# Week 3 Hands On

Eric Vara

The University of Arizona Global Campus

CYB 300

Instructor Bipin Bhatt

05, December 2022

## Part One

### Module 05: Incident Response and Contingency Planning Review Questions

1. What is the name for the broad process of planning for the unexpected? What are its primary components?
   * Answer: Contingency planning refers to the overall process of preparing for the unexpected. The main components are business impact analysis, incident response plan, disaster recovery plan and business continuity plan.
2. Which two communities of interest are usually associated with contingency planning? Which community must give authority to ensure broad support for the plans?
   * Answer: The information technology and information security communities are often involved in contingency planning. The broader business community must be empowered to gain broad support for the plan.
3. According to some reports, what percentage of businesses that do not have a disaster plan go out of business after a major loss?
   * Answer: According to some statistics, 40 percent of organizations that do not have a catastrophe plan will fail following a severe loss.
4. List the seven-step CP process recommended by NIST.
   * Answer: NIST recommends the following seven steps:
5. Develop the contingency planning policy statement.
6. Conduct the business impact analysis.
7. Identify preventive controls.
8. Develop recovery strategies.
9. Develop an IT contingency plan.
10. Plan testing, training, and exercises.
11. Plan maintenance.
12. List and describe the teams that perform the planning and execution of the CP plans and processes. What is the primary role of each?
    * Answer: The Contingency Planning and Management Team collects information about information systems and the threats they face. The team then executes his BIA and develops strategies for incident response, disaster recovery, and business continuity.
      + The incident response team maintains and implements the IR plan by identifying, assessing, and responding to incidents.
      + The disaster recovery team manages and executes disaster recovery strategies by identifying, assessing and responding to disasters and restoring core operations to operations.
      + In the event of an incident or disaster, the Business Continuity Team oversees and executes the BC strategy by setting up and initiating offsite activities.
13. Define the term *incident* as used in the context of IRP. How is it related to the concept of incident response?
    * Answer: An event, whether natural or man-made, is a cyber-attack or an accident. The incident response plan is triggered by an incident.
14. List and describe the criteria used to determine whether an actual incident is occurring.
    * Answer: An actual incident occurs when information assets are attacked, there is a good likelihood of success, and the attack threatens the confidentiality, integrity, or availability of information resources.
15. List and describe the sets of procedures used to detect, contain, and resolve an incident.
    * Answer: The CP team develops three sets of incident response procedures
      + The first set of procedures must be followed during the occurrence. These are function-specific procedures that are organized and assigned to persons.
      + The second set of measures must be carried out following the incident. These processes may also be function specific.
      + The third set of processes must be carried out in order to prepare for the incident. These processes involve data backup schedules, disaster recovery planning, training schedules, testing plans, service agreement copies, and business continuity plans.
16. What is incident classification?
    * Answer: The process of assessing an undesirable event that has the potential to escalate into an incident and determining whether it constitutes an actual incident is known as incident classification.
17. List and describe the actions that should be taken during the reaction to an incident.
    * Answer: Incident detection using incident classification, notification of key personnel, documentation of the incident, implementation of required containment strategies, and then either escalation of the incident to a disaster or beginning the incident recovery process are the steps involved in the incident response.
18. What is an alert roster? What is an alert message? Describe the two ways they can be used.
    * Answer: A reminder list is a list of employees who should be contacted when an event occurs. Alerts are canned messages that provide responders with enough information to understand the status of an incident and what elements of the incident response plan should be implemented.
19. List and describe several containment strategies given in the text. On which tasks do they focus?
    * Answer:
      + Disconnecting affected communication sources in order to shut off an attack from outside the firm network.
      + Dynamically implementing filtering rules to prevent specific forms of network access, hence focusing on the specific vulnerability exploited by the threat agent.
      + Keeping an eye on the situation while devising a more targeted strategy
20. What is a disaster recovery plan, and why is it important to the organization?
    * Answer: The disaster recovery strategy addresses both disaster planning and recovery. Natural or man-made disasters can occur. The plan is crucial to the organization because it enables issues detected by the incident response team to be escalated to disaster status.
21. What is a business continuity plan, and why is it important?
    * Answer: A business continuity plan assures that vital company processes can continue in the case of a disaster; consequently, it is critical to the organization's survival in the event of a disaster.
22. What is a business impact analysis, and what is it used for?
    * Answer: The business impact study informs the CP team about systems and the threats they face. It is used to provide critical situations so that the team can plan for disasters.
23. Why should contingency plans be tested and rehearsed?
    * Answer: A plan that has not been tested is not usable. Without testing and rehearsal, the plan's quality, and capacity to achieve its goal of reducing recuperation time are unknown. One important goal of this form of planning is to eliminate as many unknown aspects as feasible. Testing can also show faults in the plan that can be fixed before the plan is needed.
24. Which types of organizations might use a unified continuity plan? Which types of organizations might use the various contingency planning components as separate plans? Why?
    * Answer: Because they are succinct and easier to test, unified contingency plans may be used by small to medium-sized companies. Large firms cannot adopt a single plan because it would be too difficult to design and test.
25. What strategies can be used to test contingency plans?
    * Answer: To put a contingency plan to the test, two methods can be used:
      + simulation exercise
      + classroom exercise
26. List and describe two specialized alternatives not often used as a continuity strategy.
    * Answer: Two specialized options that are rarely utilized as a continuity strategy:
      + A business continuity plan is a strategy for ensuring that corporate processes can continue in the event of an emergency or tragedy.
      + The business continuity plan is completed and performed by establishing and launching off-site operations in the case of a catastrophe or disaster.
27. What is digital forensics, and when is it used in a business setting?
    * Answer: The preservation, identification, extraction, documenting, and interpretation of computer media for evidential and root-cause investigation constitutes digital forensics. In a company setting, digital forensics is used to examine policy or legal violations by an employee, contractor, or outsider, as well as attacks on a physical or information asset.
28. What is a security awareness program?
    * Answer: The CISA Cybersecurity Awareness Program is a one national public security awareness campaign aiming at boosting understanding of cyber dangers and empowering the American public to be safer and more secure online.

### Module 06: Legal, Ethical, and Professional Issues in Information Security Review Questions

1. What is the difference between law and ethics?
   * Answer: Ethics is a set of moral standards that an individual sets for himself and his or her own personal actions. Laws are written laws that are used to control society as a whole.
2. What is civil law, and what does it accomplish?
   * Answer: In contrast to criminal or administrative law, civil law is a field of law that controls non-criminal rights, duties of persons, and equal legal relations between private individuals.
3. What are the primary examples of public law?
   * Answer:
     1. Criminal
     2. Administrative
     3. Constitutional
4. Which law amended the Computer Fraud and Abuse Act of 1986, and what did it change?
   * Answer: The 1996 National Information Infrastructure Protection Act. Several provisions of the CFA Act were amended, and the penalty for certain crimes were enhanced.
5. Which law was created specifically to deal with encryption policy in the United States?
   * Answer: The Security and Freedom Through Encryption Act of 1999
6. What is privacy in an information security context?
   * Answer: Privacy is not full independence from observation, but the "condition of being free from unwelcome intrusion."
7. What is another name for the Kennedy–Kassebaum Act (1996), and why is it important to organizations that are NOT in the healthcare industry?
   * Answer: HIPPA safeguards health-care data confidentiality and security by developing and enforcing standards and standardizing electronic data transfer.
8. If you work for a financial services organization such as a bank or credit union, which 1999 law affects your use of customer data? What other effects does it have?
   * Answer: Gramm-Leach-Bliley Act of 1999, also known as the Financial Services Modernization Act.  This act mandates all financial institutions to reveal their nonpublic personal information sharing policies. Customers must also be given adequate warning so that they can request that their information not be shared with third parties.
9. What is the primary purpose of the USA PATRIOT Act, and how has it been revised since its original passage?
   * Answer: Modified a wide range of current legislation to provide law enforcement authorities more leeway in combating terrorism-related activity. The Patriot Act amended several laws, including some of the first to deal with electronic technology.
10. What is PCI DSS, and why is it important for information security?
    * Answer: The main card brands agreed on the Payment Card Industry Data Security Standard as a common, consistent, and secure minimum degree of security to be adopted by all organizations that process, store, or transfer cardholder data in order to protect payment card data and payment card customers.
11. What is intellectual property (IP)? What laws currently protect IP in the United States and Europe?
    * Answer: Interesting question, In the United States, intellectual property is recognized as a protected asset. Copyright rules in the United States extend this privilege to the published word, including electronic versions. Fair use of copyrighted works involves using them to support news reporting, teaching, scholarship, and a variety of other related activities, as long as the usage is for educational or library purposes, not for profit, and does not exceed a certain threshold.
12. How does the Sarbanes–Oxley Act of 2002 affect information security managers?
    * Answer: Top management is concerned with the reliability of information received from technical managers, but these managers require information security managers to certify that the information is confidential and uncorrupted.
13. What is due care? Why should an organization make sure to exercise due care in its usual course of operations?
    * Answer: If an organization refuses to exercise appropriate care, it raises its liability. When an organization ensures that every employee understands what acceptable and inappropriate behavior is, as well as the consequences of illegal or unethical activity, due care has been done.
14. How is due diligence different from due care? Why are both important?
    * Answer: Due diligence demands a business to make a genuine attempt to protect others and to sustain this level of effort over time.
15. What is a policy? How is it different from a law?
    * Answer: A policy is a defined set of expectations that describe acceptable and inappropriate workplace practices. The distinction between a policy and a law is that policy ignorance is a valid defense.
16. What are the three general categories of unethical computer use?
    * Answer:
      + Software License Infringement
      + Illicit Use
      + Misuse of Corporate Resources
17. What are the three general causes of illegal or unethical activity?
    * Answer: Organizations and society should strive to eliminate three types of unethical and illegal behavior: those caused by ignorance, those caused by accident, and those that are willful.
18. Of the information security organizations listed in this module that have codes of ethics, which has been established for the longest time? When was it founded?
    * Answer: Association of Computing Machinery (ACM) 1947
19. Of the organizations listed in this module that have codes of ethics, which is focused on auditing and control?
    * Answer: The Information Systems Audit and Control Association (ISACA)
20. How do people from varying ethnic backgrounds differ in their views of computer ethics?
    * Answer: Individuals will be more or less accepting of various techniques that breach or enable information security due to differing values or ethical perspectives.

### Module 07: Security and Personnel Review Questions

1. What member of an organization should decide where the information security function belongs within the organizational structure? Why?
   * Answer: No one individual should have sole authority over information security within the firm. Someone should make decisions on where the information security function goes inside each department based on the needs of that department's goals and resources.
2. List and describe the options for placing information security within the organization.
   * Answer:
     1. The Information Technology Department
     2. Standalone Department
     3. Security
     4. Administrative Services
     5. Insurance/Risk Management
     6. Legal Department
3. For each major information security job title covered in the module, list and describe the key qualifications and requirements for the position.
   * Answer:
   * CISO requires a 4-year degree, communication, interpersonal, management skills. Manages the overall infosec program, Drafts/approves information security policies, works w/ CIO on strategic, develops tactical Develops infosec budgets, sets priorities for implementation of information security projects, makes decisions/recommendations for recruiting/hiring/firing
   * Security Manager or Security Analyst requires Bachelor's in tech, bus, or security related, CISSP certification, budgeting, project management, and hiring and firing, manage technicians. some of the responsibilities correlate with Accomplishing CISO objectives and resolve technician issues, General understanding of tech, Ability to draft middle and lower-level policies, standards and guidelines, Experience in trad, Manage technicians
4. What factors influence an organization’s decisions to hire information security professionals?
   * Answer: During the screening process, firms will pay close attention to the technical competence and expertise required to fill the post. Candidates that hold and maintain relevant certifications such as CISSP and SSCP generally stand out to companies.
5. Prioritize the list of general attributes that organizations seek when hiring information security professionals. In other words, list the most important attributes first. Use the list you developed to answer the previous review question.
   * Answer:
     1. Always remember business over technology.
     2. Look at the source of the problem first and determine the factors involved.
     3. Your job is to protect the organization's information, never lose sight of the goal.
     4. Be heard not seen.
     5. Speak to users, not at them.
     6. Your education is never complete.
6. What are critical considerations when dismissing an employee? Do they change according to whether the departure is friendly or hostile, or according to which position the employee is leaving?
   * Answer: Hostile terminations must prohibit access to all points as soon as possible once the choice is made. Good security measures dictate that every termination be treated as an unfriendly exit in case anything has gone wrong in the employee's psychology. The greater the employee's access, the more significant the termination process becomes, as do legal documentation such as Non-Disclosure Agreements.
7. How do security considerations for temporary or contract employees differ from those for regular full-time employees?
   * Answer:
8. What career paths do most experienced professionals take when moving into information security? Are other pathways available? If so, describe them.
   * Answer: The most prevalent career pathways for Information Security Professionals are CISO or CIO.
9. Why is it important to use specific and clearly defined job descriptions for hiring information security professionals?
   * Answer: The descriptions can be used to boost professionalism in the IT area as well as improve role and responsibility uniformity. The description will inform the potential employee exactly what the employer is looking for.
10. What functions does the CISO perform?
    * Answer: The CISO is often the organization's leading information security officer and does not have an executive level role. Normally, this position reports to the Chief Information Officer (CIO). CISOs are first and foremost business managers, then technologists, but they must be well-versed in all aspects of information security. In many circumstances, the CISO is the program architect for information security.
11. What functions does the security manager perform?
    * Answer: The security manager oversees a company's overall security activities. They develop rules to ensure employee safety and aim to maintain an overall safe atmosphere.
12. What functions does the security analyst perform?
    * Answer: This is frequently an entry-level role, yet it takes a high level of technical expertise and knowledge to fill. Security analysts typically specialize in a specific type of software deployment, so one might deploy a firewall while another deploys an IDPS. Although familiarity with the given sort of technology may be sufficient to secure an interview, businesses prefer genuine experience with the specific piece of technology.
13. What rationale should an aspiring information security professional use in acquiring professional credentials?
    * Answer: Because technology is always changing, your credentials and expertise of technology may become obsolete in the coming years. Because technology evolve and there is no final finish with information security experts, the aim is to not view certification or mastery of a field as permanent.
14. List some of the information security certifications mentioned in this module.
    * Answer:
      + ISC2, or International Information Systems Security Certification Consortium, is a certification family that focuses on higher level security management functions and includes some of the most prominent certifications available today.
      + IASCA - these certifications target management functions and delve into supervision specializations such as systems auditing.
15. Discuss the financial costs of certification. How expensive is the process?
    * Answer: The process of determining how much money was spent on development and construction is known as cost certification.
16. List and describe the standard personnel policies and practices that are part of the information security function.
    * Answer:
17. Job descriptions should be reviewed and updated on a regular basis to avoid revealing access privileges to prospective workers.
18. Interviews - tell HR to minimize information offered to cand regarding duties and access privileges; prevent tours via secure and restricted sites.
19. Background checks should be performed prior to extending a job offer.
20. Employment Contracts - compel employees to sign written agreements and nondisclosure agreements; "employment dependent upon agreement"
21. New Hire Orientation - comprehensive security briefing; procedures for completing relevant sec ops; outline of approved levels; training provided
22. On-the-Job Security Training - instruction in security awareness
23. Evaluating Performance: Integrate information security into evaluations
24. Exit - clear the system of any emp traces; request org property from emp
25. Why shouldn’t an organization give a job candidate a tour of secure areas during an interview?
    * Answer: Job seekers are not workers; they are potential employees who may become employees; consequently, they should not be aware to the inner workings of the organization or its procedures.
26. List and describe the typical relationships that organizations have with temporary employees, contract employees, consultants, and business partners. What special security precautions must an organization consider for such workers, and why are they significant?
    * Answer: Temporary employees, contract employees, and contractors are not subject to the same stringent screening and contractual requirements as permanent employees, but they do have access to sensitive information within the firm. The organization hires temporary personnel to fill a temporary position or to enhance the existing staff.
27. What is separation of duties? How can it be used to improve an organization’s information security practices?
    * Answer: This ensures that no single individual has access to highly sensitive assets. Because it holds employees accountable to their peers, this can be utilized to strengthen information security standards.
28. What is job rotation, and what benefits does it offer an organization?
    * Answer: Job rotation is an internal control strategy that seeks to reduce both the misuse and abuse of company resources as well as economic vulnerability by requiring most employees to become familiar enough with each other's regular, individual duties to detect any suspicious anomalies in another employee's work and perform his duties in his absence. In a nutshell, it is a human redundancy control.

## Part Two

### Hands-On Project: Microsoft OS Processes and Services

Complete the Hands-On Project: Microsoft OS Processes and Services

After completing the hands-on project, answer the following prompts

### Self-Reflection and Response

What is the difference between a process and a service in the Windows operating system?

|  |
| --- |
| A process is a running instance of a specific executable (.exe computer file). A service is a background process that does not interact with the desktop. |

Can you think of why you would need to be able to determine which processes are running on your Windows computer?

|  |
| --- |
| We need to know which processes are running on a Windows computer since they can consume all of the RAM if they go unnoticed. Users should understand which processes are active and which services are required. Processes can thus be stopped and restarted as needed. |

Can you think of why you would need to be able to determine which services are running on your Windows computer?

|  |
| --- |
| We need to know which services are operating on a Windows computer because if they go undiscovered, they can devour all of the RAM. Users should be aware of which services are active and which services are necessary. As a result, services can be stopped and restarted as needed. |

### Hands-On Project: Backup and Recovery and File Integrity Monitoring

Complete the Hands-On Project: Backup and Recovery and File Integrity Monitoring

After completing the hands-on project, answer the following prompts

### Self-Reflection and Response

Have you chosen to make a backup copy of your computer system? In the space below, explain why or why not. What steps did you take (or will you take in the future) to research and implement your method?

|  |
| --- |
| Prior to taking this course, I had never given it any thought. I didn't realize how important it was for me to take these precautionary measures. Despite having an online backup plan through Google Cloud, I will ensure that I have a primary copy, a backup, and an online backup. |

Can you think of another reason, not mentioned in the lab, for using the File Integrity monitor featers found in PowerShell? Describe how you might use it.

|  |
| --- |
| Aside from utilizing PowerShell's File Integrity Monitor functions to compare files for changes, I believe another reason to use it is to determine whether a file I have received is from a secure source. To ensure that the content has not been altered when downloading from the webserver to the computer via the internet. |

Were you able to install and use the hashing tools from MaresWare? What was your experience using these tools?

|  |
| --- |
| Yes. I was able to install and use Mares Ware's hashing tools. Everything went nicely because I followed the instructions. I discovered that hash values are used to ensure that the contents of a file have not been altered in a cryptographically secure manner. |