Businesses involved in mergers and acquisitions must exercise due diligence in ensuring that the technology environment of the future organization is robust and adequately protects their information assets and intellectual property.. Such an effort requires time and open sharing to understand the physical locations, computing environment, and any gaps to address. Lack of information sharing can lead to a problematic systems integration and hamper the building of a cohesive enterprise security posture for the merged organization.

Often the urgency of companies undergoing a merger and acquisition (M&A) impedes comprehensive due diligence, especially in cybersecurity. This creates greater challenges for the cybersecurity engineering architect, who typically leads the cybersecurity assessment effort and creates the roadmap for the new enterprise security solution for the future organization. However, the business interest and urgency in completing the merger can also represent an opportunity for CISOs to leverage additional resources and executive attention on strategic security matters.

In this project, you will create a report on system security issues during an M&A. The details of your report, which will also include an executive briefing and summary, can be found in the final step of the project.

**Step 1: Conduct a Policy Gap Analysis**

As you begin Step 1 of your system security report on cybersecurity for mergers and acquisitions, keep in mind that the networks of companies going through an M&A can be subject to cyberattack. As you work through this step and the others, keep these questions in mind:

* Are companies going through an M&A prone to more attacks or more focused attacks?
* If so, what is the appropriate course of action?
* Should the M&A activities be kept confidential?

Now, look at the existing security policies in regard to the acquisition of the media streaming company. You have to explain to the executives that before any systems are integrated, their security policies will need to be reviewed.

Conduct a policy gap analysis to ensure the target company's security policies follow relevant industry standards as well as local, state, and national laws and regulations. In other words, you need to make sure the new company will not inherit any statutory or regulatory noncompliance from either of the two original companies.  This step would also identify what, if any, laws and regulations the target company is subject to. If those are different from the laws and regulations the acquiring company is subject to, then this document should answer the following questions:

* How would you identify the differences?
* How would you learn about the relevant laws and regulations?
* How would you ensure compliance with those laws and regulations?

The streaming company that is being acquired has a current customer base of 150,000 users, who on average pay $14.99 in monthly fees. Based on the overall income, use PCI Standards DSS 12 requirements, and the PCI DSS Quick Reference Guide to identify a secure strategy, and operating system protections to protect the credit card data.

Select at least two appropriate requirements from the PCI Standards DSS 12 set of requirements and explain how the controls should be implemented, how they will change the current network, and any costs associated with implementing the change.

In the next step, you will review the streaming protocols that the companies are using.

**Step 2: Review Protocols for Streaming Services**

After reviewing the policies from the company and the policy gap analysis, the M&A leader asks you about the protocols used by the streaming company. He wants to know if the protocols used would affect the current state of cybersecurity within the current company environment. For this section, review the protocols, explain how they work along with any known vulnerabilities, and how to secure the company from cyberattacks. Start with researching the commonly known streaming protocols and the vulnerabilities of those protocols. Some examples are the Real-Time Streaming Protocol (RTSP), Real-Time Transport Protocol (RTP) and the Real-Time Transport Control Protocol (RTCP).

Additionally, the leadership wants to know if any vulnerabilities identified would or could lead to a no-go on the M&A.

In other words:

1. You need to identify what streaming the companies are doing and the specific technology they are leveraging.
2. What are the technical vulnerabilities associated with the protocols involved?
3. Have those been mitigated? And to what extent (i.e., has the risk been reduced to zero, reduced somewhat, shifted to a third party, etc.)?
4. What residual risk to the target company's assets and IP remain?
5. Would those risks extend to the current (takeover) company after the merger?
a. Would that be bad enough to cancel the M&A?
6. If the response to #5 is yes, then, what should the target company do to further mitigate the risk? How should the takeover company mitigate the risk?
7. What are the costs associated to the target company (implementing the appropriate mitigation)? If the takeover firm has to take additional measures, identify those costs as well.

After assessing and reviewing the streaming protocols, move to the next step, where you will assess the infrastructure of the merged network.

**Step 3: Assess the Merged Network Infrastructure**

You’ve just reviewed the streaming services of the companies, and now you will assess the infrastructure of the new network. The networks of the two companies could be configured differently, or they could use the same hardware and software, or completely different hardware and software.

The purpose of this section is to understand what tools the company is using, the benefits and shortcomings of those tools, and the gaps within the network. Explain what tactics, techniques, and procedures you would use to understand the network. You should identify firewalls, DMZ(s), other network systems, and the status of those devices.

When your assessment of the infrastructure is complete, move to the next step, where you will assess any existing policies for wireless and bring your own device (BYOD) within the companies.

**Step 4: Review the Wireless and BYOD Policies**

Within Project 2, you learned about and discussed wireless networks. An M&A provides an opportunity for both companies to review their wireless networks. Within your report, explain the media company's current stance on wireless devices and BYOD. However, the company that is being acquired does not have a BYOD policy. Explain to the managers of the acquisition what needs to be done for the new company to meet the goals of the BYOD policy.

When the review of the wireless and BYOD policies is complete, move to the next step: developing a data protection plan.

**Step 5: Develop a Data Protection Plan**

You’ve completed the review of the wireless and BYOD policies. In this step, you will develop the recommendations portion of your report in which you will suggest additional mechanisms for data protection at different levels of the acquired company’s architecture.

Include the benefits, implementation activities required for protection and defense measures such as full disk encryption, BitLocker, and platform identity keys. You also want to convey to your leadership the importance of system integrity and an overall trusted computing base, environment, and support. Describe what this would entail and include Trusted Platform Module (TPM) components and drivers. How are these mechanisms employed in an authentication and authorization system? Include this in the report and whether the merging company has this.

In the next step, you will assess any risks with the supply chain of the acquired company.

**Step 6: Review Supply Chain Risk**

The data protection plan is ready. In this step, you will take a look at risks to the supply chain. Acquiring a new company also means inheriting the risks associated with its supply chain and those firm's systems and technologies. Include supply chain risks and list the security measures in place to mitigate those risks. Use the [NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations](https://umuc.equella.ecollege.com/file/86d36d98-d23a-4001-ac03-91ab25dd1b47/1/NISTSpecialPublication800-161SupplyChainRiskManagementPractices%20%282%29.pdf) to explain the areas that need to be addressed.

After your supply chain review is complete, move to the next step, where you will create a vulnerability management program.

**Step 7: Build a Vulnerability Management Program**

After your supply chain review, you conduct an interview with the company's current cybersecurity team about vulnerability management. The team members explain to you that they never scanned or had the time to build a vulnerability management program. So, you need to build one. Use [NIST Special Publication 800-40 Guide to Enterprise Patch Management Technologies](https://umuc.equella.ecollege.com/file/86d36d98-d23a-4001-ac03-91ab25dd1b47/1/GuidetoEnterprisePatchManagementTechnologies.pdf) to develop a program to meet the missing need.

Explain to the managers how to implement this change, why it is needed, and any costs involved.

The next step is a key one that should not be overlooked -- the need to educate users from both companies of the changes being made.

**Step 8: Educate Users**

You’ve completed your vulnerability management program, but it’s important to educate all the users of the network about the changes. During the process of acquiring a company, policies, processes, and other aspects are often updated. The last step in the process is to inform the users for the new and old company of the changes. Within your report, explain to the acquisition managers the requirements for training the workforce.

When you’ve completed this step, move to the final section of this project, in which you will prepare and submit your final report.

**Step 9: Prepare and Submit Your Report, Executive Briefing, and Executive Summary**

You’re ready now for the final step, in which you will compile and deliver the Cybersecurity for a Successful Acquisition report for the company leaders to enable them to understand the required cybersecurity strategy.

Again, keep in mind that companies undergoing an acquisition or merger are more prone to cyberattacks. The purpose of this paper is to analyze the security posture of both companies and to develop a plan to reduce the possibility of an attack.

The assignments for this project are as follows:

1. Executive briefing: This is a three- to five-slide visual presentation for business executives and board members.
2. Executive summary: This is a one-page summary at the beginning of your report.
3. Cybersecurity System Security Report for Successful Acquisition: Your report should be a minimum 12-page double-spaced Word document with citations in APA format. The page count does not include figures, diagrams, tables or citations.

Submit all three components to the assignment folder.

Deliverables: Cybersecurity for a Successful Acquisition, Slides to Support Executive Briefing

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 in a manner that promotes understanding and meets the requirements of the assignment.
* 1.2: Develop coherent paragraphs or points to be internally unified and function as part of the whole document or presentation.
* 1.3: Provide sufficient, correctly cited support that substantiates the writer’s ideas.
* 1.4: Tailor communications to the audience.
* 1.5: Use sentence structure appropriate to the task, message and audience.
* 1.6: Follow conventions of Standard Written English.
* 1.7: Create neat and professional looking documents appropriate for the project.
* 1.8: Create clear oral messages.
* 2.1: Identify and clearly explain the issue, question, or problem under critical consideration.
* 2.2: Locate and access sufficient information to investigate the issue or problem.
* 2.3: Evaluate the information in a logical and organized manner to determine its value and relevance to the problem.
* 2.4: Consider and analyze information in context to the issue or problem.
* 2.5: Develop well-reasoned ideas, conclusions or decisions, checking them against relevant criteria and benchmarks.
* 5.9: Manages and administers integrated methods, enabling the organization to identify, capture, catalog, classify, retrieve, and share intellectual capital and information content.
* 7.3: Knowledge of methods and tools used for risk management and mitigation of risk.
* 8.7: Provide theoretical basis and practical assistance for all aspects of digital investigation and the use of computer evidence in forensics and law enforcement.