *identify and describe workplace illnesses and disorders*

1. Course overview

Welcome to Risk Management: Workplace Safety, Security, and Privacy.

Welcome to Risk Management: Workplace Safety, Security, and Privacy. My name is Frank Cania and I'm certified as a senior professional in human resources by the HR Certification Institute, and I hold a master's degree in employment law. I've been teaching this course for several years and I've helped countless HR professionals successfully complete the PHR and SPHR exams.

In this course we'll examine the importance of safeguarding employee safety and health, as well as workplace security and privacy and why those safeguards are essential for business continuity and success. Next, we'll explore various aspects of employee safety and health hazards and support systems employers can offer, such as employee assistance programs, or EAPs, and an employee wellness program.

And finally, we'll cover security risk analysis methods and security measures, as well as workplace privacy issues, privacy policies, and how you can best address employer and employee privacy concerns. In topic one, Employee Safety, you'll gain insight into the importance of a safety needs analysis, the development and implementation of occupational injury and illness prevention programs and return to work programs, identifying workplace safety risks and establishing general health and safety practices, and an overview of OSHA investigation procedures.

2. Employee safety

Effective implementation of risk management plans, policies, and procedures is critical to protecting business assets and the employees. It's also a decisive factor in reducing the extent and severity of work-related accidents and injuries. To be effective, various areas of risk management are often broken down into smaller, more manageable programs, such as employee safety and health programs, which are implemented to protect employees and resources; workplace security – these programs describe the preventive measures used to protect the employees and the organization from hazards and workplace violence; and workplace privacy programs, which address employer and employee privacy concerns. Employer privacy concerns include the protection of proprietary information and the privacy

challenges technology has caused. Employee privacy concerns include identity theft and employees' personal information being compromised.

HR professionals should identify and assess workplace safety, health, security, and privacy risks before developing and implementing programs and procedures to manage them. The steps and actions in workplace risk assessment involve first identifying workplace risks – walk around the workplace, ask employees what they think, check manufacturers' instructions for operating and servicing equipment, and read the OSHA regulations to identify potential issues. Next, decide who might be harmed and how – identify employees who work with hazardous materials and under hazardous conditions, and make a list of how they can be harmed. Next evaluate the risks and decide on precautions – evaluate the nature and the amount of harm each risk could do, prioritize hazards as part of an action plan, then determine how to reduce or eliminate each risk. Record your findings and share them with a peer to ensure that all important areas have been covered. And finally, share your findings with management, including the information collected and the changes that should be made to make the workplace safer.

Since the passage of OSHA laws, workplace fatalities have been reduced by more than 60%, and injuries and illnesses are down more than 40% from the levels experienced in the mid-1970s. This is despite the fact that the workforce has doubled in that time. However, workplace fatalities, injuries, and illnesses are still huge direct and indirect costs to organizations. According to one estimate, the average cost associated with a single work-related fatality – which included direct costs, such as lost wages, medical insurance, administrative costs, and several indirect costs – was \$1.3 million, based on 2009 data. Indirect costs associated with a single fatality could result in an amount three to ten times that of direct costs. To help employers and employees understand the importance of workplace health and safety, OSHA has three primary objectives. First, promoting cooperation between organizations and other stakeholders to improve workplace safety and health for all workers. This cooperation should lead to fewer hazards, reduced exposures, and fewer injuries, illnesses, and fatalities in the workplace. Second is increased employer and employee awareness of workplace safety and health. Active employer and employee participation in the company's safety and health programs should foster a culture that values and promotes workplace safety and health. And finally, greater public confidence in OSHA programs and services offered in the workplace.

All safety programs should be aimed at preventing injuries and minimizing hazards – conditions or activities that, if ignored, may result in injury or illness. Generally speaking, OSHA leaves it up to the individual organizations to develop their own safety programs. However, there are some provisions that OSHA does require as part of all programs. First, an organization-wide policy regarding the implementation of the program. Next, an effective hazard reporting system. Third, a description of roles and responsibilities. Fourth, a safety inspection. Fifth, training on safety processes and procedures, and finally, effective record-keeping for OSHA inspections.

Roles and responsibilities in an organization may vary according to its size and typical industry practices. However, regardless of size, management often plays a key role in developing policies and creating a culture that regards safety as an uncompromised goal. Management should demonstrate its commitment to safety by ensuring a needs analysis is conducted to identify safety hazards and unfulfilled requirements, and developing the appropriate safety goals, objectives, and policies. Then, ensure that safety audits or inspections are conducted

regularly to measure progress. Line managers must support and model safety and should be held accountable for the safety of employees on their teams. They should also play more tactical roles, such as monitoring employees' safety habits, recognizing or reporting hazards and accidents, conducting follow-up actions for prevention, and following up with employees after incidents or accidents are reported.

HR professionals are often the guiding force behind the development, administration, and evaluation of organizational safety and security programs. HR can assist in coordinating safety programs across various departments, provide education and training for line managers, and provide expertise on accident investigations and ways to prevent accidents in the future. However, HR needs to gain support from the leadership and management teams first in order to be successful.

Safety committees are also useful in promoting workplace safety and health. These committees are frequently made up of workers from different departments, roles, and levels of experience. The actions of a safety committee include encouraging employee participation in workplace safety, safety planning, and idea generation programs. Safety committees can play several roles in making the organization's safety efforts more effective. Committee members can encourage employees to follow sound safety practices, help to spread safety awareness among employees, review safety programs and provide feedback for their improvement, provide help in identifying and correcting safety hazards in the earliest stages, help organizations investigate serious accidents, and monitor maintenance and initiate corrective actions. In addition, it's vital to note that HR and management must ensure that the safety committee does not violate the National Labor Relations Act by becoming an employer-dominated labor organization.

[The National Labor Relations Act is also known as the NLRA.]

Organizations, often through safety committees, conduct internal safety inspections rather than waiting until OSHA does an official inspection. A voluntary safety inspection looks to prevent accidents by proactively looking for unsafe conditions or acts. Incidents are generally classified as resulting from either an unsafe act, unsafe condition, or a combination of both. Unsafe acts are under the control of employees, such as using equipment improperly or carelessly, following an unapproved procedure, failure to use personal protective equipment, not wearing recommended safety devices that are provided by the employer, or wearing inappropriate clothing. Unsafe conditions are classified as mechanical or physical hazards that are under the control of the employer, such as poor ventilation, unsuitable lighting, unsafe floor conditions, defective equipment or missing guards, and dust, heat, noise, and vibration.

As I mentioned, safety inspections are proactive measures the organization can take to prevent accidents. Still, accidents do happen and when they happen, the employer should be prepared to act quickly. A well-documented accident investigation and reporting process helps provide a safe working environment by determining the cause or causes of an accident and then documenting the issues so that accidents can be prevented in the future. The actual procedures often depend on the nature and results of the accident, but typically, conducting an accident investigation involves similar steps. First, the investigator must define the scope of the investigation. In some instances, additional accident investigators may be assigned specific tasks as part of an overall investigation. The main tasks include, first, a preliminary briefing including a description of the accident, the time and date it occurred, the environmental conditions, damage estimates, a list of the injured, the exact site of the accident, a witness list,

any pre-accident events that occurred, and the post-accident conditions. Next, the accident site must be visited, inspected, and secured. Anyone involved and any witnesses must be interviewed. In addition, anyone present before the accident, or who arrived at the site after the accident, must also be interviewed. Third, a likely sequence of events, the probable cause or causes, and any alternative sequencing must be identified in the fact-finding stage. Fourth, the accident investigation team must gather evidence from whatever sources necessary and appropriate. This includes witnesses and personal observations. Fifth, documents containing normal operating procedures, inspection reports, maintenance charts, or other reports are particularly useful to record pre-accident conditions, the accident sequence, and post-accident conditions. Sixth, conclusions and recommendations should contain short-term and long-term actions to prevent a reoccurrence. And lastly, the final steps are implementing the recommendations and conducting follow-ups as issues arise.

All safety actions are important, but they need to be prioritized. The top priority should be eliminating the hazard. If elimination is impossible, the next priority should be using safeguards so that the accidents do not occur. If the safeguards are not foolproof, providing training and instruction should be the next priority. And then, providing personal protective equipment to employees helps them avoid negative impacts on their health and safety.

Several factors may influence a workplace accident, including human factors and internal and external factors. Human factors include knowledge, skills, and abilities, attitudes and motivations, and distractions. Internal factors include the nature of the work, peers, management goals, and the organizational culture, the leader's style and effectiveness, machinery and tools, and proper orientation. External environmental factors include economic conditions, geographic conditions and the available labor force, and the regulatory environment.

Ergonomics is the science that addresses the way a physical environment is designed and how efficient and safe that design is for the people in the environment. The goal of an effective ergonomics program is to engineer risk factors out of the workplace and work environment. An ergonomic evaluation and subsequent redesign helps address physiological factors, such as lighting and ventilation; psychological factors, such as fatigue and stress; and engineering design factors, such as layout and tools. This process helps identify ways to reduce or eliminate injuries and accidents. An ergonomics program needs to have several key elements for its success: an ergonomics team consisting of employees and management to provide feedback on ergonomic issues and to work on ergonomic projects; work site analysis, including records reviews; an ergonomic hazards analysis, and periodic workplace surveys; an ergonomic evaluation and system for reporting symptoms; on-site exercise programs; and recommendations for redesign.

Some of the most common issues associated with workplace ergonomics are musculoskeletal disorders, or MSD, which can result from repeated stress to a part of the body that is caused by the way a task is performed. Computer vision syndrome, or CVS, is a name for several complex eye and vision problems caused by the use of a computer screen. Lower back strain injuries often result in pain, limited motion, muscle spasms, and general weakness of the lower back muscles. The term sick building syndrome, or SBS, refers to acute health and comfort effects employees experience that appear to be linked to time spent in a building, but with no specific illness or cause identified.

Employees' absence due to illness, injury, or disability and the transition back to work after a prolonged absence are among the most challenging human resource situations. Return-to-work programs, also known as modified duty programs, are designed to offer injured employees less strenuous jobs, usually on a temporary basis and under medical supervision, until the employee is fit to return to his or her regular job. An independent medical examination and assessment of the injured employee performed by a qualified and impartial doctor can provide guidance on the nature and scope of the modified duty needed to allow an employee to return to work. As part of an effective return to work program, the doctor conducting the exam outlines the injured worker's restrictions, so the organization can attempt to find a position that the worker can perform within those restrictions. Three specific employment laws should be considered when designing these programs: the Family and Medical Leave Act, the Americans with Disabilities Act, and the Fair Labor Standards Act. The FMLA and ADA dictate the length of time an employee may take job-protected leave, what position the employee must return to, and what may be considered reasonable accommodations. The FLSA will dictate whether the employee can be paid only for the hours worked under a reduced schedule, or if the employee must receive his or her full salary, regardless of the number of hours worked.

3. Review

Before we move on, we're going to pause for a moment so that you can answer some review questions.

There's a Review section in every topic, and each Review section provides a link to additional materials in the form of Topic Notes.

These notes cover everything we've talked about so far, and contain additional information that's pertinent to the PHR and SPHR exams.

Supplement

Selecting the link title opens the resource in a new browser window.

Topic Notes

Click here to launch the [Topic Notes](#) .

They'll also come in useful for some of the review questions.

Question

You need to identify and assess workplace safety, health, security, and privacy risks before you can develop and implement programs and procedures to manage them.

Sequence the steps in workplace risk assessment.

Options:

- A. Identify a workplace risk
- B. Decide who might be harmed and how
- C. Evaluate the risks and decide on precautions
- D. Record your findings
- E. Share your findings with management

Answer

Correct answer(s):**Identify a workplace risk is ranked**

The first step is to identify a workplace risk. You can do this by walking around your workplace, asking employees what they think, checking manufacturers' instructions, and reading the Occupational Safety and Health Administration (OSHA) regulations.

Decide who might be harmed and how is ranked

The second step is to decide who might be harmed and how. You can do this by identifying employees who work with hazardous materials or under hazardous conditions and listing how they can be harmed.

Evaluate the risks and decide on precautions is ranked

The third step is to evaluate the risks and decide on precautions. You can do this by evaluating the nature and amount of harm each risk could do, prioritizing hazards on an action plan, and then determining how to reduce or eliminate each one.

Record your findings is ranked

The fourth step is to record your findings. You should share them with a peer to be sure you covered all the bases. Then make an action plan and prioritize the actions you could take to make the workplace safer.

Share your findings with management is ranked

The final step is to share your action plan with management. Show the information you have collected and the changes that should be made to make the workplace safer.

Question

All workplace safety programs are aimed at preventing injuries and minimizing hazards. It's important that organizational stakeholders play a role in enforcing safety programs.

Match the stakeholders of the organization to their roles and responsibilities. Some stakeholders may be used more than once.

Options:

- A. Managers
- B. Line managers
- C. HR
- D. Safety committees

Targets:

1. Conduct periodic safety audits and inspections
2. Conduct follow-up action for prevention
3. Provide education and training for line managers
4. Encourage employees to follow sound safety practices
5. Review safety programs and provide feedback for their improvement
6. Help an organization investigate serious accidents

Answer

An organization's leadership and management can demonstrate commitment to safety by conducting a needs analysis to identify safety hazards and requirements, and setting safety goals, objectives, and policies accordingly. Management can also review current performance against predetermined goals and conduct safety audits or inspections regularly.

Line managers are generally responsible for the safety of employees on their teams. They play more tactical roles, such as monitoring employees' safety habits, recognizing and reporting hazards and accidents, conducting follow-up action for prevention, and following up with employees after incidents or accidents are reported.

HR professionals are often the guiding force behind the development, administration, and evaluation of security programs in organizations. However, HR needs to gain support from the organization's leadership and management. HR also provides education and training for line managers.

The role of safety committees includes encouraging employees to follow sound safety practices and helping to spread safety awareness among employees.

The role of safety committees includes reviewing safety programs and providing feedback for their improvement. Safety committees also help to identify and correct safety hazards in the earliest stages.

The role of safety committees includes helping an organization to investigate serious accidents. Safety committees also monitor maintenance and initiate corrective actions.

Correct answer(s):

Target 1 = Option A

Target 2 = Option B

Target 3 = Option C

Target 4 = Option D

Target 5 = Option D

Target 6 = Option D

Question

The actual procedures used in a particular accident investigation depend on the nature and results of the accident, but typically, the general steps remain the same.

Sequence the steps for conducting an accident investigation that must be performed before recommendations can be implemented.

Options:

- A. Preliminary briefing
- B. Accident site visit and interviews
- C. Fact-finding
- D. Gathering evidence
- E. Documentation
- F. Conclusions and recommendations

Answer

Correct answer(s):

Preliminary briefing is ranked

The first step is a preliminary briefing, which should include an accident description, time and date, environmental conditions, damage estimates, persons

injured, accident site location, witness list, pre-accident events, and post-accident conditions.

Accident site visit and interviews is ranked

In the second step, the accident site must be visited, inspected, and secured. Evidence at the accident site must not be disturbed until inspectors have an opportunity to examine it, except to the extent necessary to contain or control a hazard to employees or the public. Accident investigation team members must not subject themselves to hazardous conditions or environments that may exist at the accident site.

Fact-finding is ranked

In the third step, a likely sequence of events, the probable cause, whether it was root, indirect, or direct, and any alternative sequencing must be identified. A post-investigation briefing must be conducted and a summary report prepared. Upon distribution, the summary report should include the recommended actions necessary to prevent a recurrence.

Gathering evidence is ranked

In the fourth step, the accident investigation team should schedule the investigation so that evidence can be gathered from several sources. Information should be gathered from witnesses and reports, as well as by observation. Witnesses should be interviewed as soon as possible after an accident. The scene of an accident should be inspected before any changes occur.

Documentation is ranked

The fifth step involves gathering supporting documentation. Documents containing normal operating procedures, flow diagrams, inspection reports, maintenance charts, or reports of difficulties or abnormalities are particularly useful to record pre-accident conditions, the accident sequence, and post-accident conditions. It is also useful to document the location of those injured, witnesses, tools, equipment, machinery, energy sources, and hazardous materials. You should keep complete and accurate notes.

Conclusions and recommendations is ranked

The sixth step is to draw conclusions and make recommendations. Determine the root causes, indirect causes, and direct causes. The recommendations should contain short-term and long-term actions to prevent a recurrence. The seventh and final task in the process includes implementing the recommendations made in the earlier step and following up if any implementation issues arise.

Question

The workplace environment can cause a number of illnesses and disorders.

Match the symptoms to the corresponding workplace illnesses or disorders. Not every illness or disorder is used.

Options:

- A. Bursitis, tendonitis, and carpal tunnel syndrome
- B. Eyestrain, blurred distant vision, dry or irritated eyes, headaches, neck aches, backaches, and blurred near vision
- C. Pain, limited motion, muscle spasms, and general weakness of the lower back muscles
- D. Acute discomfort, headache, dry cough, dry or itchy skin, dizziness and nausea, difficulty concentrating, fatigue, sensitivity to odors, and eye, nose, or throat irritation

Targets:

- 1. Musculoskeletal disorder
- 2. Computer vision syndrome
- 3. Lower back strains
- 4. Sick building syndrome
- 5. Obstructive lung disease

Answer

A musculoskeletal disorder (MSD) results from repeated stress to a part of the body that is caused by the way a task is performed – for example, awkward postures, incorrect lifting, pushing, pulling, and prolonged repetitive motions. To prevent MSDs in the workplace, many organizations consider ergonomic workplace design, frequent breaks, job rotation and enrichment, and exercise programs.

Computer vision syndrome (CVS) is the complex of eye and vision problems that are characterized by visual symptoms which result from interaction with a computer display or its environment. In most cases, symptoms occur because the visual demands of the task exceed the visual ability of the individual to comfortably perform the task. Proper positioning of monitors, relative to the individual, will help avoid related problems.

Individuals with lower back strains may also have localized inflammation with redness, swelling, and cramping. A moderate or severe strain usually causes some loss of muscle function. Severe strains that partially or completely tear a muscle or tendon are often very painful and disabling. Employers can prevent or reduce the risk of back injuries by reorganizing work flow, redesigning jobs, reducing stressful body movements, reducing pace of work, planning rest breaks, and organizing training.

From an organization's perspective, the term sick building syndrome (SBS) refers to acute health and comfort effects employees experience that appear to be linked to time spent in a building, but where no specific illness or cause can be identified.

These effects could be linked to a particular room or zone, or may be widespread throughout the building. Improvement in ventilation and avoiding or reducing exposure to air and biological pollutants can reduce the risk of SBS.

Obstructive lung disease is a respiratory disease and could be irritated by the work environment, but it's not a workplace illness or disorder.

Correct answer(s):

Target 1 = Option A

Target 2 = Option B

Target 3 = Option C

Target 4 = Option D

Target 5 =No Option Specified.

Employee Health

Learning Objectives

After completing this topic, you should be able to

- *distinguish between infectious diseases*
- *distinguish between the three types of health hazards*
- *recognize when drug testing can be performed*

1. Introduction

Ignoring the possible impact of drug and alcohol abuse on any company may be a costly error.

In topic two, Employee Health, our focus will be on identifying employee health hazards, substance abuse, and the programs employers can offer to assist employees in these areas.

2. Employee health

Employee health and well-being is essential for the day-to-day functioning and the long-term success of any organization. Managing risks associated with employee health requires identifying and understanding the nature of various kinds of health hazards present in modern workplaces. Health hazards can be divided under three broad categories: infectious diseases, such as HIV and AIDS, Hepatitis B and C, tuberculosis, and future pandemics; environmental health hazards, such as chemical, physical, and biological health hazards; and other health hazards, such as fetal protection and toxic substances.

Infectious diseases are caused by pathogenic microorganisms, such as bacteria, viruses, parasites, or fungi, and these diseases can be spread directly or indirectly from one person to another. HR professionals need to be aware of OSHA Bloodborne Pathogen Standards and requirements regarding HIV/AIDS, hepatitis B, and hepatitis C. Blood-borne pathogens are microorganisms that are present in human blood and other potentially infectious materials, known as OPIM. OPIM includes nasal mucus, pleural fluid from the lungs, saliva, and any body fluid that is visibly contaminated with blood. HR professionals should also be aware of other infectious diseases, such as tuberculosis, and also issues related to preparing workplaces for possible pandemics. Generally, the courts have given employees with infectious diseases significant protections, treating infectious diseases as disabilities under the ADA. Under OSHA guidelines, each employer should create an individualized plan for reducing the risk of infectious diseases in the workplace. Usually the responsibility of educating their workforce regarding the risk and of the response to infectious diseases lies with employers.

HIV is the virus that causes AIDS. HIV attacks and weakens the body's immune system and then the body has difficulty fighting off infections, which over time leads to AIDS. AIDS is a fatal disease for which no known cure exists. It is spread mainly through exposure to infected blood, by skin injection, or by sexual contact. The risk of occupational exposure to HIV is considered very low, with few cases of AIDS directly traceable to workplace exposure. Hepatitis B poses the greatest risk to workers with occupational exposure. HBV is very

contagious and spreads primarily from exposure to blood of an infected person. Hepatitis B mainly affects liver function and is potentially life threatening. Hepatitis C is a liver disease caused by the hepatitis C virus, or HCV. HCV is primarily spread by contact with blood of an infected person and is extremely serious. Tuberculosis, or TB, is an airborne contagious lung disease caused by bacterial infection that is spread when someone with TB coughs or sneezes and expels pathogens. According to the World Health Organization, in order for a disease to take the form of a pandemic, it requires three elements: the agent must spread easily and sustainably among humans, the disease is new or currently unknown to the population, and the infection causes serious and widespread illness. Some examples of pandemic outbreaks include various influenza viruses, and specifically the recently identified H1N1 influenza strain.

OSHA regulations strive to improve safety by reducing the risk of loss due to hazards in the working environment. Major environmental health hazards include chemical health hazards, physical health hazards, and biological health hazards. A chemical health hazard is any element or chemical compound in the workplace that carries a risk of causing immediate or long-term health problems. For example, dry-cleaning solvents, gasoline, and ammonia are toxic and carcinogenic hazards. A physical health hazard is anything that can cause a physical injury – for example, an unsecured electrical cord or a door that opens too far into a hallway. Most workplaces are loaded with potential physical hazards, but they are often easy to spot and easy to fix. Biological health hazards are agents like bacteria, viruses, fungi, other microorganisms, and their associated toxins. All of these things can invade any workplace and cause illness. The healthcare and food preparation industries are at greater risk than other industries from biological agents, but all HR professionals should understand the possible effects of infectious diseases in the workplace.

Fetal protection policies attempt to protect the fetus from workplace hazards. However, Title VII, as amended by the Pregnancy Discrimination Act, makes many of the fetal protection policies, which were adopted by many employers, unlawful. Fetal protection policies often reflect a concern for the vulnerability of the fetus, especially regarding products that affect a fetus, but not the pregnant mother. In previous challenges, the US Supreme Court has held that these policies violate equal employment laws and the bona fide occupational qualification, or BFOQ, defense does not apply. Toxic or hazardous substances may pose significant health risks to employees and may have long-term health consequences. To ensure that employees are informed about the hazardous substances they work with, OSHA requires that each employee dealing with hazardous substances must have a material safety data sheet, or MSDS, on each substance. Prepared by the manufacturer, an MSDS contains all the information an employee needs to understand about the potential hazards of each chemical, including how to treat exposures to that chemical.

Employee assistance programs, or EAPs, are employer-sponsored programs that deal with behavioral and health-related services. EAPs often include legal support, financial advice, psychological counseling, crisis management, childcare assistance, and substance abuse counseling. The specific elements of EAPs vary between organizations, but one common thread is that services are generally provided by licensed professionals or organizations and offer employees a high degree of confidentiality. Many times, a company's EAP offers services or support systems that employees may not have access to or be able to otherwise afford. EAPs can also help employers by adding value to benefits packages, influence job designs, improve labor relations by facilitating cooperation between management and employees, and have a positive effect on recruitment and staff retention.

Wellness programs can help improve the physical well-being of employees on and off the job. These programs usually focus on preventative activities and help with stress management, burnout, violent behavior, and chemical dependency and abuse issues. Wellness programs typically offer exercise and physical fitness programs, health risk evaluations, nutrition education, weight management, smoking cessation programs, flu shots, and first aid and CPR training. Employee wellness programs can also benefit the organization by reducing medical costs and insurance premiums, preventing illness and absenteeism, increasing productivity and morale, lowering employee replacement costs, and attracting highly qualified employees.

Alcohol and drug abuse is a disturbing issue throughout the world. Statistics from the Center for Substance Abuse Treatment indicate that 70% of America's substance abusers are employed. Further, it's estimated that 40% of industrial fatalities and almost 50% of industrial injuries are linked to alcohol consumption and alcoholism. In addition, drug-abusing employees are estimated to be responsible for almost 40% of employee thefts. Ignoring the possible impact of drug and alcohol abuse on any company may be a costly error. The negative impact on businesses include increased absenteeism and tardiness, more workplace accidents, and higher healthcare and insurance premium costs. Drug and alcohol abusers enrolled in a recovery program are considered to be disabled and are protected under the Americans with Disabilities Act. Because of these protections, employers must be extremely careful when taking any disciplinary actions against those employees, unless the disciplinary action is clearly unrelated to the substance abuse problem. Otherwise, the disciplinary action may lead to discrimination claims. To further avoid discrimination claims, substance abuse programs must be implemented fairly and equally throughout the organization. Therefore, if one individual is drug tested, everyone in the same category must be drug tested.

[Substance-using employees that are in a recovery program are also protected under the Rehabilitation Act.]

Organizations should have a plan in place to deal with drug abuse issues, such as creating and implementing corporate policies on substance abuse, training and educating managers and supervisors on substance abuse, educating and communicating policies on substance use to employees, being aware of some of the early warning signs of substance abuse, drug testing when drug use is reasonably suspected, using interventions such as constructive confrontation and counseling, and referring employees to professionals for treatment. Employers require drug testing at a variety of points in the employment relationship. Testing prior to employment may be done only after a candidate receives and accepts a conditional job offer. Testing may be done where there is reasonable suspicion of drug use. Testing on scheduled dates is generally the least effective testing program, because employees can take the necessary steps to ensure a clear test. However, scheduled testing can be effective for monitoring employees in a recovery program. Random drug testing can be very effective; however, the test must generally be random in order to be lawful. And post-accident testing is done when an employee is involved in an accident or unsafe practice, in order to determine if alcohol or drugs were a factor.

3. Review

OK, review time again. Let's try some questions.

Supplement

Selecting the link title opens the resource in a new browser window.

Topic Notes

Click here to launch the [Topic Notes](#) .

Question

Infectious diseases are caused by pathogenic microorganisms such as bacteria, viruses, parasites, or fungi. The diseases can be spread, directly or indirectly, from one person to another.

Match each infectious disease to its description.

Options:

- A. HIV/AIDS
- B. Hepatitis B
- C. Tuberculosis
- D. Hepatitis C

Targets:

1. The risk of occupational exposure is low. This infection attacks and weakens the body's immune system.
2. It poses the greatest risk to workers with occupational exposure. It mainly affects liver function. A vaccine is available.
3. It is a bacterial infection in the lungs spread through the coughing or sneezing of an infected person.
4. Most infected people develop chronic liver infections. No vaccine is available.

Answer

HIV is the virus that causes AIDS. HIV attacks and weakens the body's immune system. The body then has difficulty fighting off infections, which, over time, leads to AIDS. AIDS is a fatal disease for which no known cure exists. It is spread mainly through exposure to infected blood by skin injection or by sexual contact.

Hepatitis B poses the greatest risk to workers with occupational exposure. HBV is very contagious and spread primarily from exposure to the blood of an infected

person. The disease can lead to more serious chronic conditions, such as cirrhosis, liver failure, and liver cancer. A vaccine is available for HBV.

Tuberculosis, or TB, is an airborne, contagious lung disease caused by a bacterial infection that is spread when someone with TB coughs or sneezes, expelling pathogens. Those at higher risk for contracting TB in the workplace are people who share the same breathing space, such as coworkers.

Hepatitis C is a liver disease caused by the hepatitis C virus, or HCV. HCV is primarily spread by contact with the blood of an infected person. The symptoms are similar to hepatitis B. Most infected people develop chronic liver infections. No vaccine is available.

Correct answer(s):

Target 1 = Option A

Target 2 = Option B

Target 3 = Option C

Target 4 = Option D

Question

An organization can't remove hazards from the workplace, but it can reduce the risks of employees becoming injured or sick by using proper safety precautions and training employees to deal properly with the hazards.

Match the examples to the corresponding health hazards. Some hazards have more than one match.

Options:

- A. Dry-cleaning solvents
- B. A hole in the ground without signage
- C. An unsecured phone cord
- D. Loose clothing when operating moving machinery
- E. Badly preserved foods
- F. Moldy surfaces

Targets:

1. Chemical hazard

2. Physical hazard
3. Biological hazard

Answer

A chemical health hazard is defined in the OSHA statute, but may be considered to be any element or chemical compound in the workplace that carries a risk of causing immediate or long-term health problems. For example, dry-cleaning solvents, gasoline, and ammonia are toxic and carcinogenic hazards.

A physical health hazard is anything that can cause a physical injury. For example, an unsecured phone or electrical cord, a wastebasket shoved too far into a hallway, or a hole in the ground without signage can cause a fall. Most workplaces are loaded with potential physical health hazards, but they are often easy to spot and fix.

Biological health hazards are agents like bacteria, viruses, fungi, other microorganisms, and their associated toxins. All of these agents can invade any workplace and cause illness. The healthcare and food preparation industries are at greater risk than other industries from biological agents. But all HR professionals must understand the possible effects of infectious diseases in their workplaces.

Correct answer(s):

Target 1 = Option A

Target 2 = Option B, Option C, Option D

Target 3 = Option E, Option F

Question

It's important to understand your organization's policies, as well as the legal limitations to drug testing.

When can drug tests be performed?

Options:

1. Pre-employment
2. With reasonable suspicion and for cause
3. Periodically
4. Randomly
5. Post-accident

6. As part of pandemic prevention

Answer

Option 1: This option is correct. Testing prior to employment may be done only once the candidate has accepted a conditional job offer. The testing must be done uniformly; you can't test just one applicant. You can either test everyone or you can test the employees according to work-based categories.

Option 2: This option is correct. Testing may be carried out on reasonable suspicion after an incident leads a supervisor to suspect substance abuse. The testing must be done on everyone in a work-based group.

Option 3: This option is correct. Testing that is carried out on scheduled dates tends to be the least effective testing program. This is because employees can pre-empt the test, and take the necessary precautions. Scheduled testing is, however, effective when monitoring employees in recovery programs.

Option 4: This option is correct. Random drug tests are very effective. However, the tests must be genuinely random. You can use a computer program to select random names, or even pull names out of a hat. Alternatively, you can perform random testing on an entire work-based group.

Option 5: This option is correct. Post-accident testing is done on an employee involved in an accident or unsafe practice to determine whether alcohol or drug abuse was a factor.

Option 6: This option is incorrect. Testing for drug use cannot prevent future pandemics. Substance abuse programs can help prevent workplace accidents, low morale, increased absenteeism and tardiness, and higher healthcare and compensation costs.

Correct answer(s):

1. Pre-employment
2. With reasonable suspicion and for cause
3. Periodically
4. Randomly
5. Post-accident

Workplace Security

Learning Objectives

After completing this topic, you should be able to

- *identify the measures that can be implemented to protect an organization's assets*
- *identify the steps in the risk analysis process*
- *identify the elements of an emergency response plan*
- *identify workplace security threats*

1. Introduction

Workplace security involves the physical and procedural measures taken to protect company assets.

In topic three, Workplace Security, we'll discuss workplace and organizational threats, security risk analysis methods, emergency response planning, and workplace violence.

2. Workplace security

Workplace security involves the physical and procedural measures taken to protect company assets and reduce or eliminate internal and external threats to those assets. Companies face physical, human, financial, and intellectual loss resulting from external threats and internal vulnerabilities like natural disasters, such as fires, earthquakes, hurricanes, and tornadoes; man-made disasters, such as terrorist attacks, workplace violence, industrial sabotage, and theft; the intentional or unintentional release of information, such as trade secrets, intellectual property, and confidential information.

An organization can implement a variety of measures to protect its business assets from potential loss. Important and valuable business assets include the physical assets of an organization, like buildings, property, computers, vehicles, heavy machinery, and equipment that the organization owns. Protective measures include fire alarms, smoke detectors, and locks, as well as the use of security guards, gates, cameras, entry barriers, and security programs. An organization's employees are its human assets. Restrict the distribution of keys, change locks when keys aren't returned, and also implement the same measures used to protect physical assets to protect your employees. The intellectual assets of an organization include customer lists, inventions, software code, business operations, and other confidential organization information. To protect its intellectual property, an organization can use nondisclosure agreements. Cash, inventories, and accounts receivable make up the organization's financial assets. An organization can use internal financial controls to prevent the loss of financial assets and ensure that financial assets are not mishandled, stolen, or embezzled.

In order to plan and implement a workplace security program that reduces the risks that organizations face, safety and security managers should perform a security risk analysis. Using the information from the risk analysis, security managers can then implement security

measures and controls to protect the organization's assets from the emergencies that are most likely to occur. The first step in the risk analysis process is to identify and list all the external forces or threats, and internal weaknesses or vulnerabilities that the organization faces. In step two, the safety and security manager calculates the probability of occurrence and potential financial cost of specific emergencies. In the third step, the severity of the impact of specific emergencies on business operations is determined. Severity should be rated as fatal to the organization, most severe, very serious, moderately serious, and negligible, which is the least severe. In the fourth and final step of the risk analysis process, the safety and security manager should develop security and fire prevention plans that prevent damage to business assets. In addition, vulnerability can be estimated with a commonly used risk analysis formula – that is, vulnerability equals degree of probability a loss will occur plus the severity of the impact of that loss.

[Heading: Security Risk Analysis, Risk Analysis Process In order to plan and implement a workplace security program that reduces the risks that organizations face, safety and security managers need to perform a security risk analysis. It includes several stages: identifying threats, assessing probability and costs, assessing impact, and developing plans.]

To be prepared for emergencies, such as fires, floods, earthquakes, severe storms, or terrorist attacks, and ensure the safety of employees and business assets, organizations need to develop an emergency response plan as part of their integrated security plan. Emergency response plans provide information on the procedures for reporting emergencies and the course of action to follow in different emergency situations. The procedure for conducting and shutting down critical operations is detailed in these plans, and the procedures for emergency evacuations are contained as well. These plans also list the names and job titles of office emergency action plan coordinators, the individuals responsible for training staff members in emergency procedures and taking roll call after evacuations. It also contains the names of people responsible for reporting an emergency to the authorities, those who perform critical plant operations, and anyone who can perform rescue and medical duties in emergencies. An emergency response plan should also address how to warn employees of an emergency. It describes alarm systems, where the alarms are located, the type of emergency a specific alarm indicates, what the alarm systems sound like, and whether the alarm notifies emergency personnel. The plan also needs to include information on training employees in emergency procedures. A schedule for training and emergency drills should also be developed. And finally, records of the maintenance of safety equipment and equipment inspections, as well as training records and plans of the building are included in the plan because these documents are useful in emergency situations.

Mandated plans are required by OSHA and the Environmental Protection Agency. OSHA's Process Safety Management standard requires employers who store, manufacture, or use highly hazardous chemicals, toxins, or reactive materials to have emergency response plans and provide training to their workers. Further, the EPA's standard under Section 112(r) of the Clean Air Act requires employers to notify governmental authorities about such substances that are maintained at the job site, provide information on emergency contingency plans, coordinate response efforts, and outline worst-case scenarios. The Federal Emergency Management Agency has developed an emergency management guide for business and industry that works as a step-by-step guide to emergency planning, response, and recovery for organizations.

Workplace theft and frauds are serious threats to an organization's legal, financial, and operational security. Organizations need to put measures in place to make sure that integrity and ethics are maintained and practiced from the top-down. Workplace fraud occurs when someone knowingly lies to obtain a benefit or an advantage, or to ensure a benefit is denied. Fraud is divided into three major categories: embezzlement, corruption, and fraudulent documents. Organizational areas that are vulnerable to workplace theft and fraud and require internal operational and financial controls include financial management practices, procurement, corporate credit cards, and business expenses. A workplace investigation represents an organization's best efforts to sort through and document all sides of a complaint, to resolve it, and to take appropriate disciplinary action. Investigations require authorization to undertake the investigation, a commitment to confidentiality, creation of a findings report, and possibly cooperation with law enforcement authorities.

Workplace violence is directed toward people at work or on duty, and occurs when individuals react to a situation with threatening behavior, harassment, verbal abuse, physical assault, or the threat of assault. According to OSHA, workplace violence is any act or threat of physical violence, harassment, intimidation, or other threatening disruptive behavior that occurs at a work site. It ranges from threats and verbal abuse to physical assaults and even homicide. Potential causes of workplace violence include excessive stress, personality conflicts, a mishandled termination or other disciplinary action, weapons which are taken onto a work site, drug or alcohol use on the work site, and personal circumstances. Organizations can prepare for acts of workplace violence by developing and communicating a workplace security program to all employees. This involves determining if any acts of workplace violence are likely to occur, and developing and implementing steps to prevent any incidents.

Terrorism is the use of force or violence against persons or property in violation of criminal laws of the United States for purposes of intimidation, coercion, or ransom. The Federal Bureau of Investigation, or FBI, categorizes terrorism in the United States as one of two types. First, domestic terrorism, which involves groups or individuals whose terrorist activities are without foreign direction. And second, international terrorism, which involves groups or individuals whose terrorist activities are foreign-based or whose activities transcend national boundaries. A terrorist incident can take many forms and an organization's response must vary depending on the type of attack. Antiterrorism regulations and responses to attacks of terrorism include the passage of the USA PATRIOT Act, creation of the Department of Homeland Security, or DHS, and the National Response Framework by DHS.

3. Review

Now, let's take a look at some review questions.

Supplement

Selecting the link title opens the resource in a new browser window.

Topic Notes

Click here to launch [Topic Notes](#) .

Question

An organization can implement a variety of measures to protect its business assets from potential loss.

Which options are examples of measures organizations can use to protect their assets?

Options:

1. Fire alarms
2. Security pass cards
3. Intellectual property agreements
4. Audit committees
5. Stress management
6. Regular physicals

Answer

Option 1: This option is correct. The physical assets of an organization include organization buildings, property, computers, vehicles, heavy machinery, and equipment that the organization owns. To protect its physical assets, an organization can install fire alarms, smoke detectors, and locks, as well as use security guards, gates, cameras, entry barriers, and security programs.

Option 2: This option is correct. An organization's employees are its human assets. Organizations can restrict the issuing of security passes, and use security guards and gates to protect their human assets. They can also provide training on how to react in emergencies, and develop plans for preventing workplace violence, such as antiharassment and antibullying policies.

Option 3: This option is correct. The intellectual assets of an organization include customer lists, inventions, software code, business operations, and other confidential organization information. To protect its intellectual property, an organization can use intellectual property agreements or nondisclosure agreements to ensure that employees are aware of restrictions and confidentiality.

Option 4: This option is correct. Cash, product and supply inventories, and accounts receivable make up an organization's financial assets. An organization can use internal financial controls – for example, audit committees, accurate financial recording, and proper financial authorization and approval – to prevent the loss of these financial assets.

Option 5: *This option is incorrect. Stress management is a type of health and wellness program that an organization may choose to implement, but it's not a way for an organization to protect its assets.*

Option 6: *This option is incorrect. Regular physicals to assess health and fitness are often offered as part of an organization's wellness program. However, this isn't a way for an organization to protect its assets.*

Correct answer(s):

1. Fire alarms
2. Security pass cards
3. Intellectual property agreements
4. Audit committees

Question

In order to plan and implement a workplace security program that reduces the risks that organizations face, safety and security managers need to perform a security risk analysis.

What are the steps to the risk analysis process?

Options:

1. Identifying workplace security risks
2. Assessing probability and costs of the risks
3. Assessing impact of the risks on the organization
4. Developing workplace security plans
5. Identifying the strategic role of safety committees in employee safety
6. Eliminating all workplace safety risks

Answer

Option 1: *This option is correct. Identifying and listing all the external forces, or threats, and internal weaknesses, or vulnerabilities, that the organization faces is the first step in the risk analysis process. These risks can include man-made threats, natural disasters, and the unintentional release of information.*

Option 2: *This option is correct. Assessing the probability and costs of the risks is part of the risk analysis process. The safety and security manager calculates the*

probability of occurrence and potential financial costs to the organization should the identified emergencies occur.

Option 3: *This option is correct. Assessing the impact of these risks on business operations is part of the risk analysis process. The severity of the impact on the organization can be rated as fatal to the organization, very serious, moderately serious, or negligible. Next, the emergencies are ranked so that the organization can focus on addressing those with the highest probability, costs, and operational impact first.*

Option 4: *This option is correct. The final step is for the safety and security manager to develop security and fire prevention plans that aim to prevent damage to business assets. The organization also develops emergency action plans that aim to reduce the effect of an emergency situation on the organization and its employees.*

Option 5: *This option is incorrect. Identifying the strategic role of a safety committee is not part of the risk analysis process. Safety committees encourage employees to follow sound safety practices, help spread safety awareness, and review programs to provide feedback. They should already be a stakeholder in the organization's workplace security programs.*

Option 6: *This option is incorrect. This is not one of the steps in the risk analysis process. You can reduce workplace safety risks, but it's close to impossible to eliminate all workplace risks.*

Correct answer(s):

1. Identifying workplace security risks
2. Assessing probability and costs of the risks
3. Assessing impact of the risks on the organization
4. Developing workplace security plans

Question

Emergency response plans document the actions employers and employees should take, as well as their responsibilities in the event of emergency situations at work. These plans contain several elements that describe how the employers and employees in an office should deal with an emergency situation.

What are these elements?

Options:

1. Procedures
2. Responsibilities

3. Notification
4. Training
5. Record-keeping
6. Drug testing policy

Answer

Option 1: This option is correct. Emergency response plans provide information on the procedures for reporting emergencies and the course of action to follow in different emergency situations.

Option 2: This option is correct. Emergency response plans identify the office emergency action plan coordinators, emergency procedure trainers, and those who must take roll call after evacuation. In addition, it identifies the people responsible for reporting the emergency to the authorities, those who perform critical plant operations, and those who perform rescue and medical duties in emergencies.

Option 3: This option is correct. An emergency response plan addresses how to warn employees of an emergency. It describes alarm systems, where the alarms are located, the type of emergency a specific alarm indicates, what the alarm systems sound like, and whether the alarm notifies emergency personnel.

Option 4: This option is correct. Emergency response plans need to include information on how an organization plans to train employees in emergency procedures. A schedule for training and emergency drills should also be developed.

Option 5: This option is correct. Records of the maintenance of safety equipment and equipment inspection, as well as training records and plans of the building, are included in the plan because these documents are useful in emergency situations.

Option 6: This option is incorrect. A drug testing policy should be documented in the organizational policy and signed by employees. It is not part of the emergency response plan.

Correct answer(s):

1. Procedures
2. Responsibilities
3. Notification
4. Training
5. Record-keeping

Question

Match the examples to the corresponding workplace security threats. More than one example may match to each threat, and some examples will not have a match.

Options:

- A. Counterfeit documents
- B. Verbal abuse
- C. Intimidation
- D. Bomb threats
- E. HIV/AIDS

Targets:

- 1. Theft and fraud
- 2. Workplace violence
- 3. Terrorism

Answer

Workplace theft and fraud are serious threats to an organization's legal, financial, and operational security. Workplace fraud occurs when someone knowingly lies to obtain a benefit or advantage, or to cause some benefit that is due to be denied. Fraud is divided into three major categories: embezzlement, corruption, and fraudulent documents.

Workplace violence is directed toward people at work or on duty and occurs when individuals react to a situation with threatening behavior, harassment, verbal abuse, physical assault, or the threat of assault.

Terrorism is the use of force or violence against persons or property in violation of the criminal laws of the United States for purposes of intimidation, coercion, or ransom. Terrorism includes bomb threats, biological attacks, and building explosions.

Correct answer(s):

Target 1 = Option A

Target 2 = Option B, Option C

Target 3 = Option D

Workplace Privacy

Learning Objectives

After completing this topic, you should be able to

- *identify employer monitoring and search practices*
- *identify workplace privacy concerns*

1. Introduction

The biggest privacy concern for employers is protecting proprietary information.

In topic four, Workplace Privacy, we'll examine internal and external security and privacy policies, the appropriate use of electronic media and hardware such as e-mail, social media, and Internet access, data integrity techniques, and technology applications.

2. Workplace privacy

Balancing employee privacy and the employer's need for monitoring is an ongoing and delicate process. Employers justify monitoring to deal with fraud and theft, to safeguard intellectual property due to increasing litigation over harassment and discrimination and resource misuse and productivity challenges. Workplace monitoring is also important because of increased security precautions in the face of terrorist threats. Today employers are monitoring employee e-mail, phone calls, and the contents of computer files. Other examples of privacy-invasive employee monitoring include drug testing, closed-circuit video monitoring, Internet monitoring and filtering, instant message monitoring, location monitoring, personality and psychological testing, and keystroke logging.

A written privacy policy explains the employer's rights in the event that monitoring, searches, and investigations are necessary. It notifies employees of the level of privacy that is reasonable to expect in the workplace and it explains the employer's policies regarding certain types of monitoring and searches. A privacy policy should outline the steps involved in conducting a search and spell out exactly what the employer can monitor and search. These policies should always be reviewed against applicable laws and regulations to ensure complete compliance.

While employees commonly use e-mail and instant messaging for business and personal use, most employees don't realize that e-mail and instant messages that are sent using the employer's equipment are the property of the employer. And those messages can be monitored, reviewed, and seized at any time, unless the employer's policies have lead the employee to expect a higher level of privacy. Phone calls may or may not be private. Computers that are used at work and all their contents belong to the employer and are subject to search at any time. Many employers reserve the right to review data stored on hard drives. The privacy policy should include a statement of acceptable Internet uses, reasons to restrict access or use, and whether or not the employer allows personal use of Internet resources. In addition, video surveillance is an important security tool. However, employers that use video surveillance must generally inform their employees that surveillance is being used. Restricting

cell phone use is difficult and problematic for many employers. However, cell phone cameras are a different story. They've been used to harass and embarrass others, as well as to photograph proprietary work processes and classified documents. Employers should define what they consider inappropriate cell phone camera use in their privacy policies and carefully monitor these devices. And finally, employers generally have the ability to search their employees' work area and their personal property, such as purses, backpacks, and vehicles parked on company property.

The biggest privacy concern for employers is protecting proprietary information in the face of various privacy challenges today's technologies present. Proprietary information provides the organization with a competitive advantage and can be critical to the organization's sustainability and profitability. If organization's proprietary information is intentionally or unintentionally passed on to the competitors, an organization's competitive edge, sustainability, and profitability can be seriously compromised. In addition, proprietary information is threatened when current and former employees, may attempt to use trade secrets and other information for their own advantage. Companies can safeguard against proprietary information leaks, corporate espionage, and corporate sabotage by conducting a needs assessment to determine proprietary information most valuable to the organization, its vulnerability and the protections needed; conducting a threat analysis to identify internal and external threats; requiring employees, suppliers, and other stakeholders to sign confidentiality and nondisclosure agreements; training managers and supervisors and employees about the organization's policies, protection plan, and security of intellectual properties; and limiting access to proprietary knowledge on a need-to-know-only basis.

Access to proprietary information, such as financial accounts, inventories, customer data, marketing plans and schedules, sales figures, production data, e-mails, and personal employee information stored on company computers or servers should definitely be restricted. Security protocols for workstations, networks, databases, software, and servers should be maintained and followed and any breaches should be considered a potential risk to the organization's sensitive information. Security plans and environmental systems should be in place to guard computers and their files. These files contain proprietary and valuable information and should be protected against temperature, smoke, dust, fire, and water damage. Data should be routinely backed up and stored electronically at different secure places to provide easy access as needed or in the event of a system or software failure. And ongoing protection should include secure file backups off-site in the event of any facility or technology disaster.

Identity theft is also a growing concern for HR departments and employees alike. An individual's name, date of birth, address, credit card, Social Security details, and other personal identification information can be used to open credit card and bank accounts, redirect mail, establish cell phone service, rent vehicles and equipment, and even for employment. With the explosion of Internet use, information sharing, online services, and social media, organizations should expect increased incidence of compromised personal information. This results in increased legal liability, so managers and HR professionals should be careful when collecting, saving, and retrieving employee and customer information. The Federal Trade Commission, or FTC, has issued policies governing employer disposal of applications and employee records, and some states have passed laws to protect employee data and the use of Social Security numbers. Balancing employers' needs for ensuring productivity and workplace security and safety with the employees' need for privacy and autonomy is a difficult challenge.

Social media has increasingly blurred the line between private and public life and made the balancing act even more complicated. New technologies make it possible for employers to monitor their employees, especially on telephones, computer terminals, through e-mail and voicemail, and when employees are using the Internet. To avoid problems under the Electronic Communications Privacy Act, or ECPA, employers should not monitor e-mails when they're in transmission, only after transmission is complete and the e-mails are in storage.

3. Review

So, here's the next set of review questions.

Supplement

Selecting the link title opens the resource in a new browser window.

Topic Notes

Click here to launch [Topic Notes](#) .

Question

Which actions are employers allowed to take while monitoring for privacy and security in the workplace?

Options:

1. Monitor and review employee e-mails
2. Listen to phone calls
3. Monitor computer and Internet usage
4. Watch video surveillance footage
5. Monitor cell phone usage
6. Conduct a body search

Answer

Option 1: *This option is correct. Employees use e-mail and instant messaging all the time for both business and personal use. Most employees don't realize that messages sent using the employer's equipment are the property of the employer. As such, they can be monitored, reviewed, and seized at any time, unless the employer's policies have led the employees to expect otherwise.*

Option 2: *This option is correct. Phone calls may or may not be private. Some states require that employees be informed that their calls are being monitored. Generally, employer monitoring must stop if the call turns out to be personal.*

Option 3: *This option is correct. Computers that are used at work and all their contents belong to the employer and are subject to monitoring and search at any time. The privacy policy should include a statement of acceptable Internet use, reasons to restrict access or use, and whether or not the employer allows personal use.*

Option 4: *This option is correct. Video surveillance is an important security tool. However, employers that use video surveillance must generally inform their employees that surveillance is in effect and why it is being used. They should also spell out conditions under which tapes will be reviewed, and how the information from them will be used.*

Option 5: *This option is correct. Cell phones are ubiquitous in the workplace. Restricting cell phone use is difficult and problematic for an employer. However, cell phone cameras are a different story. They have been used to harass and embarrass others, as well as to photograph proprietary work processes and classified documents. Employers should define what they consider inappropriate cell phone camera use in their privacy policies, and carefully monitor these devices.*

Option 6: *This option is incorrect. Generally, employers are allowed to search employees' workplaces and their personal property, not their bodies. The privacy policy should state the kinds of property that are subject to search – for example, desks, purses, backpacks, and cars. It should also spell out the kinds of situations that will result in a search, and how the search will be conducted.*

Correct answer(s):

1. Monitor and review employee e-mails
2. Listen to phone calls
3. Monitor computer and Internet usage
4. Watch video surveillance footage
5. Monitor cell phone usage

Question

Which options are privacy concerns for employers and employees?

Options:

1. Protection of proprietary information
2. Technology security

3. Safety of computer files
4. Identity theft
5. Invasive employee monitoring
6. Terrorism

Answer

Option 1: This option is correct. If an organization's proprietary information is passed on to its competitors, the organization's competitive edge, sustainability, and profitability can be seriously compromised. Proprietary information is also threatened if current and former employees attempt to use trade secrets and other information for their own advantage.

Option 2: This option is correct. More organizations and organizational functions are moving to technology-based architecture. The safety of valuable information and organizational systems depends on how effective the technology's security is.

Option 3: This option is correct. Security plans and environmental systems should be in place to guard equipment and computer files with proprietary and valuable information against temperature, smoke, dust, fire, and water damage. Even computer files that don't contain proprietary information should be carefully protected.

Option 4: This option is correct. Identity theft is a growing concern for HR departments and employees alike. An individual's name, date of birth, address, credit card, Social Security details, and other personal identification information can be used to open credit card and bank accounts, redirect mail, establish cellular phone service, rent vehicles, equipment, or accommodations, and even secure employment.

Option 5: This option is correct. New technologies make it possible for employers to monitor many aspects of their employees' jobs. This has been a matter of concern for employees and employee rights advocates. To avoid problems under the Electronic Communications Privacy Act (ECPA), employers shouldn't monitor e-mails while they are in transmission, but rather only after transmission is complete and the e-mails are in storage.

Option 6: This option is incorrect. Terrorism is the use of force or violence against persons or property in violation of the criminal laws of the United States for purposes of intimidation, coercion, or ransom. Terrorism is a workplace security concern and not a privacy concern.

Correct answer(s):

1. Protection of proprietary information
2. Technology security
3. Safety of computer files
4. Identity theft
5. Invasive employee monitoring

© 2018 Skillsoft Ireland Limited