Local Network Security in the Real World

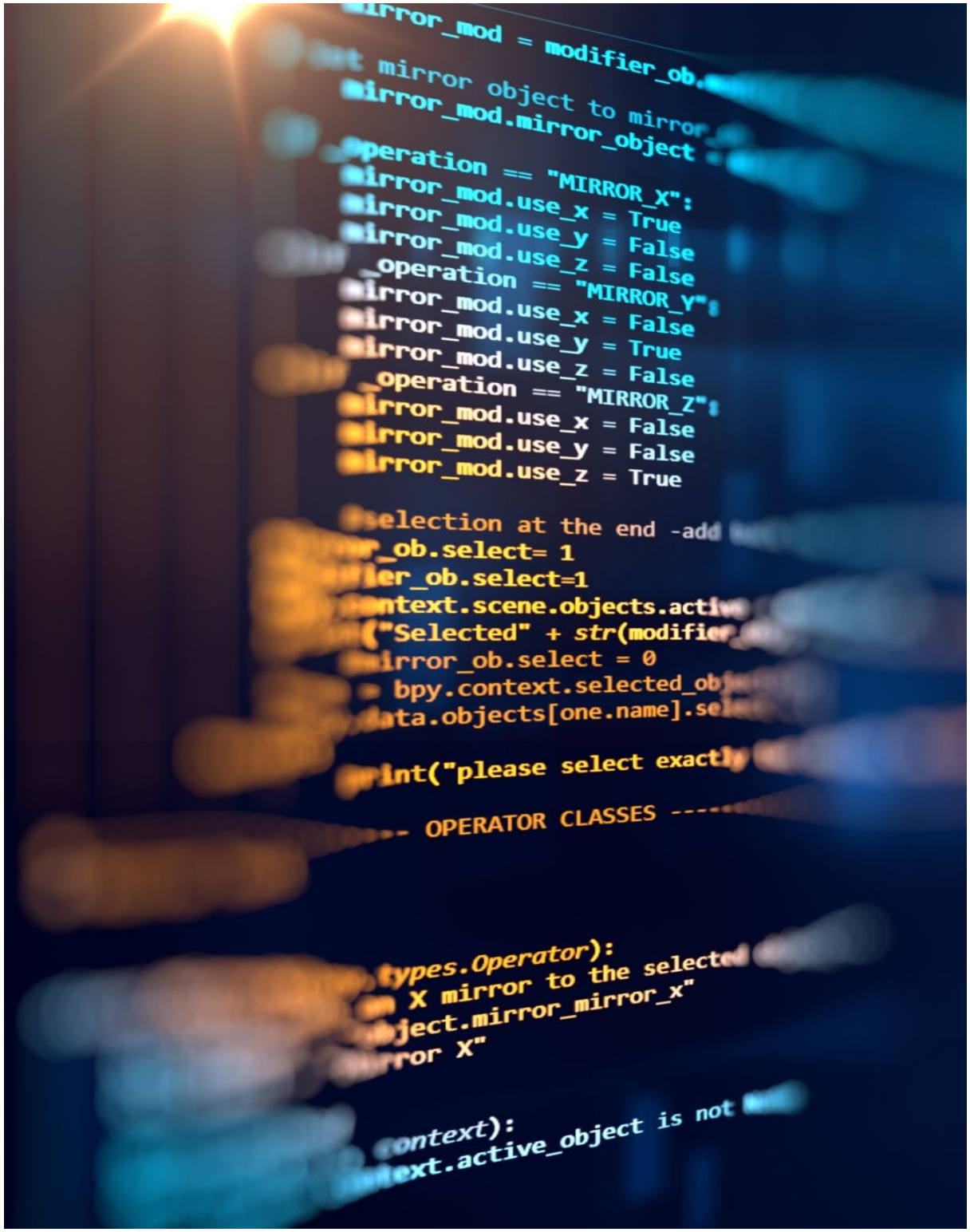
Chapter 11

Professors: David A. Cass and Kevin McKenzie

Lecture 7 part 1

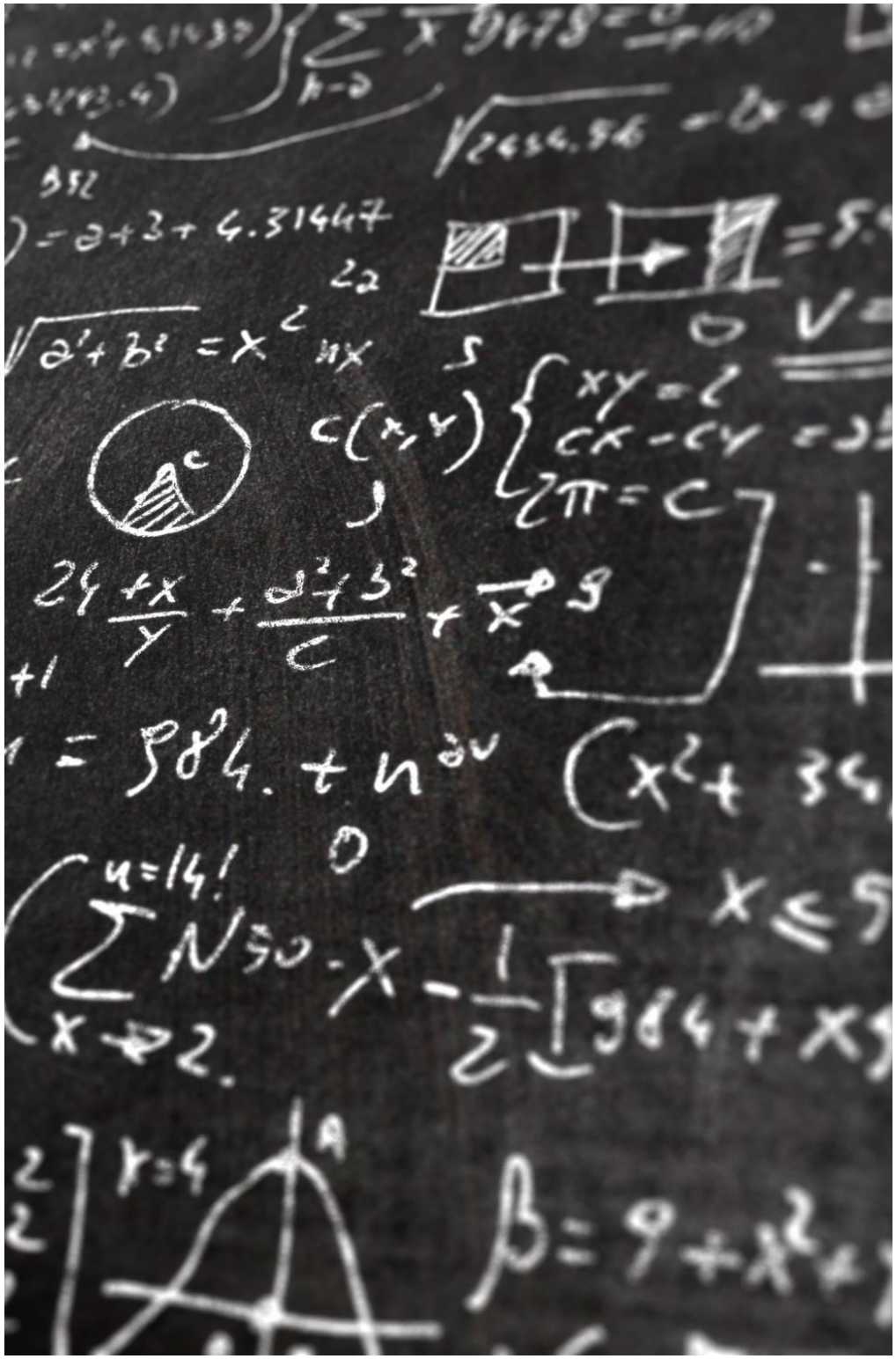
In this lecture, you'll learn to:

- Apply applicable Categories and Subcategories of the NIST Cyber Security Framework's Identify function to a specific scenario to document the network's assets and their possible vulnerabilities.



In this lecture, you'll learn to:

- Use applicable Categories and Subcategories of the Protect function to generate specific policies and actions that can be used to secure the network's assets for the specific scenario.



In this chapter, you'll learn to:

- Apply applicable categories and Subcategories of the Detect function to identify technologies, policies, practices, and strategies that can be used to monitor the network in the scenario to determine whether security events are occurring.

In this chapter, you'll learn to:

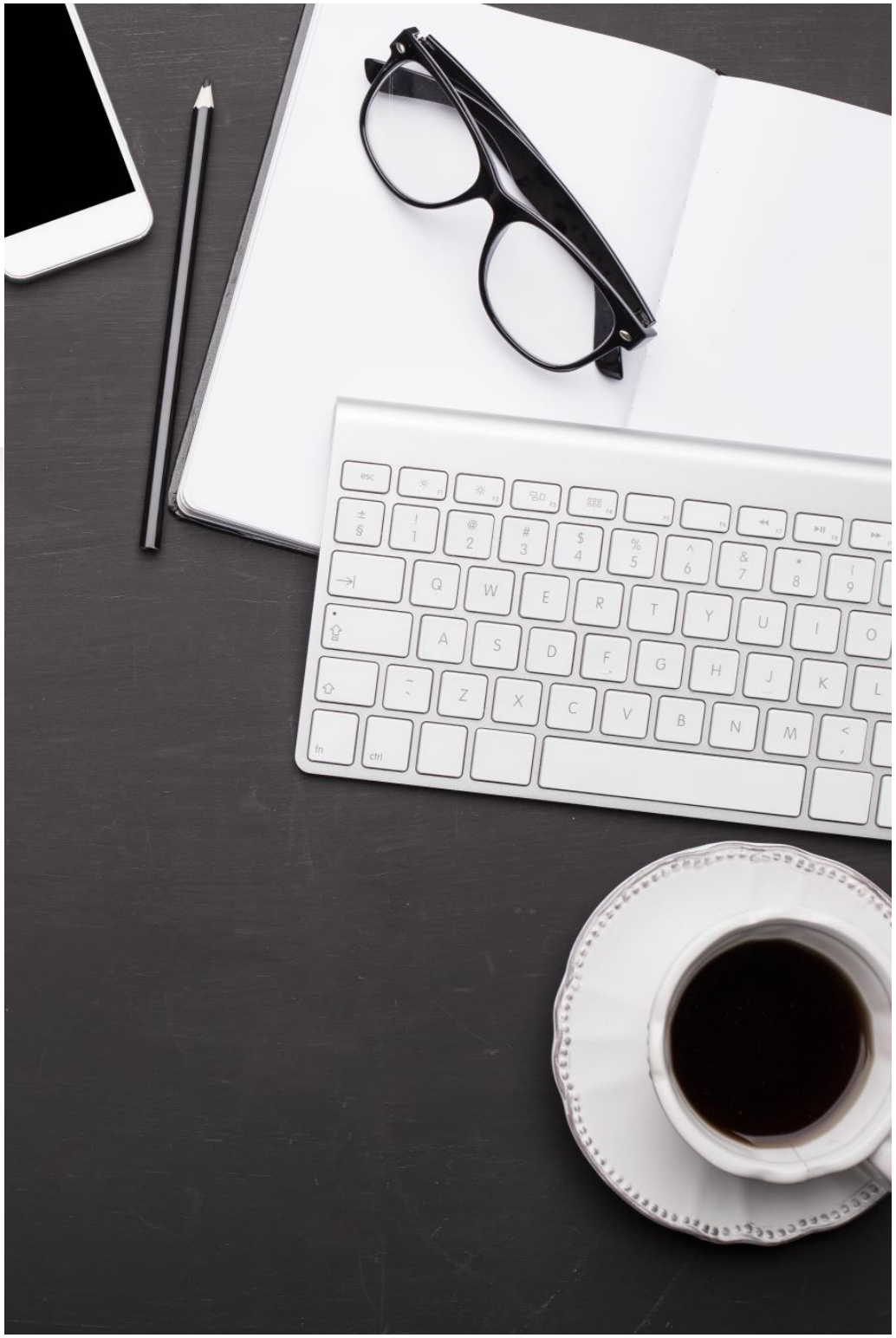
- Apply applicable Categories and Subcategories of the Respond function to create an incident response plan to cover specific security events associated with the scenario presented.

In this chapter, you'll learn to:

- Apply applicable Categories and Subcategories of the Recover function to the scenario to implement solutions for recovering from specific cyber events.

Scenario 1 computers are equipped with:

- Executive Staff – The executive staff conducts the following electronic activities:
  - Conducting electronic banking activities via the Internet



Scenario 1 computers are equipped with:

- Administrative Staff - The administrative staff is involved in the following electronic functions:
  - Managing server-based accounting, warehousing and inventory program
  - Managing electronic employee payroll and time-keeping records

Scenario 1 computers are equipped with:

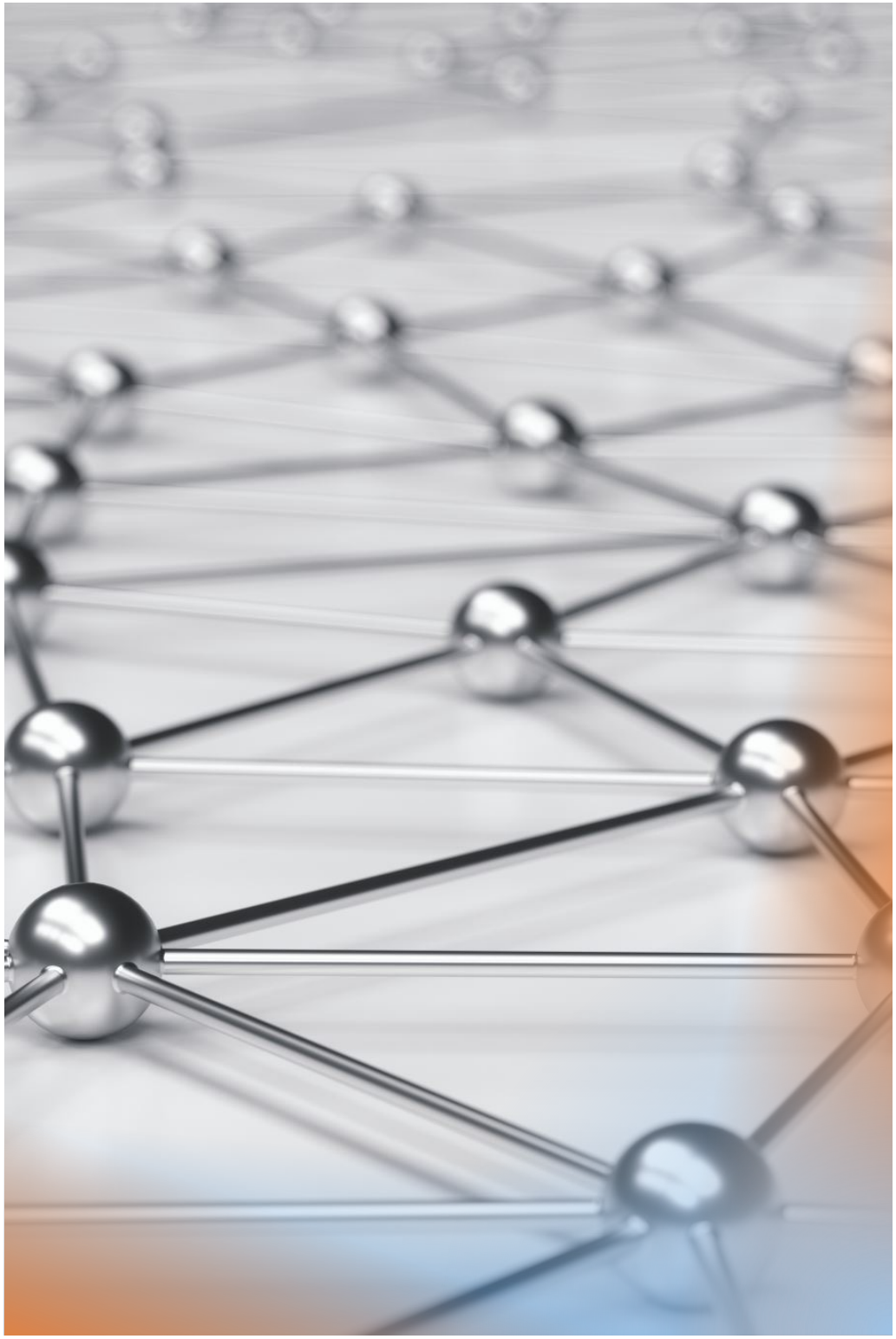
- Sales and Marketing Team – Sales and marketing personnel that work in-house and on the road as required to prospect for customers, interact with outside sales representatives, and make customer visits and presentations. They are involved in the following electronic activities:
  - Handling incoming emails and customer sales calls
  - Operating an outbound email contact manager

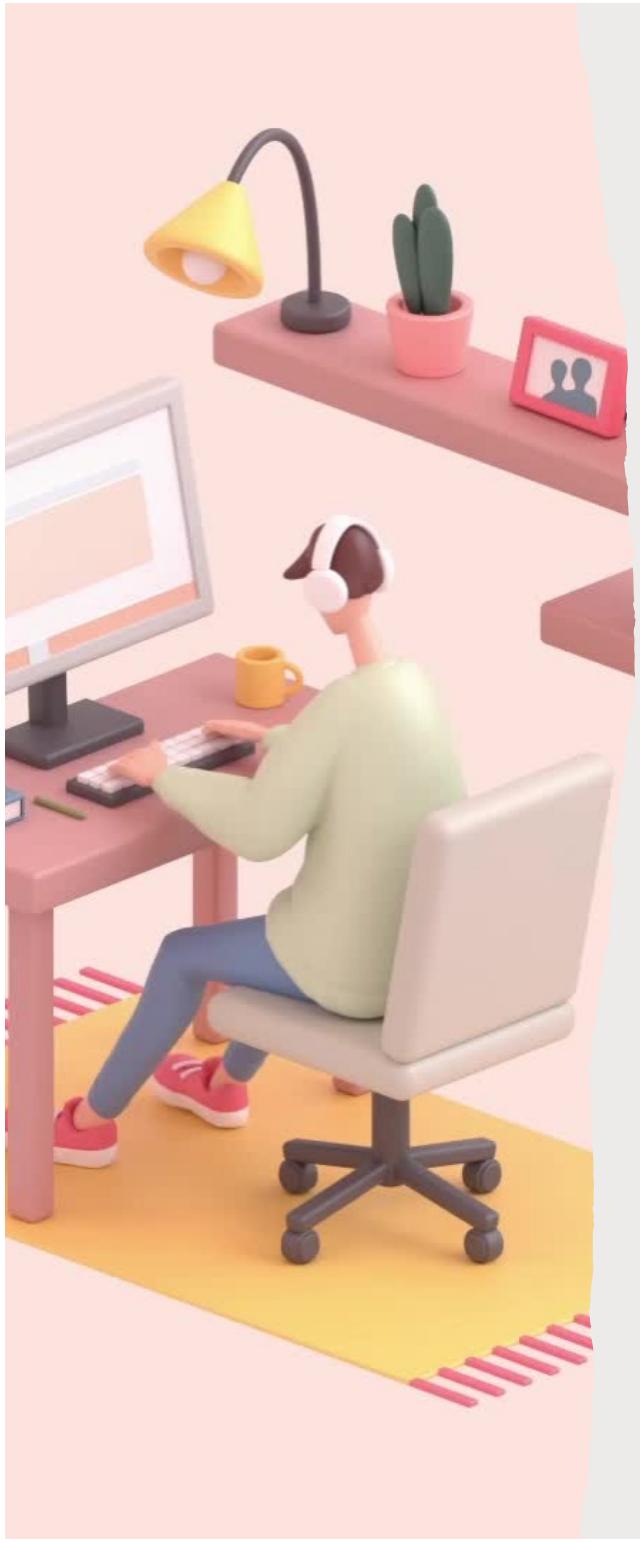
Scenario 1 computers are equipped with:

- Sales and Marketing Team –They are involved in the following electronic activities:
  - Tracking customer interactions using a server-based customer management database program
  - Interacting with the home office when traveling to retrieve documents, product updates, emails and other communications

Scenario 1 computers are equipped with:

- Sales and Marketing Team –They are involved in the following electronic activities:
  - Interacting with their Internet ISP and their internal content development team to manage and update the company's website





Scenario 1 computers are equipped with:

- Content Development Team – Writers, editors and artists. Some of these workers are located in the company facility, some live and work remotely and never physically access the facilities, and some combine in-house work with telecommuting so they are in the office one or two days per week. Their electronic activities include the following:
  - Create text and graphic content on local machines but with the need to share that information as freely between the team members as possible

Scenario 1 computers are equipped with:

- Content Development Team – Their electronic activities include the following:
  - Conducting web-based and hands-on research on technical products within a lab environment

Scenario 1 computers are equipped with:

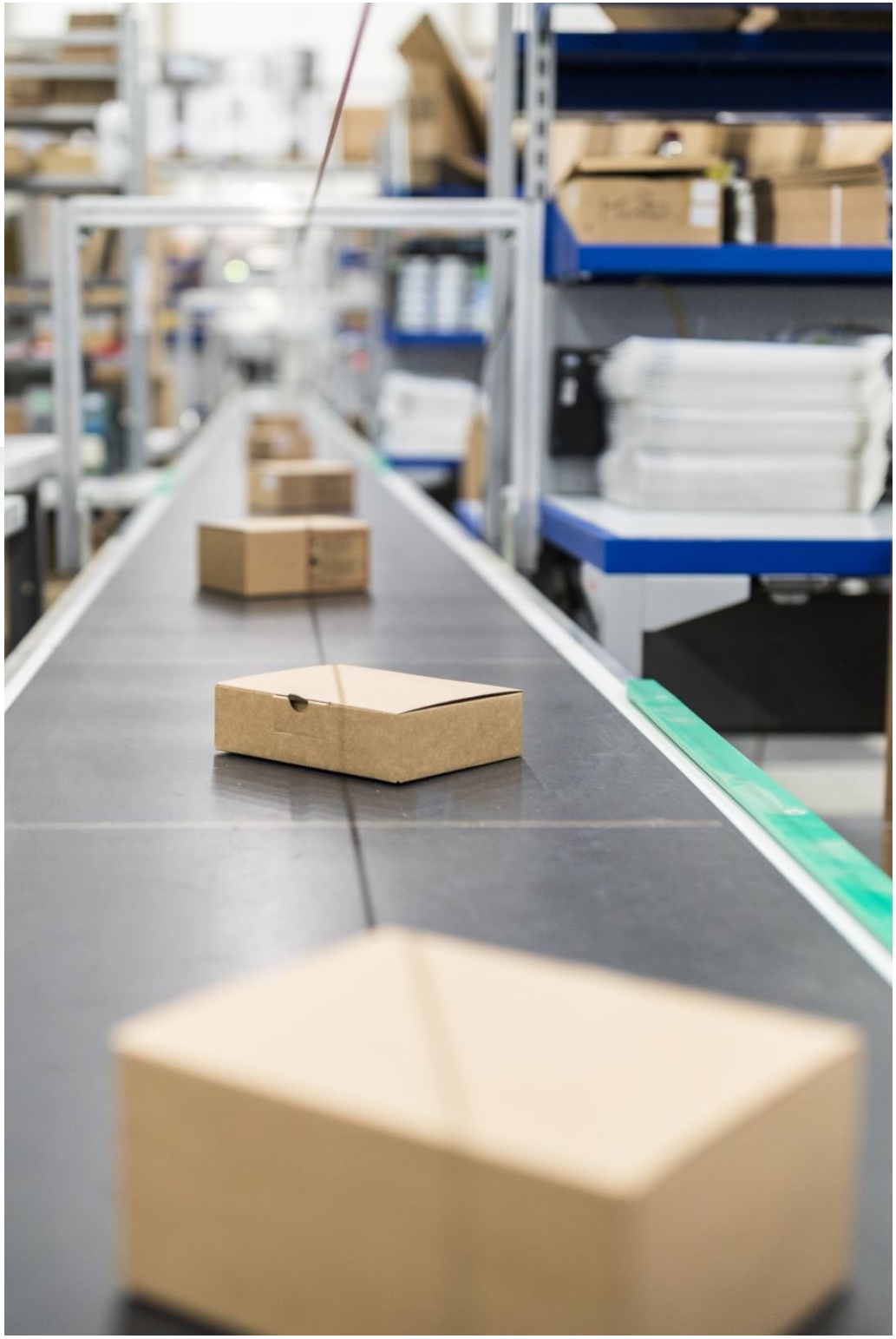
- Customer Support Team – Technicians dedicated to handling customer technical-support calls, testing failure reports, and creating new or updated content for any errors or omissions in the IP. They also arrange and track replacement and update products that must be delivered to the customers.
    - Interacting with the customer management program to review past customer interactions and create service records of problem calls and resolution actions

Scenario 1 computers are equipped with:

- Customer Support Team – Technicians dedicated to handling customer technical-support calls, testing failure reports, and creating new or updated content for any errors or omissions in the IP.
  - Interact with the Content Development Team to share content problems reported by customers and offer rough revision materials as required

Scenario 1 computers are equipped with:

- Warehouse and Shipping Team – Workers involved in the receiving, storage, inventory tracking and shipping of products. These employees have the following electronic activities associated with their jobs:
  - Interacting with the warehouse and inventory portion of the company's accounting software to update and track product receiving and shipping, as well as current inventory levels



Scenario 1 computers are equipped with:

- Warehouse and Shipping Team –These employees have the following electronic activities associated with their jobs:
  - Interact with Federal Express, United Parcel Service, and over-the-road trucking companies via Internet to schedule and track shipments

Detect

- What types of systems do you need to have in place to monitor personnel activity to detect potential cybersecurity threats associated with the servers (NIST DE.CM-1, 3)?

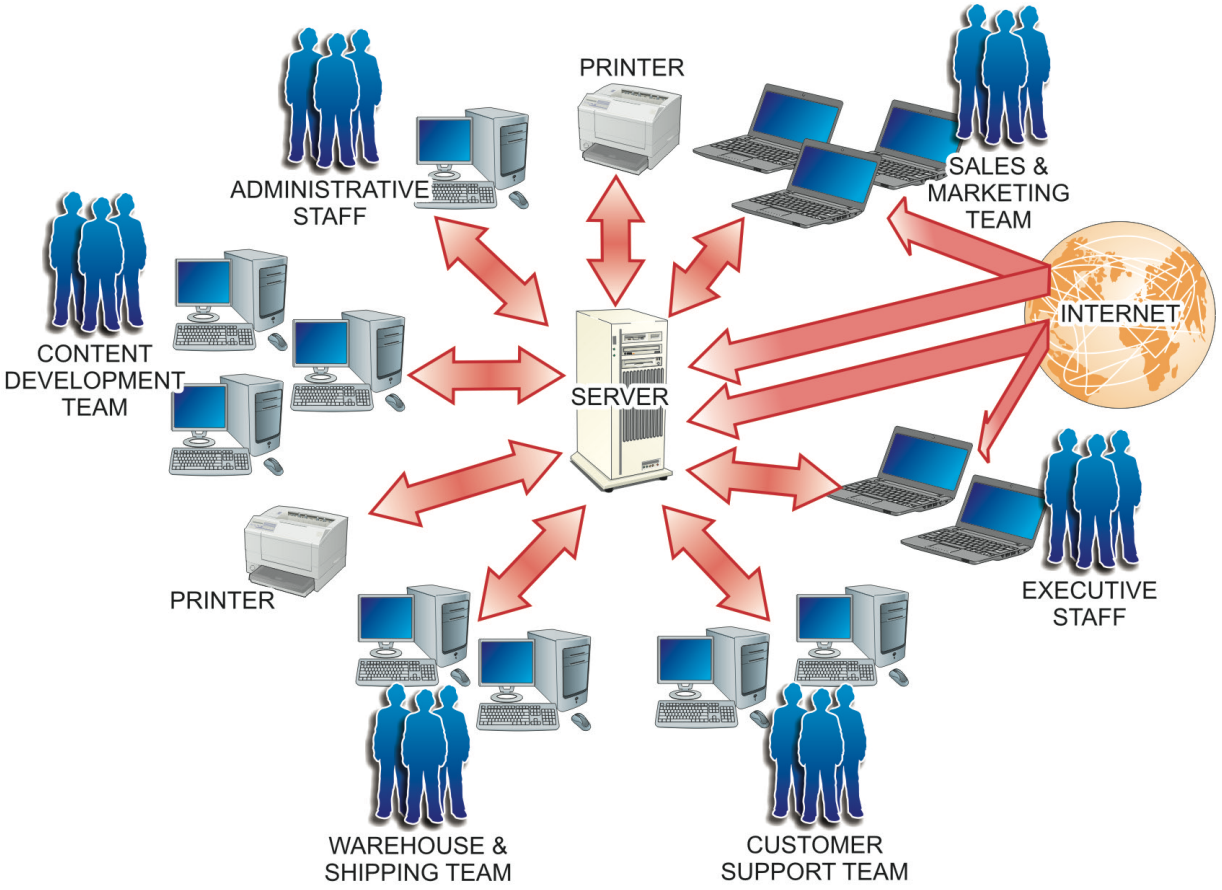
Respond

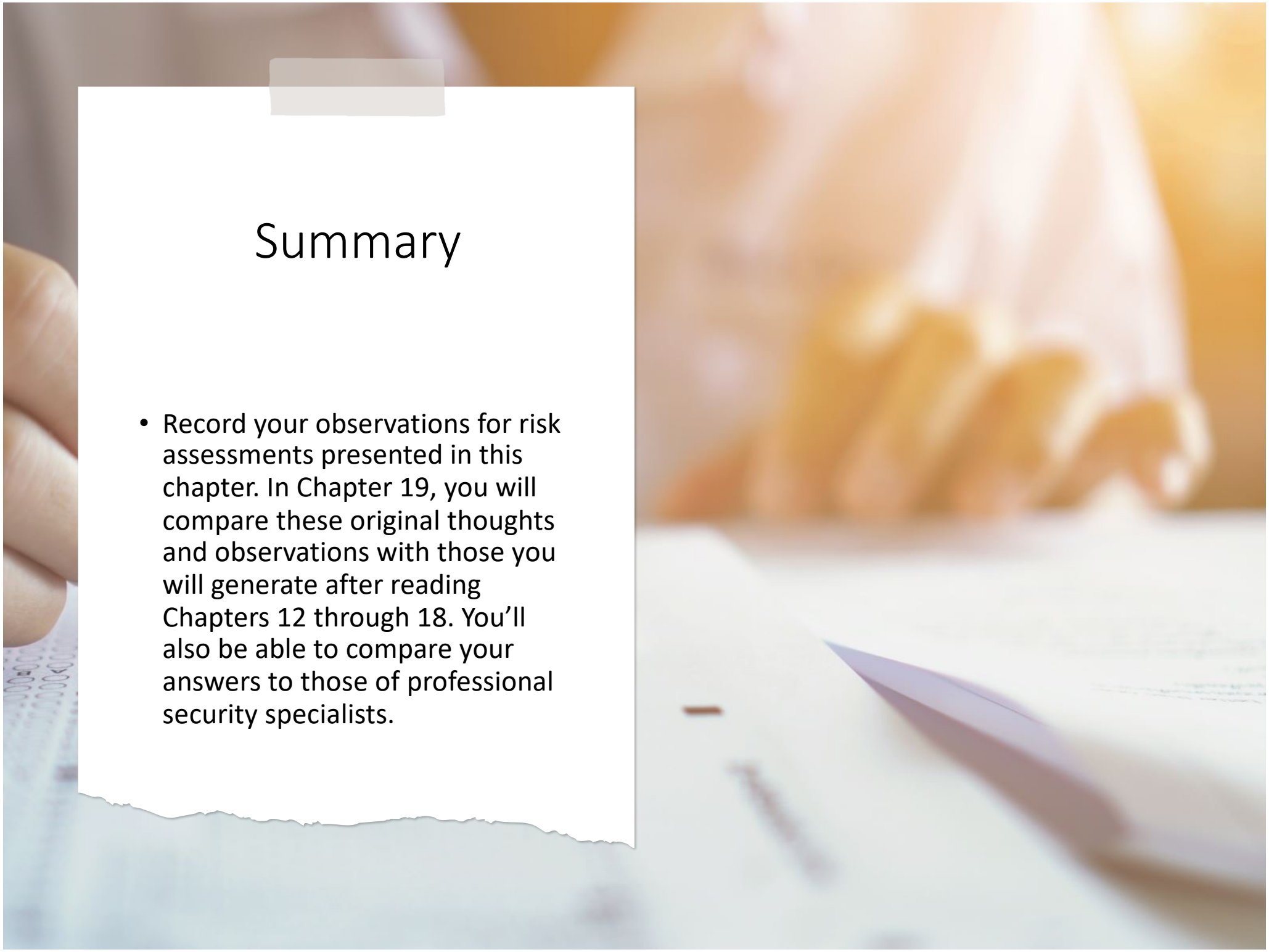
- Considering the information kept on the company's servers, which type of response plan might be necessary when physical security is breached in the server room (NIST RS.CO-4, 5)?

Recover

- What items might a recovery plan include if server security is breached at the company (NIST RC.CO-1, 2)?

The Company Network Layout





Summary

- Record your observations for risk assessments presented in this chapter. In Chapter 19, you will compare these original thoughts and observations with those you will generate after reading Chapters 12 through 18. You'll also be able to compare your answers to those of professional security specialists.