**Project 1: Information Systems and Identity Management**

Start Here:

Daily life requires us to have access to a lot of information, and information systems help us access that information. Desktop computers, laptops, and mobile devices keep us connected to the information we need through processes that work via hardware and software components. Information systems infrastructure makes this possible. However, our easy access to communication and information also creates security and privacy risks. Laws, regulations, policies, and guidelines exist to protect information and information owners. Cybersecurity ensures the confidentiality, integrity, and availability of the information. Identity management is a fundamental practice. Part of identity management is the governance of access, authorization, and authentication of users to information systems, Identity management is one part of a layered security defense strategy within the information systems infrastructure. Your work in this project will enable you to produce a technical report and nontechnical presentation that addresses these requirements.

There are five steps that will help you create your final deliverables. The deliverables for this project are as follows:

Nontechnical presentation: This is an 8-10 slide PowerPoint presentation for business executives and board members.

Technical report: Your report should be a 6-7 page double-spaced Word document with citations in APA format. The page count does not include figures, diagrams, tables or citations.

Executive summary: This should be a 2-3 page double-spaced Word document.

In a Word document, share your lab experience and provide screen prints to demonstrate that you performed the lab.

When you submit your project, your work will be evaluated using the competencies listed below. You can use the list below to self-check your work before submission.

1.1: Organize document or presentation clearly in a manner that promotes understanding and meets the requirements of the assignment.

2.3: Evaluate the information in a logical and organized manner to determine its value and relevance to the problem.

6.2: Creating a roadmap for organizations to use in development of an Identity Access Management program (to address gaps in their current offerings).

Step 1: Defining the Information System Infrastructure

Select a hospital or healthcare organization to research. You may choose an organization you are familiar with or can readily obtain information about. To maintain confidentiality, you do not need to mention the name of the organization. You may also choose a hypothetical/fictitious healthcare organization.

Others have researched several healthcare organizations, which have suffered major security breaches, extensively.

1. Describe the organization and structure including the different business units and their functions. You may use an organizational chart to provide this information.
2. Choose one or more mission-critical systems of the healthcare organization. Define the information protection needs for the organization's mission-critical protected health information (PHI). This information is stored in database medical records for doctors, nurses, and insurance claims billing systems, which are used to fulfill the organizational information needs.
3. Define the workflows and processes for the high-level information systems that you have just identified that will store PHI. Workflows and processes for healthcare organizations define how the organization gets its work done. They describe the movement of patient information to the business units that have needs to process and manage that information, from billing to physician care. All these organizations have hardware and software implementations of their information systems, and it is critical to understand these components, and how they are connected (known as their topology), so the appropriate protections can be applied. Your research may produce instances and examples of how an information system is connected, to include cybersecurity components like firewalls, in the information system and network diagram. Be sure you understand the benefits and weaknesses for the different network topologies.

You may incorporate what you find in your research, in your definition for workflows and processes for the high-level information systems and provide explanation of how that topology fulfills the mission for the health care organization. Your definition should include a high-level description of information systems hardware and software components and their interactions. Take time to read the following resources. They will help you construct your definition.
	* Information systems hardware
	* Information systems software

You may supply this information as a diagram with inputs, outputs, and technologies identified. Consider how you might restrict access and protect billing and PHI information.

1. The links shown below provide access to essential information you’ll need to complete this part of the hospital’s information system infrastructure definition. Click each link, review its resources, and refer to them as you compose this part of the definition.
	* Open Systems Interconnections (OSI) Model
	* TCP/IP protocols
	* network protocols

You will include these definitions in your report.

Step 2: Threats

Now that you have defined the hospital's information system infrastructure, you will have to understand what are the threats to those systems and describe the types of measures that could address those threats. In this section, you will learn about different types of identity access management solutions and how they protect against the threat of unauthorized access.

To complete this section of the report, you’ll brush up on your knowledge of threats by reading the following resources: web security issues, insider threats, intrusion motives/hacker psychology, and CIA triad. Take what you learned from these resources to convey the threats to the hospital's information systems infrastructure. Include a brief summary of insider threats, intrusion motives, and hacker psychology in your report as it relates to your hospital data processing systems. Relate these threats to the vulnerabilities in the CIA triad.

This section of your report will also include a description of the purpose and components of an identity management system to include authentication, authorization, and access control.  Include a discussion of possible use of laptop devices by doctors who visit their patients at the hospital, and need access to hospital PHI data. Review the content of the following resources.  As you’re reading, take any notes you think will help you develop your description.

1. Authorization
2. Access control
3. Passwords
4. Multi-factor authentication

Next, expand upon your description.  Define the types of access control management to include access control lists in operating systems, role-based access controls, files, and database access controls. Define types of authorization and authentication and the use of passwords, password management, and password protection in an identity management system. Describe common factor authentication mechanisms to include multi-factor authentication.

You will include this information in your report.

Step 3: Password Cracking Tools

You have successfully examined the threats to a healthcare organization's information systems infrastructure. Now, you must begin your research into password cracking software. Do some quick independent research on password cracking as it applies to your organization.

You can click on this link to find the instructions for [Navigating the Workspace and the Lab Setup](https://umuc.equella.ecollege.com/file/86d36d98-d23a-4001-ac03-91ab25dd1b47/1/UMUCDigitalLabsRev2.pdf).

Enter [Workspace](http://virtualdesktop.umuc.edu/) and complete the lab activities outlined in the Project 1 Workspace Exercise Instructions. There are additional password cracking tool resources, tutorials, and user guides to continue your familiarity with the tools.

Click here to access the [Project 1 Workspace Exercise Instructions.](https://umuc.equella.ecollege.com/file/f634286e-5b85-4e39-a6b5-b785a36ec2cc/4/CYB610Project1Lab.pdf)

After completing the lab, you will have successfully tested more than one password cracking tool. Not all password cracking tools will necessarily perform with the same speed, precision, and results, making it important to test a few different products. Compare the password cracking tools based on these characteristics, and include as part of your assessment and recommendations on the use of such tools. You will test the organization's systems for password strength and complexity and complete validation testing. You will compare the results obtained from your first and second tool.
You have tested and made comparisons of the performance of various password cracking tools and you have the data to support your recommendations for the use of such tools.
Not all password cracking tools will necessarily perform with the same speed, precision, and results, making it important to test a few different products. The comparison will be part of your assessment and help you make recommendations on the use of such tools. You will test the organization's systems for password strength and complexity and complete validation testing. You will compare the results comparing the various tools.

1. Read this article about cyberattacks, perform two different types of cyberattacks in the first, and in the second tool, crack user account passwords. Describe them in simple nontechnical terms for the leadership. You can identify which tool is the most effective and why for your organization's IT environment
2. Compare and contrast the results from the two methods used to crack the accounts for the three passwords (each encrypted by the two hash algorithms). Show their benefits. You can make certain conclusions that help your company's cybersecurity posture after using these methods.
3. Explain to the director of IT and the members of the board that the healthcare organization’s anti-virus software will detect password cracking tools as malware. Also explain how this impacts the effectiveness of testing security controls like password strength. Help the leadership understand the risks and benefits of using password cracking tools, through persuasive arguments in your report and presentation. If any of the tools take longer than 4-5 minutes to guess a password, record the estimated length of time the tool anticipates to guess it.

Include this information in your presentation.

Step 4: The Non-Technical Presentation

You now have the information you need to prepare your product for stakeholders. Based on the research and work you've completed in Workspace, you will develop two items: a technical report for the director of IT, and a nontechnical slide show presentation for the members of the board. You will tailor the language of your reports appropriately to the different audiences.

**The nontechnical presentation:** Your upper-level management team consists of technical and nontechnical leadership, and they are interested in the bottom line. You must help these leaders understand the identity management system vulnerabilities you discovered in password cracking and access control. They need to clearly see what actions they must either take or approve. The following are a few questions to consider when creating your presentation:

1. How do you present your technical findings succinctly to a non­technical audience? Your technical report for IT will span many pages; but you will probably be afforded no more than 30 minutes or 8-10 slides for your presentation and the following discussion with leadership.
2. How do you describe the most serious risks factually but without sounding too temperamental? No one likes to hear that their entire network has been hacked, data has been stolen, and the attackers have won. You will need to describe the seriousness of your findings while also assuring upper-level management that these are not uncommon occurrences today.
3. How do your results affect business operations? Make sure you are presenting these very technical password cracking results in business terms upper-level management will understand.
4. What do you propose? Management will not only want to understand what you have discovered; they will want to know what you propose as a solution.

Step 5: The Technical Report and Executive Summary

The technical report and the nontechnical presentation will identify compromises and vulnerabilities in the information systems infrastructure of the healthcare organization, and identify risks to the organization's data. You will propose a way to prioritize these risks and include possible remediation actions.

**The technical report:** Provide recommendations for access control and authentication mechanisms to increase the security within the identity management system. Review the mission and organization structure of this healthcare organization. Review the roles within the organization, and recommend the accesses, restrictions, and conditions for each role. Present these in a tabular format as part of your list of recommendations.

Provide a comparison of risk scenarios to include the following:

1. What will happen if the CIO and the leadership do nothing, and decide to accept the risks?
2. Are there possible ways the CIO can transfer the risks?
3. Are there possible ways to mitigate the risks?
4. Are there possible ways to eliminate the risks?
5. What are the projected costs to address these risks?

Provide an overall recommendation, with technical details to the director of IT.

**The executive summary:** In addition to your technical report, also create a nontechnical report as an executive summary.

The deliverables for this project are as follows:

1. Nontechnical presentation: This is a 8-10 slide PowerPoint presentation for business executives and board members.
2. Technical report: Your report should be a 6-7 page double-spaced Word document with citations in APA format. The page count does not include figures, diagrams, tables or citations.
3. Executive summary: This should be a 2-3 page double-spaced Word document.
4. In a Word document, share your lab experience and provide screen prints to demonstrate that you performed the lab.

Submit your deliverables to the assignment folder.

Before you submit your assignment, review the competencies below, which your instructor will use to evaluate your work. A good practice would be to use each competency as a self-check to confirm you have incorporated all of them in your work.

* 1.1: Organize document or presentation clearly in a manner that promotes understanding and meets the requirements of the assignment.
* 2.3: Evaluate the information in a logical and organized manner to determine its value and relevance to the problem.
* 6.2: Creating a roadmap for organizations to use in development of an Identity Access Management program (to address gaps in their current offerings).