ISC2

Domain 7 Key Takeaways

Overall, security professionals reviewing CISSP Domain 7 must understand the principles of security operations and the different tools and techniques used to manage security incidents, disaster recovery, and business continuity planning. This includes understanding the importance of ongoing monitoring and review of security controls and systems and of following regularly updated policies and procedures.

1. Security operations involve the day-to-day management and implementation of security controls, including incident management, disaster recovery, business continuity planning and ongoing monitoring of security controls and systems.

2. Incident management involves responding to security incidents, including identifying and containing the incident, conducting forensic analysis, and restoring normal operations.

3. Disaster recovery involves preparing for and responding to natural disasters and other catastrophic events that could disrupt normal operations.

4. Business continuity planning involves developing and implementing plans to ensure that critical business functions can continue in the event of a disruption.

5. Security operations should be guided by policies and procedures and should be reviewed and updated on a regular basis to ensure that they remain effective.

6. Collaboration and communication with other departments, such as legal, human resources, and IT, is essential to ensure effective security operations.

Investigations

- Regardless of the investigation type and its potential to end up in a court of law, all personnel involved with an investigation must first and foremost accept that protecting the integrity of that investigation must be of paramount importance.

- Failure to balance rights and responsibilities against normal business pressures can cause even more trouble for the organization and the ones who violate these boundaries than the original incident would have caused by itself.

- One of the challenges of conducting digital investigation is that during a cyber incident, the incident scene can involve various geophysical locations and jurisdictions, not limited to where the compromised systems/data reside, the location of the intruder (if unauthorized intrusion was an element of the incident) and any locations between the compromised systems and the intruder where resources were used to aid the intruder.

- When presenting evidence, the security professional should adhere to the tenets of admissibility, accuracy, comprehensibility, and objectivity.

- Some general digital forensics principles to be aware of include documenting everything, avoiding unrecorded or unintended modification and maintaining evidence. Because forensic analysis requires such specific knowledge and skills, it is best to use a certified (and if need be, licensed) external contractor when necessary. Take care that your organization considers all applicable laws when crafting its own policies regarding evidence collection, analysis, and presentation.

Logging and Monitoring

- Log management underlies all of the analytical activities that rely on system reporting. The diverse purposes of those activities demand flexibility in logging infrastructure and practices to meet the different detection, compliance, process improvement, and operational requirements.

- Every security framework addresses logging expectations in some fashion. Well-structured log management practices address issues such as:

    - Logging compliance and standards
    - Logging policies throughout the systems and information lifecycles
    - Logging infrastructure
    - Log generation, collection, and normalization
    - Log protection from creation to disposition (archiving or defensible destruction)
    - Log review, analytics, and reporting

- Unauthorized entry into an organization's environment, and especially into its information systems, can affect all of the security elements of the CIA triad or the broader CIANA+PS set. Security professionals often discuss two general conceptual classes of intrusion security mechanisms: intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).

- The general idea of a security information and event management (SIEM) solution is to gather log data from various sources across the enterprise to better understand potential security concerns and apportion resources accordingly.

- Information Security Continuous Monitoring (ISCM), coupled with automation, maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The organization must have the tools and underlying systems infrastructure to gather, analyze, and report on the monitored environment.

- Threat intelligence activities rely heavily on proper reporting and correlation of information to develop a comprehensive list of current organizational threats. In turn, metrics can be applied to various threats, threat scenarios and activities that indicate a particular threat is likely or active. This allows the organization to detect incidents in a timelier manner, speeding appropriate response and reducing the impact of events.

- User and entity behavior analytics (UEBA) systems rely on information collected by the logging and SEIM systems and are often implemented as an analytical function of the SEIM

environment. They typically create a template of normal behavior based on monitoring of the environment over time. These templates can include both individuals in the IAM environment as well as system behaviors. This allows UEBA systems to identify previously unknown attacks.

Configuration Management, Patch, and Vulnerability Management and Change Management Processes

- One of the more widely adopted information technology change practices is defined in the Information Technology Infrastructure Library (ITIL) version 4, under the name of Change Enablement. This standard provides broad guidelines for change management practices, recognizing that individual organizations' implementation of change practice will be affected by the organization's culture, business practices, statutory and regulatory requirements, and other factors.

- All of the major change management practices address a common set of core activities that start with a request for change and move through various development and test stages until the change is released to the end users. Well-structured change management practices include:

    - Change initiation
    - Change review and approval
    - Implementation and evaluation
    - Release and deployment planning and control
    - Patch management
    - Vulnerability management

- Configuration management is a formal, methodical, comprehensive process for defining, documenting, and enforcing the minimum controls necessary to safeguard an organization's information systems. Configuration management requires that the organization identify its configuration items (CIs), which are the assets under its security scope.

Security Operations Concepts

- Defense in Depth can be used as a framework for showing how AC models can be used as part of an organization's overall information security architecture.

    - The concept of least privilege is that every person, process, service and system should have the minimum level of permissions required to perform their assigned duties and tasks—and nothing else.
    - Restricting access to information and individuals based on an entity's need to know is another important concept of AC.
    - Separation of duties (SoD) means that no individual person can complete an entire trusted action or process alone. The concept of SoD is to reduce chances of fraud within sensitive parts of the organization.
    - Dual custody, also known as dual control, provides a more secure AC architecture by requiring two or more individuals to simultaneously perform separate actions as part of a task or workflow that completes a critical action.

Incident Management

- Well-structured organizations have established business practices for handling information security incidents. Incident detection, assessment, escalation, communication, recovery, and learning from the event are activities typically integrated into the organization's incident response process. Clarifying who does what in an incident and under what circumstances will help the organization recover business functions.

- The security professional should understand their legal and organizational responsibilities for incident management and be able to evaluate the activities and overall effectiveness of the organization's incident response practice.

- When an incident occurs, the organization is often faced with a competing set of priorities in the recovery process. The incident management process must clarify how decisions are to be made, and by whom, so that all organizational interests are taken into account.

- Although each of these standards, sets of principles, frameworks, or regulations may disagree on a number of fine points, such as how many steps or stages there are in a "proper" incident response process, one thing is clear: litigation as an incident result means that investigations must thoroughly respect the chain of custody, the rights of all parties involved, and the laws of the jurisdictions that apply.

- The organization's incident response activities are designed to ensure that events with potential for harm are detected, assessed, and addressed efficiently to minimize the impact on an organization's business functions.

Operating and Maintaining Detective and Preventative Measures

- The security professional has a wide range of tools and techniques available to address security threats. Selecting the right approach requires a deep understanding of the organization's risk posture, as well as the capabilities of the tools and their limitations.

- Organizations can avail themselves of services offered by external entities to enhance security. This is especially true for organizations where security is not a core competency. When contracting third-party services of any kind, due diligence must be performed to confirm the provider's ability to actually do the work. This is even more essential when the services in question involve security that requires the client to place a great deal of trust in the provider.

Implementing recovery strategies

- Accurate and comprehensive backups are instrumental to facilitating business continuity and disaster recovery (BCDR) efforts; this is an essential aspect of the availability facet of the CIA triad.

- In the event the normal physical production environment (the building/ campus/location the organization's personnel perform work) no longer functions, the organization will require an alternate processing capability to remain viable. Organizations have many options to consider as they plan for an alternate operating location as part of their BCDR processes.

- Organizations with extreme sensitivity to downtime—medical providers, military and or intelligence agencies, high-volume online retailers, utilities, and others—have a greater need to provide high levels of availability and ensure BCDR capabilities are comprehensive and effective.

Implement and Test Disaster Recovery and Participate in Business Continuity Planning and Exercises

- A BCDR action can be triggered by a number of possible circumstances (e.g., natural disaster or severe weather, fire, physical damage to resources, external attack).

- In addition to the member(s) of senior management authorized to initiate the BCDR response action, the response plan should specifically task personnel who will be involved in the process.

- The organization will need to have the capacity and resources for two types of essential contingency communications: internal and external.

- There is a fundamental need to calculate the entire, overall impact of the contingency; this includes both the damaging effects of the event itself, as well as the cost of the response efforts. This assessment is best performed by accounting and audit personnel, with input from subject matter experts and HR.

- The goal of the response action is to resume full normal operations. The decision of when to return to normal operations must be made by senior management—often the head of the organization.

- The best way to assess the organizations' BCDR plan is to test it to see whether the designed plan actually operates as intended, or whether alterations are required to assure the plan meets the organizations' objectives. Running BCDR exercises should be mandated as part of the BCDR plan. Major types of exercise include:

    - Read-through and tabletop

- Walk-through
- Simulation
- Parallel
- Full interruption

Physical Security and Personnel Concerns

- In many cases, security professionals must advocate for proper facilities management practices and the integration of physical controls with logical and technical controls protecting the organization's assets.

- Protecting information requires that we protect the people who process that information. This requires the organization to develop appropriate policies, training and awareness programs to ensure people know what to do to protect themselves and the organization.