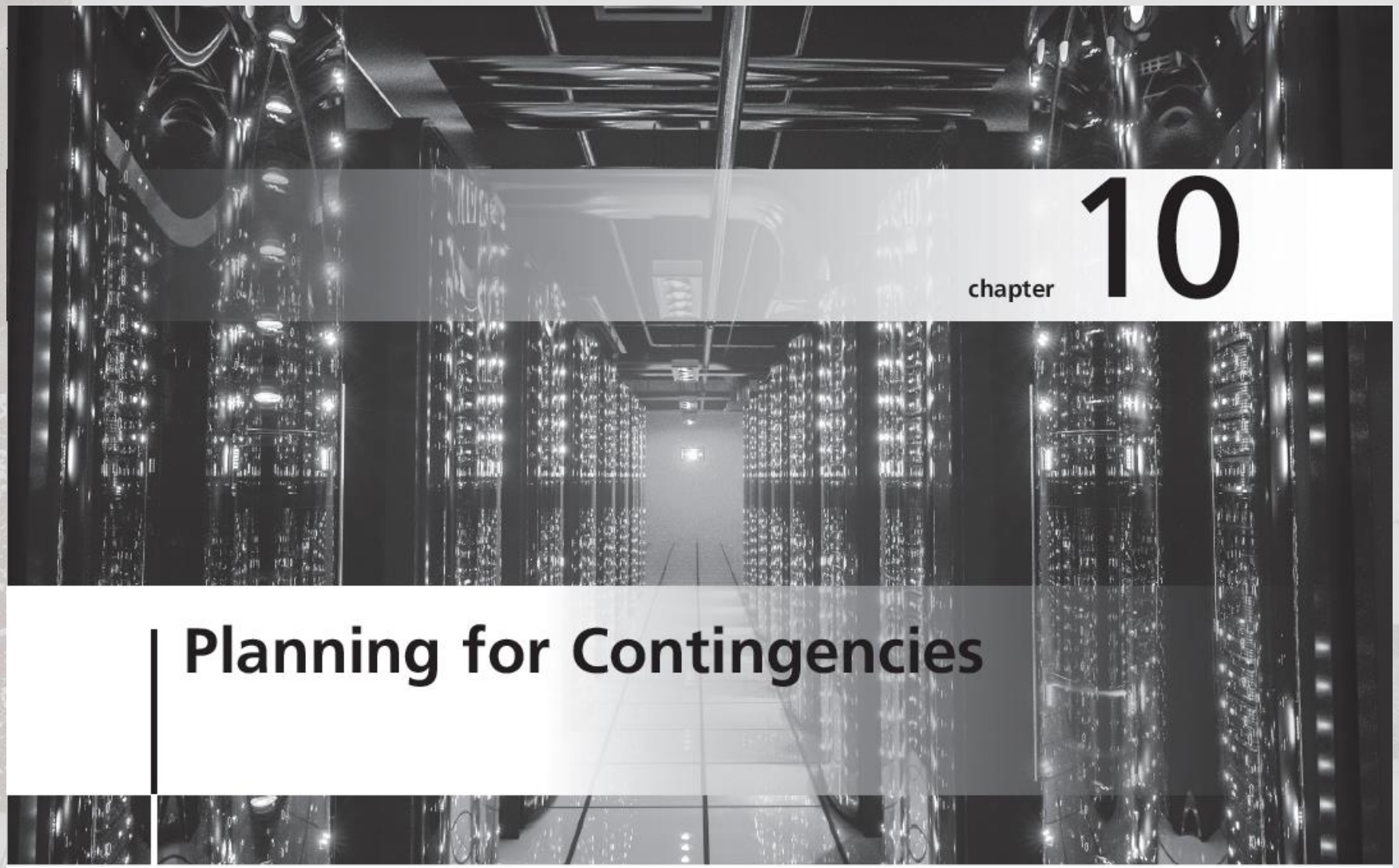
MANAGEMENT of INFORMATION SECURITY, Fifth Edition



chapter 10

Planning for Contingencies

Anything that can go wrong will go wrong.

—MURPHY'S LAW

TESTING CONTINGENCY PLANS

Testing Contingency Plans

- Very few plans are executable as initially written; instead, they must be tested to identify vulnerabilities, faults, and inefficient processes
- There are four testing strategies that can be used to test contingency plans:
  - Desk Check
  - Structured walkthrough
  - Simulation
  - Full interruption

Final Thoughts on CP

- Iteration results in improvement
- A formal implementation of this methodology is a process known as continuous process improvement (CPI)
- Each time the plan is rehearsed it should be improved
- Constant evaluation and improvement leads to an improved outcome

MANAGING INVESTIGATION IN THE ORGANIZATION

Managing Investigations in the Organization

- When - not IF - an organization finds itself having to deal with a suspected policy or law violation, they must appoint an individual to investigate it
- How the internal investigation proceeds will dictate whether or not the organization has the ability to take action against the perpetrator if in fact evidence is found that substantiates the charge
- In order to protect the organization, and to possibly assist law enforcement in the conduct of an investigation, the investigator (CISO, InfoSec Manager or other appointed individual) must act to document what happened and how

Digital Forensics

- Forensics is the coherent application of methodical investigatory techniques to present evidence of crimes in a court or court-like setting
- Digital forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis
- Like traditional forensics, it follows clear, well-defined methodologies, but still tends to be as much art as science

Digital Forensics

- Evidentiary material (EM), also known as an item of potential evidentiary value, is any information that could potentially support the organizations legal- or policy-based case against a suspect
- An item does not become evidence until it is formally admitted to evidence by a judge or other ruling official

Digital Forensics

- Digital forensics can be used for two key purposes:
  - To investigate allegations of digital malfeasance. A crime against or using digital media, computer technology or related components, is referred to as digital malfeasance
  - To perform root cause analysis. If an incident occurs and the organization suspects an attack was successful, digital forensics can be used to examine the path and methodology used to gain unauthorized access, as well as to determine how pervasive and successful the attack was

Affidavits and Search Warrants

- Many investigations begin with an allegation or an indication of an incident
- In law enforcement, the investigating agent would create an affidavit requesting a search warrant
- When an approving authority signs the affidavit or creates a synopsis form based on this document, it becomes a search warrant and grants permission to search for EM at the specified location and/or to seize items to return to the investigator's lab for examination
- In corporate environments, the names of these documents may change and in many cases may be verbal in nature, but the process should be the same
- Formal permission is obtained before an investigation occurs

Digital Forensics Methodology

- In digital forensics, all investigations follow the same basic methodology:
  1. Identify relevant items of evidentiary value (EM)
  2. Acquire (seize) the evidence without alteration or damage
  3. Take steps to assure that the evidence is at every step verifiably authentic and is unchanged from the time it was seized
  4. Analyze the data without risking modification or unauthorized access
  5. Report the findings to the proper authority

Evidentiary Policy and Procedures

- Organizations should develop specific digital forensics procedures, along with guidance on the use of these procedures
- EM policy should specify:
  - Who may conduct an investigation
  - Who may authorized an investigation
  - What affidavit-related documents are required
  - What search warrant-related documents are required
  - What digital media may be seized or taken offline
  - What methodology should be followed
  - What methods are required for chain of custody or chain of evidence
  - What format the final report should take, and to whom it should it be given

Law Enforcement Involvement

- When an incident violates civil or criminal law, it is the organization's responsibility to notify the proper authorities
- Selecting the appropriate law enforcement agency depends on the type of crime committed: Federal, State, or Local
- Involving law enforcement has both advantages and disadvantages:
  - They are usually much better equipped at processing evidence, obtaining statements from witnesses, and building legal cases
  - However, involvement can result in loss of control of the chain of events following an incident