(b) Each employee shall comply with occupational safety and health standards and all rules, regulations, and orders issued pursuant to this Act which are applicable to his own actions and conduct.

Other Considerations or Expensive Research QUESTION NO: s for Lawyers (Sorry, Eddie!)

The Foreign Corrupt Practices Act of 1977
Internal Revenue Service (IRS) Law for Protecting Taxpayer Information Food and Drug Administration (FDA) Mandated Requirements Homeland Security and Terrorist Prevention Pandemic (Bird Flu) Prevention
ISO 9000 Certification
Requirements for Radio and TV Broadcasters
Contract Obligations to Customers
Document Protection and Retention Laws
Personal Identity Theft...and MORE!

Suffice it to say you will need to check with your legal department for specific requirements in your business and industry!

I would like to thank my good friend, Eddie
M.Pope, for his insightful contributions to this article, our upcoming book, and my ever-growing pool of lawyer jokes. If you want more information on the legal aspects of recovery planning, Eddie can be contacted at my company or via email at mailto:mempope@tellawcomlabs.com. (Eddie cannot, of course, give you legal advice, but he can point you in the right direction.)

I hope this article helps you better understand the complex realities of the legal reasons why we plan and wish you the best of luck

See original article at:
http://www.informit.com/articles/article.aspx?p=777896
See another interesting article on the subject at:
http://www.informit.com/articles/article.aspx?p=677910&seqNum=1

References used for this question:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 281).

QUESTION 574
The absence of a safeguard, or a weakness in a system that may possibly be exploited is called a(n)?

A. Threat
B. Exposure
C. Vulnerability
D. Risk

Correct Answer: C
Explanation:
A vulnerability is a weakness in a system that can be exploited by a threat.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 237.
QUESTION 575

When first analyzing an intrusion that has just been detected and confirming that it is a true positive, which of the following actions should be done as a first step if you wish to prosecute the attacker in court?

A. Back up the compromised systems.
B. Identify the attacks used to gain access.
C. Capture and record system information.
D. Isolate the compromised systems.

Correct Answer: C
Explanation:
When an intrusion has been detected and confirmed, if you wish to prosecute the attacker in court, the following actions should be performed in the following order:

Capture and record system information and evidence that may be lost, modified, or not captured during the execution of a backup procedure. Start with the most volative memory areas first.
Make at least two full backups of the compromised systems, using hardware-write- protectable or write-once media. A first backup may be used to re-install the compromised system for further analysis and the second one should be preserved in a secure location to preserve the chain of custody of evidence.

Isolate the compromised systems.
Search for signs of intrusions on other systems.
Examine logs in order to gather more information and better identify other systems to which the intruder might have gained access.
Search through logs of compromised systems for information that would reveal the kind of attacks used to gain access.
Identify what the intruder did, for example by analyzing various log files, comparing checksums of known, trusted files to those on the compromised machine and by using other intrusion analysis tools.

Regardless of the exact steps being followed, if you wish to prosecute in a court of law it means you MUST capture the evidence as a first step before it could be lost or contaminated. You always start with the most volatile evidence first.

NOTE:
I have received feedback saying that some other steps may be done such as Disconnecting the system from the network or shutting down the system. This is true. However, those are not choices listed within the 4 choices attached to this question, you MUST avoid changing the question. You must stick to the four choices presented and pick which one is the best out of the four presented.

In real life, Forensic is not always black or white. There are many shades of grey. In real life you would have to consult your system policy (if you have one), get your Computer Incident team involved, and talk to your forensic expert and then decide what is the best course of action.

Reference(s) Used for this question:

http://www.newyorkcomputerforensics.com/learn/forensics_process.php
and ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 273-277).

QUESTION 576

A business continuity plan should list and prioritize the services that need to be brought back after a disaster strikes. Which of the following services is more likely to be of primary concern in the context of what your Disaster Recovery Plan would include?

A. Marketing/Public relations
B. Data/Telecomm/IS facilities
C. IS Operations
D. Facilities security

Correct Answer: B
Explanation:
The main concern when recovering after a disaster is data, telecomm and IS facilities. Other services, in descending priority order are: IS operations, IS support services, market structure, marketing/public relations, customer service & systems support, market regulation/surveillance, listing, application development, accounting services, facilities, human resources, facilities security, legal and Office of the Secretary, national sales.
Source: BARNES, James C.& ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 129).

QUESTION 577
For which areas of the enterprise are business continuity plans required?

A. All areas of the enterprise.
B. The financial and information processing areas of the enterprise.
C. The operating areas of the enterprise.
D. The marketing, finance, and information processing areas.

Correct Answer: A
Explanation:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 578
What is called an event or activity that has the potential to cause harm to the information systems or networks?

A. Vulnerability
B. Threat agent
C. Weakness
D. Threat

Correct Answer: D
Explanation:
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

QUESTION 579
Which of the following cannot be undertaken in conjunction or while computer incident handling is ongoing?

A. System development activity
B. Help-desk function
C. System Imaging

D. Risk management process

Correct Answer: A
Explanation:
If Incident Handling is underway an incident has potentially been identified. At that point all use of the system should stop because the system can no longer be trusted and any changes could contaminate the evidence. This would include all System Development Activity.

Every organization should have plans and procedures in place that deals with Incident Handling.

Employees should be instructed what steps are to be taken as soon as an incident occurs and how to report it. It is important that all parties involved are aware of these steps to protect not only any possible evidence but also to prevent any additional harm.

It is quite possible that the fraudster has planted malicous code that could cause destruction or even a Trojan Horse with a back door into the system. As soon as an incident has been identified the system can no longer be trusted and all use of the system should cease.

Shon Harris in her latest book mentions:

Although we commonly use the terms "event" and "incident" interchangeably, there are subtle differences between the two. An event is a negative occurrence that can be observed, verified, and documented, whereas an incident is a series of events that negatively affects the company and/ or impacts its security posture. This is why we call reacting to these issues "incident response" (or "incident handling"), because something is negatively affecting the company and causing a security breach.

Many types of incidents (virus, insider attack, terrorist attacks, and so on) exist, and sometimes it is just human error. Indeed, many incident response individuals have received a frantic call in the middle of the night because a system is acting "weird." The reasons could be that a deployed patch broke something, someone misconfigured a device, or the administrator just learned a new scripting language and rolled out some code that caused mayhem and confusion.

When a company endures a computer crime, it should leave the environment and evidence unaltered and contact whomever has been delegated to investigate these types of situations. Someone who is unfamiliar with the proper process of collecting data and evidence from a crime scene could instead destroy that evidence, and thus all hope of prosecuting individuals, and achieving a conviction would be lost.

Companies should have procedures for many issues in computer security such as enforcement procedures, disaster recovery and continuity procedures, and backup procedures. It is also necessary to have a procedure for dealing with computer incidents because they have become an increasingly important issue of today's information security departments. This is a direct result of attacks against networks and information systems increasing annually. Even though we don't have specific numbers due to a lack of universal reporting and reporting in general, it is clear that the volume of attacks is increasing.

Just think about all the spam, phishing scams, malware, distributed denial-of-service, and other attacks you see on your own network and hear about in the news. Unfortunately, many companies are at a loss as to who to call or what to do right after they have been the victim of a cybercrime. Therefore, all companies should have an incident response policy that indicates who has the authority to initiate an incident response, with supporting procedures set up before an incident takes place.
This policy should be managed by the legal department and security department. They need to work together to make sure the technical security issues are covered and the legal issues that

surround criminal activities are properly dealt with. The incident response policy should be clear and concise. For example, it should indicate if systems can be taken offline to try to save evidence or if systems have to continue functioning at the risk of destroying evidence. Each system and functionality should have a priority assigned to it. For instance, if the file server is infected, it should be removed from the network, but not shut down. However, if the mail server is infected, it should not be removed from the network or shut down because of the priority the company attributes to the mail server over the file server. Tradeoffs and decisions will have to be made, but it is better to think through these issues before the situation occurs, because better logic is usually possible before a crisis, when there's less emotion and chaos.

The Australian Computer Emergency Response Team's General Guidelines for Computer Forensics:

Keep the handling and corruption of original data to a minimum.
Document all actions and explain changes.
Follow the Five Rules for Evidence (Admissible, Authentic, Complete, Accurate, Convincing).
Bring in more experienced help when handling and/ or analyzing the evidence is beyond your knowledge, skills, or abilities.
Adhere to your organization's security policy and obtain written permission to conduct a forensics investigation.
Capture as accurate an image of the system(s) as possible while working quickly.
Be ready to testify in a court of law.
Make certain your actions are repeatable.
Prioritize your actions, beginning with volatile and proceeding to persistent evidence. Do not run any programs on the system(s) that are potential evidence. Act ethically and in good faith while conducting a forensics investigation, and do not attempt to do any harm.

The following answers are incorrect:

help-desk function. Is incorrect because during an incident, employees need to be able to communicate with a central source. It is most likely that would be the help-desk. Also the help-desk would need to be able to communicate with the employees to keep them informed.

system imaging. Is incorrect because once an incident has occured you should perform a capture of evidence starting with the most volatile data and imaging would be doen using bit for bit copy of storage medias to protect the evidence.

risk management process. Is incorrect because incident handling is part of risk management, and should continue.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21468-21476). McGraw-Hill. Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21096-21121). McGraw-Hill. Kindle Edition.
NIST Computer Security incident handling http://csrc.nist.gov/publications/nistpubs/800- 12/800-12-html/chapter12.html

QUESTION 580