

Module 12: Assignment

12-1: Testing Password Strength

How strong are your passwords? Various online tools can provide information on password strength, but not all feedback is the same. First, assign the numbers 1 through 3 to three passwords that are very similar (but not identical) to passwords you are currently using, and write down the number (not the password) on a piece of paper. Then, enter those passwords into these three online password-testing services:

- How secure is My Password (howsecureismypassword.net/)
- Password checker online (password-checker.online-domain-tools.com)
- Password Meter (www.passwordmeter.com/)

Record next to each number the strength of that password as indicated by these three online tools. Then use each online password tester to modify the password by adding more random numbers or letters to increase its strength.

- How secure are your passwords?
- Would any of these tools encourage someone to create a stronger password?
- Which provided the best information?

Create a one-paragraph summary of your findings.

12-2: Password Management

Applications research at least four password vaults, more commonly known as password management applications, one of which is a stand-alone application and another of which is a browser-based application.

- Create a table that lists and compares their features.
- Which would you recommend? and why?

Create a report on your findings.

12-3: Create your Own Cognitive Biometric Memorable Event

- What type of cognitive biometric “memorable event” do you think would be effective?

Design your own example that is different from those given in the module. There should be five steps, and each step should have at least seven options. The final step should be a fill-in-the-blank user response. Compare your steps with those of other learners.

- Which do you think would be the easiest for users?

Module 13: Assignment

13-1: Forensics Tools

Search the Internet for websites that advertise computer forensic tools. Locate reviews of four tools.

- Create a chart that lists the tool, the type of data that it searches for, its features, the cost, etc.

Which would you recommend if you could purchase only one tool and budget were not a concern?

13-2: Diamond Model of Intrusion Analysis

The Diamond Model of Intrusion Analysis is a framework for examining network intrusion events. Use the Internet to research this model.

- Identify how it is used, its strengths and weaknesses, and how widely implemented it is.
- What is your conclusion about this framework?
- How useful does it appear to be to you?

Write a one-page analysis of your research.

13-3: SOAR Run-books and Playbooks

Research SOAR run-books and playbooks. If possible, locate an example and read through each type.

- What are their advantages?
- What are their disadvantages?
- How are they used?

Write a one-page paper on your research.

13-4: Sources of Forensics Data

IP software monitors can provide insight into an incident for a forensics evaluation. Use the Internet to research NetFlow, sFlow, and IPFIX.

- How are they used?
- What are their differences?
- What are their similarities?

Create a table that lists the strengths and weaknesses of each.

13-5: Log collection and analysis tools

Research the log tools syslog, nxlog, rsyslog, syslog-ng, and journalctl.

- Create a table that compares each of them, and list how they are used.
- Include a detailed description of the strengths and weaknesses of each tool.

Write a one-page paper on your research.

13-6: Cloud Forensics

Use the Internet to research cloud forensics.

- What can a cloud provider customer do when they are alerted to a cloud security breach?
- What are the responsibilities of the cloud provider when this occurs?
- What are the responsibilities of the customer?
- How can customers insulate themselves from damages?
- If you were a cloud customer, what would you require of the cloud provider?

Write a one-page paper on your research.

13-7: North Ridge Security

North Ridge security provides security consulting and assurance services. You have recently been hired as an intern to assist them.

Impact Industries is a new client of North Ridge and wants an update on forensics investigations. You have been asked to make a presentation to them.

- Create a PowerPoint presentation for Impact Industries about forensics, including the procedures for conducting an investigation and the tools that can be used. Your presentation should contain at least 10 slides.
- After the presentation, Impact Industries has asked about how a forensic examination would be performed on the data stored by their cloud provider. Use the Internet to research cloud forensics and then create a memo about your findings and recommendations.

Module 14: Assignment

14-1: Business Impact Analysis

Using your school or organization, develop a brief business impact analysis.

- What are the impacts?
- What is the mission-essential function?
- What are the critical systems?
- What is the single point of failure?

Use the steps outlined earlier in the module. What did you learn? Modify your plan accordingly.

14-2: Impossible Travel

Impossible Travel detection identifies two user activities originating from geographically distant locations within a time shorter than the user could travel between locations. Research Impossible Travel.

- How does it work?
- How does Impossible Travel learn about a user's normal activities?
- What are the levels that the sensitivity slider allows administrators to configure to define how strict the detection logic is?
- What happens if a user regularly uses two more locations on a regular basis?
- How accurate would you determine Impossible Travel be?
- How could the information gleaned by Impossible Travel pose a threat?

Write a one-page analysis of your research.

14-3: Continuous Data Protection (CDP)

Use the Internet to research continuous data protection (CDP).

- Identify three different solutions and compare their features.
- Create a table of the different features to make a side-by-side comparison.

Which product would you consider the best solution for an enterprise environment? and Why?

14-4: Personal Disaster Recovery Plan

Create a one-page document of a personal disaster recovery procedure for your home computer. Be sure to include what needs to be protected and why.

- Does your DRP show that what you are doing to protect your assets is sufficient?

- Should any changes be made?

14-5: RAID Level 6 Costs

Use the Internet to research the costs of adding RAID Level 6 to a computer, which is generally recognized as the best general RAID level.

- Create a chart that lists the features, costs, and operating systems supported for this level.

Would you purchase this for your computer? Why or why not?

Module 15: Assignment

15-1: Multiparty Risks Until

Recently, multiparty risks have not been considered as serious. Use the Internet to research multiparty risks.

- Why is there now heightened emphasis on multiparty risks?
- What are three examples of security incidents that were the result of a vulnerability in one organization affecting multiple other organizations?
- What were the outcomes of each of these?
- Should an organization that allows other organizations to be compromised through a multiparty risk be held liable?
- What should be the penalty?
- How can these be mitigated?

Write a one-page paper on your findings.

15-2: Intellectual Property (IP) theft

Use the Internet to find details on four recent incidents of intellectual property (IP) theft from an organization.

- What was stolen?
- What vulnerability did the threat actors exploit?
- How valuable was the IP?
- What did the threat actors do with it?
- What loss did it create for the organization?
- How could it have been prevented?

Write a one-page paper on your findings.

15-3: Unconscious Biases in cybersecurity

How could unconscious biases impact cybersecurity?

- Review the information in Table 15-4 page 457 from the textbook and select four of the biases.
- Then create a practical example of how each bias or effect could impact cybersecurity.
- Now return to the table and list in order what you consider your own biases from most prevalent to least.

What can be done to minimize the impact of these biases?

15-4: Reacting to Risks

Using the six reactions to risks in this module, identify a specific risk that you would place in each category. This risk should be something that involves you by identifying intentional actions, accidents, etc. Evaluate your reaction to these risks.

- Could these play a part in how you might evaluate cybersecurity risks in an organization?
- How could they be addressed?

Write a one-page paper on your analysis.

15-5: User Awareness and Training

What user security awareness and training is available at your school or place of business?

- How frequently is it performed?
- Is it available online or in-person?
- Is it required?
- Are the topics up to date?
- On a scale of 1–10, how would you rate the training?
- How could it be improved?

Write a one-page summary.

15-6: Privacy Notices

Identify four different privacy notices and read them.

- What information do they contain?
- How easy are they to understand?
- Who are they intended to protect, the user or the organization?
- Now assign a letter grade (A–F) for each notice. Finally, using these as a basis, write your own privacy notice that you consider being thorough and fair.
- How does it differ from those that you have found? Why?

Write a one-page summary.