



STUDENT: PHYSICAL SECURITY

Document Version: **2018-10-01**



Copyright © 2018

This material is based upon work supported by the National Science Foundation under DUE #1501990. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

This work is licensed under the Creative Commons Attribution 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/>.

Contents

Overview	2
Objective: Recommending Physical Security Measures for a Student Data Center	2
Supplemental Materials.....	2
Website Links	2
Project Scenario	2
1 Review Layers for Physical Security	3
2 Research and Document Physical Security Recommendation	3
2.1 Technology needed	3
3 Presentation of Physical Security Recommendations	3
Conclusion.....	3

Overview

This project includes the following tasks:

1. Review the basic layers of physical security and how they interact. Your team will be assigned to focus your work on addressing **one** of the layers for this activity.
2. Research, discuss with others, and document recommendations for physical security of the layer assigned to your team.
3. Recommend physical security measures that consider accommodating and protecting the following types of access to your data center:
 - Local
 - Wireless (on campus)
 - Remote (off campus)

Objective: Recommending Physical Security Measures for a Student Data Center

In this project, you will work as a team to

1. Research the known physical vulnerabilities for a data center, and discuss with your team possible solutions.
2. Develop a detailed plan to address the physical vulnerabilities for the layer assigned to your team.
3. Present your team's recommendations to the instructor and other "administrators."
4. Respond with suggested fixes to potential deficiencies in your plan pointed out to you by your "administrators."

Supplemental Materials

Website Links

- a. [The Four Necessary Basic Layers Required for Proper Physical Security](#)
- b. [Physical Security and Why It Is Important](#) (PDF, copy and paste URL into browser)
- c. [Best Practices for Designing Your Physical Security Infrastructure System](#)
- d. [Protecting Your System: Physical Security](#)
- e. [Data Center Physical Security Checklist](#) (PDF, copy and paste URL into browser)

Project Scenario

STATE University is a public four-year university offering a full array of graduate and undergraduate programs, including information technology (IT), information security (INFOSEC), and information assurance (IA). Students built and maintain a classroom network that supports coursework and prepares students for security-based competitions. The classroom network has been active for two years and is contained within the classroom, where there have been minor incidents of sabotage and component theft. The department gave the students permission to expand the scope of the classroom network to a **student data center**, to help expand student knowledge and skills *outside the classroom*. However, with the expansion, which includes multiple levels of remote access, the administration asked for recommendations that will address the **physical security** for your student-run data center, taking into consideration the past incidents that have occurred.

If successful, the university hopes to expand this data center to include the growing number of students participating in security competitions—perhaps expanding to a campus-wide availability. Before taking this step, though, your team must develop and present your recommendations to provide adequate physical security for the network (layer assigned to you). Your recommended network architecture should include technologies to provide 1) secure local access, 2) secure wireless access on campus, and 3) secure access from off campus. These additional access modes must maintain the privacy of users as well as the security of the data center.

1 Review and Research Layers for Physical Security

1. As a team, use the provided resources to better understand your assigned layer of physical security.
2. As a team, create a list of related aspects of physical security for your assigned layer of the expanded data center. Use the provided resources as a guide.
3. Specifically address the incidents identified in the scenario that resulted from having the student network in an unsecure classroom location.

2 Document Your Physical Security Recommendations

1. Your team's recommendation should address secure access for:
 - a. Local users
 - b. Remote (wireless) users on campus
 - c. Off-campus users

2.1 Technology needed

1. As a team, research any tools or components required to implement your team's physical security solutions.
2. Identify the recommendations that may require additional funding.

3 Presentation of Physical Security Recommendations

Put together a 15-minute professional presentation of the team's recommendations, using modern presentation tools. Every member of the team must contribute in some way to the delivery of the presentation, such as presenting his or her main contribution to the overall plan.

Conclusion

As networked resources become increasingly valuable to the stakeholders of an organization, there is increased pressure to allow greater access to these resources. This includes remote and local access, wireless access, and remote access to individuals. This increased access must be balanced by the security needs of the organization. The goal is to provide the additional access required in a secure fashion that does not comprise the overall security posture of the organization. This project explored how to research, identify, and evaluate physical security solutions for a student data center in ways that would be typical in workplace environments.