Information Security and IT Risk Management

Student manual containing end-of-chapter questions

Each chapter contains the following types of questions

1. End-of-chapter review questions: These are simple questions to help students revise the content in the chapter.
2. Example case questions: These questions are related to the example case introduced in the chapter. The case typically describes one organization's experience with the issues discussed in the chapter. These questions help students put the information covered in the chapter into the professional contexts they are likely to encounter when they start their careers.
3. Hands-on exercise questions: These questions relate to the hands-on activity(ies) introduced at the end of the chapter. These activities are related to the content covered in the chapter and give students hands-on experience which is highly sought after by employers for the exciting entry-level positions in the industry.
4. Design case questions: These questions relate to the threaded design case introduced in chapter 1. This case is intended to give students the opportunity to conduct industry research, and learn best practices using information that may not be covered in the chapters.

Many chapters also include critical-thinking questions. These questions are intended to get students to think about important issues related to the chapter.

The rest of this document contains the text of all the questions. It is intended that students will use this document to answer the questions so that instructors have ready access to the text of the questions that the students are answering.

Suggestion

The document is tightly styled. After every question, there is space to respond to the question. Questions use the "question" style and the blank space between questions uses the "answer" style. Students should just start typing into the space provided for the answers and their answers will be distinct from the questions to facilitate grading.

Chapter 1

Chapter review questions

1. **What are some of the strengths of information security as a career choice?**

Information security is a good career chooice because of the strong employment numbers combined with attractive salaries. The estimated emplyment numbers exceed 200,000 and mean annual wages are close to $80,000. Further, these positions provide attractive career paths.What are some of the ways in which stolen information can be used for profit?

2. **What are some of the most common ways in which the carelessness of end-users can lead to a loss of sensitive information?**

End users can compromise information security in a number of ways. Examples include weak passwords, reusing passwords across safe and unsafe sites, opening malicious email attachments out of temptation or a sense of responsibility, following unsafe web links.

3. **What are some of the common professional responsibilities of information security professionals?**

Professional responsibilities of information security professionals include a mix of technical and non-technical activities. Their technical responsibilities include planning, implementing, upgrading, or monitoring security measures for the protection of computer networks and information. They also ensure that appropriate security controls are in place to safeguard digital fi les and vital electronic infrastructure. In emergencies, they also respond to computer security breaches and viruses.

Non technical responsibilities of information security professionals include researching new technologies, internal/ political issues, meeting regulatory compliance and developing internal security policies, standards and procedures

4. **Provide a brief description of the activities on which information security professionals spend most of their time.**

Information security professionals report spending most of their time on non-technical activities such as researching new technologies, internal/ political issues, meeting regulatory compliance and developing internal security policies, standards and procedures. Researching new technologies involves anticipating the risks created by the introduction of new technologies into the organization. Internal or political issues are associated with managing any restrictions placed by information security guidelines on end user behaviors. Regulatory compliance deals with ensuring that the organization's IT infrastructure is deemed safe by regulators and standards bodies. Developing internal standards refers to establishing procedures to ensure consistency in IT operations for all end users.

5. **Briefly describe the most important skills that information security professionals are expected to possess to succeed in their job.**

Based on a survey of information security professionals, the skills that information security professionals most need to be trained on include risk management, secure SDLC, forensics, end-user awareness, security architecture, access control, security management practices, and planning for business continuity and disaster recovery.

6. **How did the development of inexpensive computer networking technology (TCP/ IP) affect information security?**

The development of inexpensive and ubiquitous computer networking technology affected information security by enabling users, most of whom had no awareness of the security implications of IT, to get on to the Internet. These users became targets of early attacks, and very often became participants in attacks when adversaries were able to use the computers of these unwitting users to launch attacks on other targets.

7. **Briefly describe the activities of the gang of 414's.**

The gang of 414's was a group of six teenagers from Milwaukee, who got their name from the telephone area code for Milwaukee. These teenagers found it exciting to get into systems that were supposed to be out of their reach. Using home computers, phone lines, and default passwords, this group was able to break into approximately 60 high-profile computer systems, including those at the Los Alamos Laboratories and the Memorial Sloan-Kettering Cancer Center in New York.

8. **Briefly describe the impact of the gang of 414's on information security.**

The gang of 414's received wide coverage, including a Newsweek cover story titled "Beware: Hackers at play." This is believed to be first use of the term "hacker" in the mainstream media in the context of computer security. While the teenagers themselves did no harm, it was easy for the industry to see that the simple techniques used by the kids could easily be replicated by others. As a result, the US Congress held hearings on computer security. After more such incidents, Congress passed the Computer Fraud and Abuse Act of 1986, which made it a crime to break into federal or commercial computer systems.

9. **Briefly describe the Morris Worm. What are some of the factors that make it a landmark in the evolution of information security?**

Robert Morris, then a graduate student at Cornell, and now a Professor of Computer Science and Artificial Intelligence at MIT, released a 99-line self-replicating program on November 2, 1988, to measure the size of the then nascent Internet. As a result of a design feature of the program, it brought down many systems it infected.

The Morris Worm is considered a landmark in the evolution of information security for several reasons. It is considered the first Internet worm. In percentage terms, it is estimated to have brought down the largest fraction of the Internet ever (10%). It also resulted in the first conviction under the 1986 Computer Fraud and Abuse Act. Robert Morris was sentenced to probation, community service and a fine. The Morris worm also prompted the US Government to establish the CERT/CC (CERT

coordination center) at Carnegie Mellon University as a single point to coordinate industry–government response to Internet emergencies.

10. What was the impact of Windows 95/ 98 on information security?

Windows 95 was designed primarily as a stand-alone single-user desktop operating system and therefore had almost no security precautions. Most users ran Windows 95 without passwords and most applications ran on Windows 95 with administrative privileges for convenience. However, Windows 95 supported TCP/IP, thereby bringing TCP/ IP into mainstream businesses. This combination of a security-agnostic networking technology (TCP/IP) combined with an equally security-agnostic business desktop created a fertile environment for information security compromises to flourish. Many information security experts refer to this environment as the source of the information security profession. Even the introduction of Windows 98 on June 25, 1998, made no change to the basic security design of Windows desktops.

11. How does HIPAA (the Health Insurance Portability and Accountability Act) affect the profession of information security?

The HIPAA law had provisions to make organizations responsible for maintaining the confidentiality of patient records in the health-care industry. At the current time, the health-care industry has until 2014 to move over completely to EHR. This is a major driver of demand for information security at the time of writing this edition (2012–2013).

12. What are the provisions in the Sarbanes-Oxley act that are related to information security?

The Sarbanes-Oxley act of 2002 focused on making the key executives personally accountable for the correctness of financial reports filed by publicly traded companies. The act had three major provisions. Section 302 of the act requires the CEO and CFO of firms to sign a declaration of personal knowledge of all the information in annual filings. Section 906 of the act imposes criminal penalties including imprisonment of up to 20 years for incorrect certification. Section 404 of the act has had a major impact on the information security profession because it requires that the certification in Section 302 be based on formal internal controls. This has led to significant investments in internal controls over financial reporting in publicly traded fi rms.

13. What were some of the immediate factors that led to the creation of the US Cyber Command?

In April 2009, reports emerged that intruders had broken into the computer networks of defense contractors developing the Joint Strike Fighter, also called the F-35 Lightning II. The $300 billion project was the Defense Department ’s costliest weapons program ever, and used 7.5 million lines of computer code. Intruders had stolen terabytes of data related to the aircraft ’s design and electronics. It was believed that the theft would help enemies plan their defenses against the fighter. The contractors involved in the project include Lockheed Martin, Northrop Grumman, and BAE Systems. The same month, it was also reported that the US electricity grid had been penetrated by spies from China, Russia, and other countries. The spies also inserted computer software in the grid, which could be used to cause damage by remote control. Soon thereafter, on June 23, 2009, the US

Cyber Command was created to defend US military computer networks against attacks from adversaries and also to respond in cyberspace as necessary.

14. Provide a brief description of the US Cyber Command and its activities.

From Wikipedia and the US DoD Fact sheet regarding the US Cyber command, dt. May 25, 2010:

The USCYBERCOM is an armed forces sub-unified command subordinate to United States Strategic Command.

According to its mission statement, the USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

The command is charged with pulling together existing cyberspace resources, creating synergy and synchronizing war-fighting effects to defend the information security environment. USCYBERCOM is tasked with centralizing command of cyberspace operations, strengthening DoD cyberspace capabilities, and integrating and bolstering DoD's cyber expertise.

15. What was operation Aurora?

On January 12, 2010, a blog post by Google 's Chief Legal Officer reported that the company had detected an attempt to steal its intellectual property originating from China. The attacks were also aimed at accessing emails of Chinese human-rights activists. The US Government soon escalated the incident. Congress announced its intention to investigate the allegations and the Secretary of State labeling the Chinese censorship of the Internet to an information-age Berlin Wall. Further investigations traced the attacks to two educational institutions in China—Shanghai Jiaotong University and the Lanxiang Vocational School. Jiaotong is home to one of China 's elite computer science programs, and Lanxiang is involved in training computer scientists for the Chinese military. China has however denied formal government involvement and called the attacks simply an attempt by students to refine their computer skills. This incident is labeled operation Aurora.

16. Briefly describe the outage that affected the Sony PlayStation network in 2011.

In April 2011, Sony announced that an external intrusion had compromised its PlayStation Network and Qriocity service), and that hackers had obtained personal information on the 70 million subscribers of the network. The company could not rule out the possibility that credit card numbers may also have been stolen. In response, the company took the network offl ine while it tried to ensure that all traces of the offending software had been removed from the network. During the time, millions of kids all over the world who had planned their summer breaks around catching up with online gaming on PSN had to fi nd alternate ways to pass their time. For this reason, while the intrusion affected a relatively innocuous network, the impact on families around the world was huge and almost every family with kids followed the daily developments around the attacks.

17. **What is information security?**

Information security is defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability

18. **What is confidentiality?**

Confidentiality means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information . Confidentiality is the responsibility of custodians of information to provide that privacy to the individuals whose information they have in their possession.

19. **What is integrity?**

Integrity is defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Integrity enables IT systems to be actionable.

20. **What is availability?**

Availability is defined as ensuring timely and reliable access to and use of information. Availability makes information systems useful.

21. **Provide an example of a violation of confidentiality**

The ability of attackers to steal credit card information from retailers such as Target and Neiman-Marcus is an example of a violation of confidentiality. Other violations include the theft of software code in Project Aurora.

22. **Provide an example of a violation of integrity**

The numerous instances where executives were able to fraudulently manipulate financial records of their firms are examples of violations of integrity. Firms where such instances occurred include Enron, Adelphia, MCI, and WorldCom.

23. **Provide an example of a violation of availability**

The outage at Sony PlayStation networks in 2011 is an example of a violation of availability. Users were deprived of a service they were planning to use during their summer break, and the company was potentially

24. **Which in your opinion is the most important of the three components of information security? Why?**

<This is a question for students to formulate and express opinions.>

Example case questions

1. **Of the three dimensions of information security, which was/ were affected by Cablegate?**

Cablegate involved unauthorized access to information. Therefore, it affected the confidentiality dimension of information security. The documents were still available for analysts and were not modified from the source. So, neither availability nor integrity were affected.

2. **What do you think motivated Pfc Bradley Manning to release the memos to Wikileaks, and then discuss his actions with Adrian Lamo, well aware of the risks of these actions?**

Pfc Manning seems to have been motivated by a desire to inform the public about the activities of the Intelligence services. He was disturbed by the information he was privileged to access.

3. **Based on publicly available information, what were some of the measures taken by the US Government to secure the memos?**

Access to the documents was limited to personnel in intelligence roles who had secret or top secret clearance. These amounted to over 3 million people. Data exchange is carried out over encrypted networks.

4. **To what extent were these measures effective?**

Evidently not much, because one of the people with access to the information was able to disclose it to the public.

5. **If you were responsible for the information security of these memos, what would you have done to prevent an incident such as Cablegate from happening?**

I would have prevented electronic downloads of the documents. I would also have prevented people from bringing in cameras or other recording devices in rooms where they accessed these networks.

6. **Why do you think the recommended actions above were not taken by the experts responsible for the information security of these memos?**

These actions do not appear to have been taken consistently for end-user convenience. With over 3 million users accessing these networks, and with almost all of these users handling the information responsibly, any efforts to introduce strict security controls are likely to have been resisted in the name of productivity.

Hands-on activities questions

PC audit questions

1. **Run a PC audit tool such as Secunia's online software inspector on one of your home computers. Submit a screenshot such as the one shown in the figure.**

Students should submit a screenshot similar to the one in the chapter

2. **What are some actions you are considering after viewing the results of your PC audit?**

Students often find software that needs updating.

Steganography questions

1. **Create one steganographic image following the directions in this section.**

   Students should be able to replicate the instructions provided in the chapter.

2. **Submit printouts of the original image, the modified image and a screenshot of the text embedded in the image as in the figure.**

   This is self-explanatory

Critical thinking exercise

1. **Identify the CIA area(s) affected in each of these incidents and some actions organizations can take to ensure that these incidents do not happen to them.**

Incident	CIA area(s) affected	Potential prevention methods
414's	Confidentiality	Passwords, firewalls
Morris worm	Availability	Anti-virus software
ILOVEYOU virus	Availability, integrity	Anti-virus software
T.J.Maxx	Confidentiality	Encryption, separation of duties
Georgia govt. websites	Integrity	Strong passwords
Joint Strike Fighter	Confidentiality	Encryption, firewalls, access control
Google-China	Confidentiality	Passwords
Sony PlayStation Network	Availability	Separation of duties, passwords, anti-virus

Design case questions

1. **What are some of the ways in which weaknesses in information security can potentially cause embarrassment or financial losses to the university?**

   Much like a business, the reputation of a University directly relates to the customer's views and financial support. For instance, an incident involving Alumni data could affect the number of alumni willing to donate to the school. A breach involving the Department of Electrical engineering could adversely affect the number of federal grants the department receives.

   Take a very recent (January 2014) development, for instance. New regulations by the National Institute of Health state that "None of the funds … may be used to maintain or establish a computer network unless such network blocks the viewing, downloading, and exchanging of pornography." If a researcher is found perusing porn on a computer purchased with NIH funds (a) the funds may be in jeopardy, (b) punitive sanctions may be applied, affecting other NIH grants, and (c) when the event hits the local newspapers, the University will have a lot of containment to do.

2. **List three items of information stored in the university's information systems for which the university is expected to maintain confidentiality. What are some of the ways in which the confidentiality of each of these items may be compromised?**

Student Grades: Confidentiality of grades can be breaches as easily as having a grad student posting grades on the door of a classroom.

Employee SSN: Faculty and staff SSNs are stored in the Human Resources database. A vulnerability on this database could result in a leak of records.

Department of Defense research: DoD research materials are usually highly controlled. Granting access to a foreign national to these materials may, in certain cases, also be considered a compromise.

3. **List three items of information stored in the university's information systems for which the university is expected to maintain integrity? What are some of the ways in which the integrity of these items may be compromised?**

While the expectation of confidentiality comes from laws and regulations such as FERPA, HIPAA, etc, expectation for integrity comes from the users of the data themselves. As such, users expect that ALL data handled by their employee will be conserved and not altered.

Student Grades: The University is not only expected to maintain the confidentiality but also the integrity of the data. The Registrar of the University has to ensure the grade is not altered, even years after a student's graduation. A simple scenario: a student pays an adjunct professor to alter his/her final grade in the system.

Web Pages: Something as simple as a web page defacement may bring embarrassment for any organization, even an University. If a login page is hijacked, for instance, the credentials of many faculty, staff, and students could be lost.

Departmental Budget Data: A department depends on its budgeted funds to determine how to operate within a fiscal year. A data entry error in the beginning of the fiscal year could alter the integrity of a spreadsheet to such an extent to go unnoticed until the end of the year.

4. **List three items of information stored in the university's information systems for which the university is expected to maintain availability? What are some of the ways in which the availability of these items may be compromised?**

Email Data: In many ways email is the foundation of a University communication system these days. An outage of this system, no matter how brief, cause critical delays with a variety of consequences to the day to day operations.

Phone System: In these days of IP telephony, a configuration error could bring the entire phone system down for hours.

Power: Accidental interruptions are unfortunately common place when it comes to power. The construction of a new building next door to a data center, for instance, could accidently cut of the power to the data center for hours. Battery power only lasts for a couple of hours. Generators are needed for prolonged outages.

Chapter 2

Chapter review questions

1. **What is system administration?**

System administration is a set of functions that provides support services, ensures reliable operations, promotes efficient use of the system, and ensures that prescribed service-quality objectives are met. System administration includes the installation, configuration, and maintenance of network equipment (switches, routers, DHCP, DNS servers, etc.) and computer systems (database systems, email systems, ERP systems, etc.).

2. **Why is system administration important to information security?**

System administration is important to information security because it is the first line of defense for all the three dimensions of information security—confidentiality, integrity, and availability.

3. **Who is a system administrator?**

The system administrator is the person who is responsible for the day-to-day operation of a technology system.

4. **What are some of the important day-to-day activities performed by system administrators?**

The important day-to-day tasks performed by system administrators include installation and configuration of the system so it can be used, access control and user management so users can find what they need without inadvertently causing damage to the system, ongoing monitoring of the system to ensure all components are operating as expected, applying updates when monitoring reveals performance or other security-related issues.

5. **Define Infrastructure as a Service (IaaS).**

Infrastructure as a Service is a business model in which an organization uses hardware equipment such as processors, storage , and routers from the IaaS provider. IaaS is considered a form of cloud computing. The IaaS provider only provides the hardware and takes responsibility for just the hardware installation and maintenance. All operating system and application administration must be performed by the organization ’s system administrators. Pricing is typically on a subscription basis and is based on usage (e.g., per GB of storage, per million CPU cycles). Amazon and Rackspace are some of the better known IaaS providers.

6. **What are some of the benefits of using an IaaS provider?**

Some benefits of using an IaaS provider include the conversion of upfront capital expenses into variable ongoing costs. Consumers are spared the effort of ensuring that the hardware is up and running because the IaaS providers can amortize the cost of building hurricane-proof infrastructures over their entire customer base.

7. **What is a virtual server?**

A virtual machine is a software container into which an operating system and applications can be installed. Virtual machines are a recent technology used by system administrators to increase the efficiency of utilization of their computer hardware.

8. **What are some benefits of virtualization?**

Virtual machines increase the efficiency of utilization of computer hardware. Virtual machines function exactly like their physical counterparts but without the possibility of hardware failure. Virtual machines can be started and stopped on demand, so during times of business ' peak load, such as the holiday season for an online merchant, new virtual machines can be started to run as web servers. Once the holidays are over and load returns to normal, the extra virtual servers can be removed.

9. **What is the role of a system administrator in maintaining information security in an organization?**

Virtually everything that system administrators do is related to information security and most technical aspects of information security are addressed by system administrators. For example, by setting up appropriate password rules, system administrators can make their IT infrastructures and applications more resilient to attacks.

10. **What is software configuration?**

Software configuration is the act of selecting one among many possible combinations of features of a system.

11. **How does software configuration impact information security?**

Software configuration has several information security implications. Complex configurations can create vulnerabilities due to the interactions among components and the inability of system administrators to fully comprehend the implications of these interactions. Many desirable software components are not maintained, creating information security hazards. For these reasons, whereas the general rule of thumb among consumers regarding configuration may be "when in doubt, install or update," among professional system administrators it is "when in doubt, do not install."

12. **Define access control. How can weak access controls impact information security?**

Access control is the act of limiting access to information system resources only to authorized users, programs, processes, or other systems. Access controls establish what users can do on a system. Typically, this refers to which files or directories a user can read, modify, or delete, but in some operating systems, access to network ports and other OS-level structures can also be limited. Access controls can also be applied at the application level, limiting which rows and/ or columns a user can see in a database or which screens are available in a business application.

Weak access controls can allow intruders easy access into a system and violate all dimensions of information security – confidentiality, integrity and availability.

13. Define user management. How does user management impact information security?

User management is a key component of access control. User management refers to defining the rights of organizational members to information in the organization . Creating and removing user accounts are probably the first thing that people think of when they hear the term user management. However, user management also includes updating records appropriately when users change roles.

User management impacts information security by reducing the likelihood that users have improper privileges over information resources. This reduces the likelihood of information security compromises.

14. What is monitoring? How does it help information security?

Monitoring is the act of listening and/or recording the activities of a system to maintain performance and security. Monitoring helps information security by alerting system administrators when abnormal activity is detected in a system, and identifying the systems affected by the abnormal behavior. This speeds up the response to an incident and potentially reduces the damage from such incidents.

15. What is reactive monitoring? What are some common reactive monitoring methods?

Reactive monitoring is the act of detecting and analyzing failures after they have occurred. Common reactive monitoring methods include health monitoring and log management. Automated monitoring tools such as Nagios can send instant notifications when problems occur on the network. Similarly, log management tools collect and analyze the system logs from all of the servers across a network and correlate events between servers.

16. What is proactive testing? What are some common proactive testing methods?

Proactive testing is the act of testing a system for specific issues before they occur. Methods include using vulnerability scanners and penetration testing. Vulnerability scanners can access systems and look for potential vulnerabilities. These vulnerabilities can then be prioritized and resolved. Penetration testing is usually carried out by a professional security firm, and actively exploits vulnerabilities found to assess the level of access that is gained.

17. What is a system update? What are the challenges in keeping systems updated? Why is it important for information security?

Operating system updates are software updates that fix issues with the low-level components of the system software. They are developed and released by the operating system vendor directly. All modern operating systems include software for automatically checking for and installing required updates without system administrator intervention.

It is challenging to keep systems updated because applications are often customized with plugins from other vendors and sometimes even by in-house developers. Many of these customizations are not well documented or well tested. It is not easy to predict the impact of an application update on these customizations. Therefore, updates can lead to unpredictable behaviors of installed applications on updated systems.

Updates are important for information security to respond to vulnerabilities revealed during ongoing use of software.

18. **What is a single point of failure? How do system administrators typically deal with single points of failure?**

A part of a system whose failure will stop the entire system from working is called a single point of failure. Single points of failure generally have availability implications. For example, a common single point of failure in desktop computers is the power supply. If the power supply fails, the computer cannot function until a replacement is installed.

The standard solution to deal with single points of failure is redundancy. Redundancy is surplus capability, which is maintained to improve the reliability of a system. For example, to minimize downtime, you could have a spare power supply ready to install right away.

19. **What is the difference between cold spares and hot spares?**

Extra parts kept at hand for use to replace defective parts are known as cold spares. Hot spares are redundant components that are actually housed inside the server and can replace the failed component with no downtime. Cold spares are useful for minimizing downtime, but there is still some amount of time during which the system would be unavailable, while the cold spare is being installed. Most critical computer servers utilize hot spares.

20. **What is Active Directory? What role does it play in maintaining information security on Windows computers?**

Active Directory is a collection of technologies that provide centralized user management and access control across all computers that are “members” of the domain. Active directory centralizes the administration of information security policies in an organization.

21. **What are group policies? How do group policies assist system administrators in maintaining information security?**

Group policy is a technology developed by Microsoft that allows administrators to implement specific configurations for users and computers. Group Policies are often used to restrict certain actions that may pose potential security risks, e.g., to disable the downloading of executable files or to deny access to certain programs. As the name suggests, group policies allow administrators to organize individual users into groups and apply policies to these groups, rather than individual users. This improves the consistency in implementation of policies across an organization.

22. **What is a domain controller?**

The server that implements the active directory rules within a domain is called the Domain Controller for the domain. The Domain Controller maintains information on user accounts, authenticates users on the domain based on this information, and authorizes these users to access resources on the domain based on the group policy. Each domain requires at least one Domain Controller, but more can be added for redundancy.

23. **Provide a brief description (2-3 sentences max) of the information security features of the latest version of Microsoft's System Center or comparable product.**

From the Microsoft White Paper on Systems Center 2012 (accessed 03/05/14):

System Center 2012 R2 delivers unified management and agile system administration for the Cloud OS by offering consistent management experiences across on-premises, service provider, and Windows Azure environments.

24. **What is Linux? Why is it popular? What are some of the most popular distributions of Linux?**

Linux is an open source implementation of the UNIX operating system, distributed under the GPL license, which obligates any change made to the system to be made available to all other users of the system. Linux is popular because it provides a lot of functionality at no cost. Some of the popular Linux distributions include Redhat, Ubuntu, Debian and CentOS.

25. **Provide a brief overview (2-3 sentences max) of the capabilities of Puppet, the IT automation software used by many system administrators.**

From the Puppet web page, accessed 03/05/2014

Puppet Enterprise is IT automation software that gives system administrators the power to easily automate repetitive tasks, quickly deploy critical applications, and proactively manage infrastructure, on-premises or in the cloud.

Example case questions

1. **Based on the information provided above, list as many example of violation of confidentiality, integrity and availability identified in the case.**

Confidentiality violations: End user passwords could be read, database content (credit card numbers) could be read.

Integrity violations: Unauthorized transactions were made on stolen credit cards

Availability violations: Stolen credit cards became unusable

2. **Based on the case, identify the failures in execution of the common system administration tasks at T J Maxx at the time of the case.**

There were numerous systems administration weaknesses. The passwords were not encrypted over the wireless network. The databases could be accessed from the job employment stations at stores.

The store manager's passwords gave access to the database. The payment details database was not on a separate network.

3. **If you were responsible for system administration at T J Maxx, what are the things you would have done to prevent the occurrence of the incidents reported in the case?**

I would have eliminated the system administration weaknesses identified in the previous question. I would have enabled encryption on the wireless network. I would have limited access privileges to end users so they could not perform transactions on corporate systems.

Hands-on activities questions

1. **Provide a brief description of VirtualBox and its uses.**

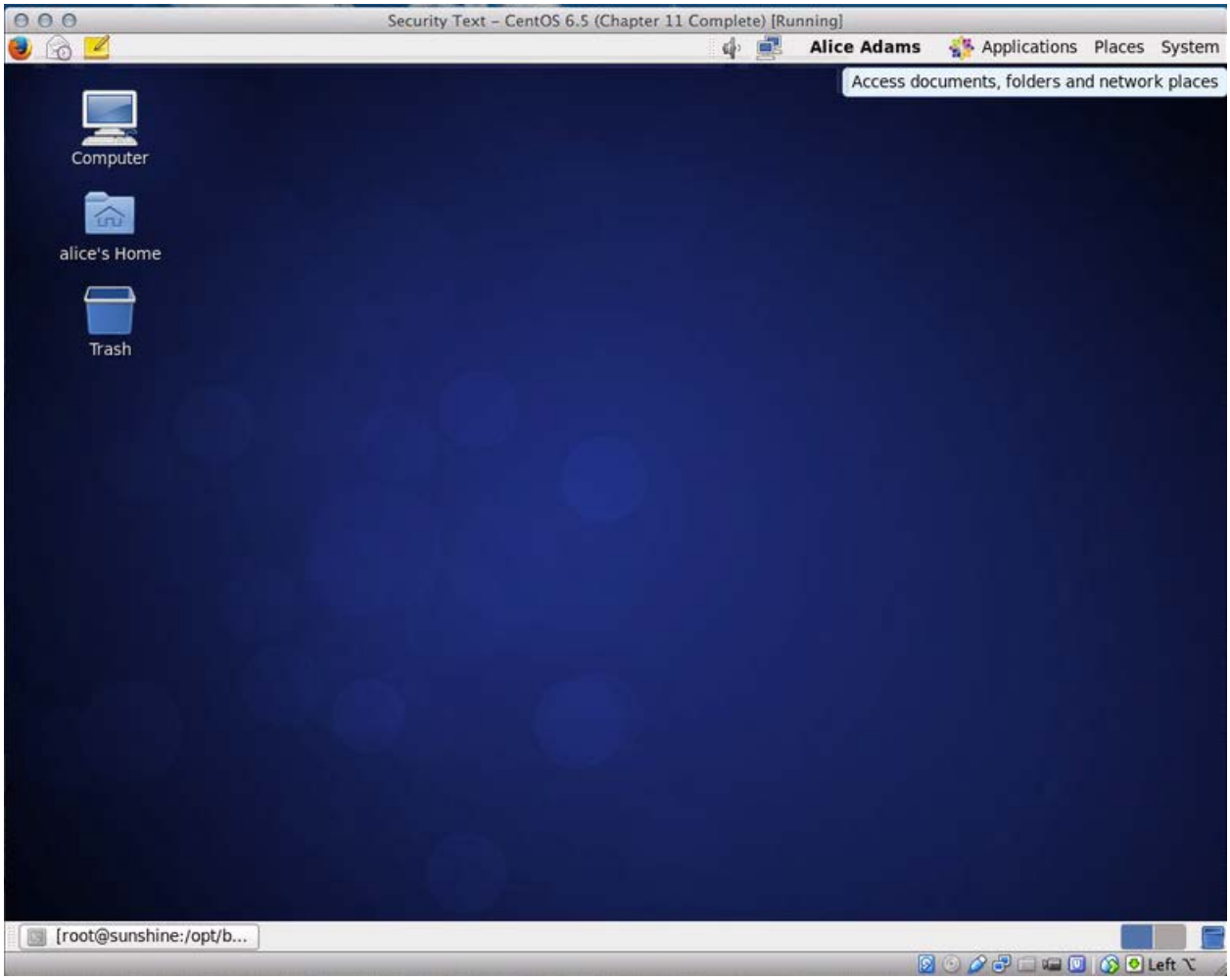
VirtualBox is a hardware virtualization package that allows you to run multiple "guest" Operating Systems on a single physical computer. Virtualization allows business to utilize more of their hardware resources by running more than one virtual server on each of their physical servers.

2. **Provide a brief description of the OVA file format.**

The OVA file format is a compressed (archive) of the Open Virtualization Format (OVF) image format used by most major hardware virtualization packages. The OVF/OVA format allows you to create a virtual server image with one package, such as VirtualBox, and share it with someone using VMWare or some other virtualization package that supports the format.

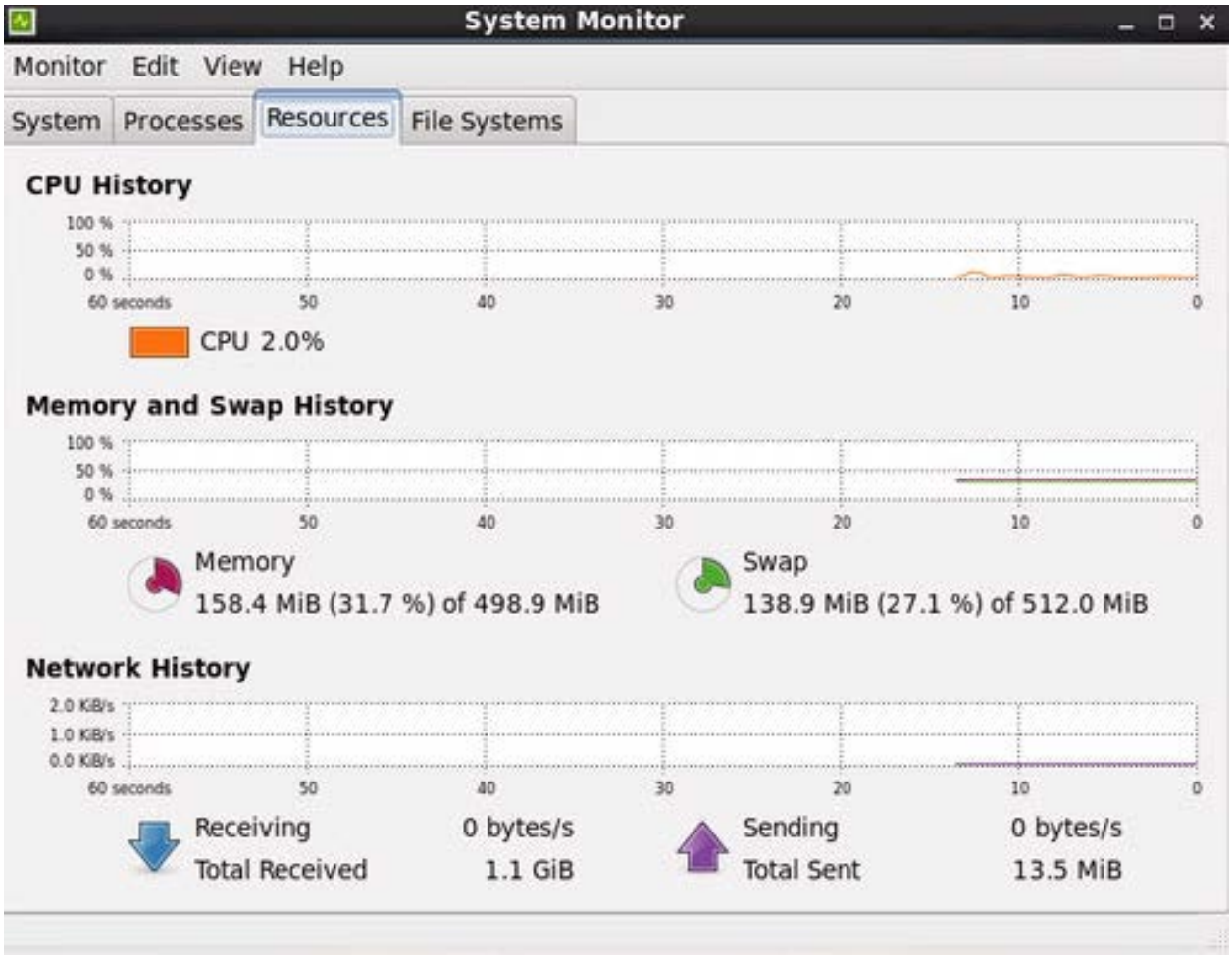
To demonstrate that you have successfully installed the VM, submit the following:

3. **A screenshot of the CentOS desktop**

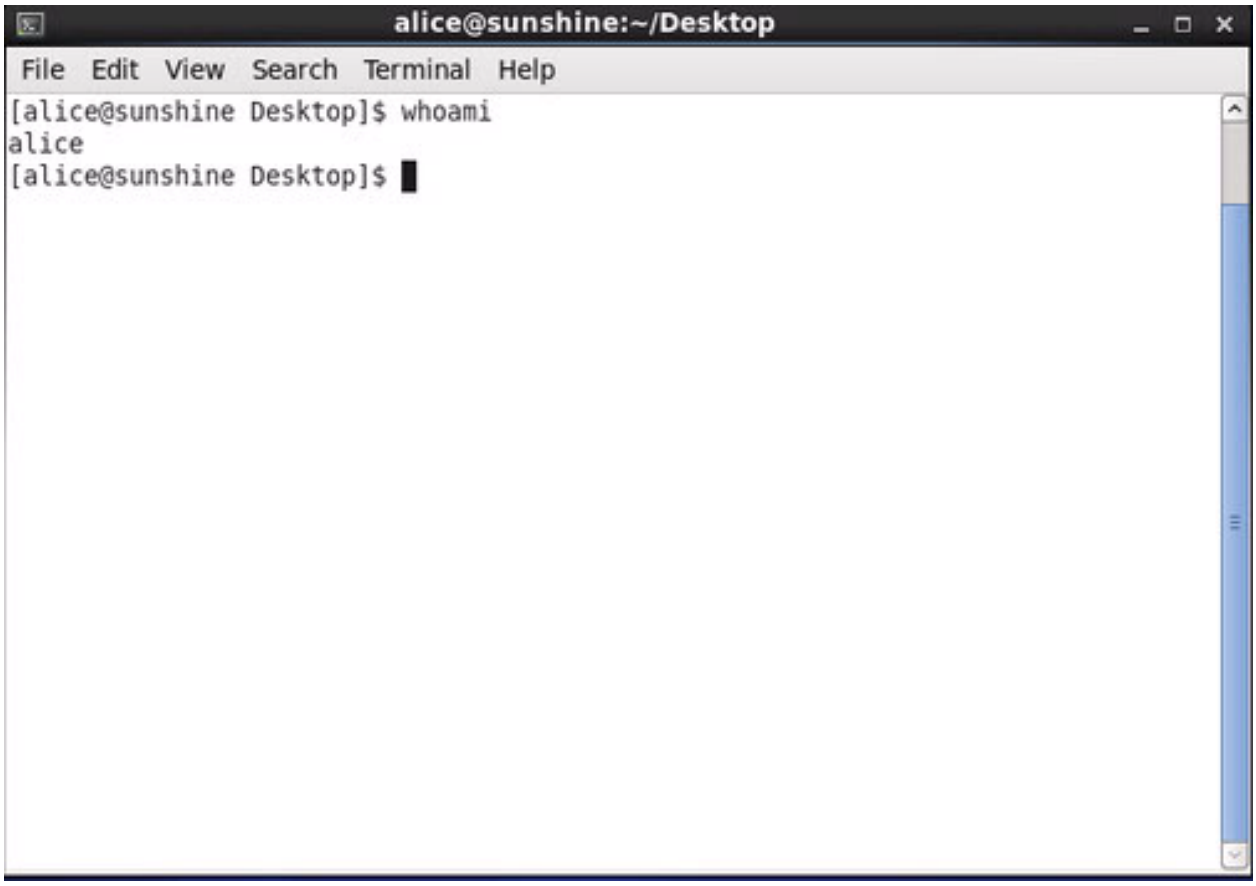


4. **Start the browser using Applications → Internet → Firefox web browser. Submit a screenshot of the browser window showing the default home page of the browser.**

5. **Start the system monitor using Applications → System tools → System monitor. Submit a screenshot of the System monitor.**



6. **Start the terminal by selecting Applications → System Tools → Terminal. At the prompt, type in the command 'whoami'. Submit a screenshot of the terminal window showing the command and its output. (most of the hands-on activities in the book will make extensive use of this terminal window)**



Stop the VM by selecting Machine → Close → Poweroff the machine.

Critical thinking questions

1. **What is your opinion about the incident?**

This incident seems to reflect judicial overreach by the Italian court against an American company. It is also possible that the incident reflects case law in these matters. Companies are generally not held liable for how their technologies are used by people. For example, gun manufacturers are not held responsible for irresponsible use of the weapons. Similarly, if content providers expeditiously remove objectionable content, they are generally not held liable.

2. **Should system administrators and companies be responsible for the content posted by users of a website?**

As stated in the previous question, companies and their employees are generally not held liable for how their technologies are used by people. Therefore content firms and systems administrators at these firms should not be held liable for the content posted by users of a website.

3. **Say you are the system administrator of a website and you receive a request from a user to delete a picture uploaded by a friend at a party that includes the user. Would you consider the request reasonable?**

Yes, I would consider the request reasonable, on privacy grounds.

4. **How would you respond to such a request?**

I would delete the picture instantaneously.

Design case questions

1. **What is a JBOD anyway?**

   JBOD stands for "Just a Bunch of Disks." It is an actual technical term, referring to a disk attached to a computer. Something like an external USB drive.

2. **As you research your options for Sunshine State University, you are advised to start with a common procedure – looking at what your closest peers are doing. Businesses call this benchmarking. In your context, this means what peer Universities are doing in terms of email systems.**

   a. **List three universities or colleges in your area that you would consider the closest peers to Sunshine State. (Keep this list handy. You will find yourself returning to this list often to research what these schools are doing to address the challenges you face in this and later chapters.)**

      Students could list any universities for this purpose.

   b. **Which of these options has each of the institutions selected for email service? Why did they select this choice? (you may find information regarding this on their web sites. You can also call their technical support help line).**

      This will take some research. Here are some of the options as of January 2014:

      - Office 365
      - Google Apps for Education
      - Hosted Exchange
      - Locally hosted Exchange Server (Outlook)
      - Locally hosted UNIX mail, such as sendmail or procmail

   c. **If your own institution is not on the list in (a), what is your own institution doing for email service? Why?**

      The answer to this will vary depending upon the institution.

3. **What problems can you anticipate from Sunshine State's current system shown in the figure? What are the single points of failure? What would have to happen for the local system to be able to safely handle email service if any of these single points of failure were to fail?**

- The "normal" server lifetime is 3-5 years. Anything older than that has increased chance of multiple failure.
- The current server has a single power supply. Someone trips on the cable and there goes availability (and possible integrity)
- It also only has one network connection. (see previous bullet)
- Single external drive for mail storage

As it stands, any Sys Admin that looks at this setup should be classifying it as "woefully inadequate," unless it only holds totally non-critical emails for "one" user. Any failure would cause email to bounce back to the sender.

4. **What features (if any) do the cloud service models (IaaS and SaaS) offer that could not be currently provided locally?**

Email started many, many years ago. Most of the old, local UNIX-based mailers only work with email. New cloud offerings, and Exchange, offer a variety of added services such as word processor, spreadsheet, sharing services, calendars, and more.

These services also offer redundancy and reliability. That is not to say they never go down, but they are certainly better equipped to deal with outages that a local system would.

Finally, cloud services such as Google or Microsoft also offer archiving, legal holds, additional quota, usually for an additional fee.

5. **During your research you find that one of the common queries fielded by technical support is restoration of accidentally deleted email. What facilities (if any) does each alternative provide in the restoration of accidentally deleted e-mails?**

It all depends on the system. Most systems work with the principle of "DELETED" then "PURGED." The email is not really deleted until it is purged from the system. The purge can be done manually by the user, or automatically, once quota hits a certain threshold or after a preset number of days. After purged, email is gone unless (1) it is archived by the system, or (2) it is present in a backup tape.

6. **Another important feature request from the student body is email access from a wide variety of devices, especially non-web clients such as smart phones, and traditional email clients such as Thunderbird and Eudora. What support does each of the choices provide for email access from these devices. What advantages or disadvantages does each system have for such access?**

Again, the answer here will depend on the system. Most users really will not care what server is used, as long as their current mail client can continue to be used. In order for a system to accommodate the largest number of clients possible the student should look at compatibility and support of both know email protocols: IMAP and POP. From the security perspective, they also