MALIK AND SEEME HASAN SCHOOL OF BUSINESS

2200 BONFORTE BLVD.
PUEBLO, COLORADO 81001-4901
(719) 549-2142 Fax: (719) 549-2909

Academic Program Assessment Report for AY 2020-2021 **Program:** Computer Information Systems: Cyber Security Program-Level Learning Outcomes

Date Report completed: May 5, 2021
Completed By: Dr.Roberto J. Mejias, Ph.D.

Statement of Program Mission and Goals:

The Cyber Security Program under the Center for Cyber Security Education, Research (CCSER) shall have as part of its mission the following GOALS:

- To reduce vulnerability in our national information infrastructure by promoting higher education and research in the areas of Cyber Security, Information Assurance and Cyber Defense.
- To produce a growing number of students and professionals with expertise in Cyber Security, Information Assurance and Cyber Defense that will contribute significantly to the advancement of state-of-the-art knowledge and practice in these respective areas.
- To provide collaboration and outreach opportunities among students, faculty, professionals and public and private institutions committed to excellence in the areas of Cyber Security, Information Assurance and Cyber Defense.
- To foster and continuously improve scholarship, professional development, education, research and outreach in the areas of Cyber Security, Information Assurance and Cyber Defense.
- To promote the awareness, understanding, integration and adoption of Cyber Security, Information Assurance and Cyber Defense education, research and related in all relevant departments, centers and organizations at Colorado State University-Pueblo.

Cyber Security Program of Study, Program-Level Learning Outcomes (PLOs)

After successfully completing the Cyber Security Program of Study, students will possess the following skills:

1. Demonstrate the ability to understand and recognize the nature and range of Cyber Threats, Exploits, Attacks.
2. Demonstrate appropriate analysis and application of Cyber Defense (CD) tools and methodologies to address and defend organizations and Information Systems (I.S.) from cyber attacks.
3. Understand the best application of Info Security Models, Cyber Sec Planning and Policies to analyze, and integrate appropriate cyber security methodologies into viable solutions.
4. As a team project member, the ability to develop and communicate Threat-Vulnerability-Asset (TVA) grids and IT solutions for cyber attack and vulnerability risk analysis.
5. Demonstrate the ability to develop Disaster Recovery, Business Continuity and Risk Mitigation Strategies and solutions within financial, ethical and cyber Law boundaries.

Created by CCSER Sept 2020, Revised April, 2021, Revised May, 2021

I. Program-Level Learning Outcomes (PLOs) Indicators, Metrics Assessed for Academic Year (2020-2021)

Program-Level Learning Outcome #1: Demonstrate the ability to understand and recognize the nature and range of Cyber Threats, Exploits, Attacks

Related PLO Assessment Indicator	Course That Formally Assess This PLO	When Was This PLO Last Assessed?	Methods, Metrics, Rubrics Used To Assess Indicator? (Include Copies of Methods)	Results of the PLO Assessment Indicator	Average Performance Score for this PLO Assessm't	Recommended Changes for Improvement	Next Period When PLO Will Be Assessed
Correct identification of type and effect of range of cyber threats	CIS 460 (Cyber Security,Defense)	May, 2021	In-Class, Team exercises, specific Quiz, Exam Questions	Although CIS students (Juniors, Seniors) have a good technical foundation in Networking, Database, Win, Linux, Operating systems, and various programming courses, there appears to a consistent low level understanding of the changing cyber threatscape and its effects on many levels of an I.S. Some students simply do not read the required chapter assignments, and forgot to submit their lab assignments. Many students expected to submit a missed in-class several weeks later for full credit. Now requesting all lab assignments submitted by NEXT day	78%	*Course deliverables need to be repeated throughout the course. *More additional required outside reading assignment followed up with class discussion of assigned cyber security readings *More in-class demos. illustration, before in-class labs are conducted * Divide Labs into 2 Parts Part 1 (in-class labs) to allow for "peer-mentoring" with fellow students, Part 2 (take home-class labs) to develop individual knowledge and skills	Spring, 2022

Correctly identifying specific types of Cryptos, Stegos, Password (PW) hashes Network (NW) and Web attacks.	CIS 460 (Cyber Security,Defense)	May, 2021	CIS 460-graded Individual in-class Kali Linux labs and take home labs to identify a range of Cryptos (Hex, Base64, etc.), Stegos, PW (Password) hashes (salted, NTLM PW), Network (NW) range of NW web exploits Quizzes and Exams on specific subject matter (SM) cited above	CIS 460: The graded Individual in-class and take home labs are at expectation levels but could be a bit higher. Although students have taken Windows, Linux O/S required courses, Kali-*Linux* has a specific suite of vulnerability analysis, penetration testing and security auditing tools, often not experienced by some students. Many students were not familiar with basic Kali-Linux terminal commands. Proficiency in Kali-Linux terminal commands is critical in conducting vulnerability tests such as PW cracking, ID of Crypto hashes, NW scanning and web exploitation and students took up a lot of semester time to develop basic proficiency	77%	* More intro Labs on the Linux environment and terminal commands, * More graded Individual in-class, take home labs (this will increase grade performance in subject, matter quizzes and Exams) * Will provide specific in-class examples of Kali-Linux commands as related to assigned Lab assignments	Spring, 2022
Correctly identifying potential cyber security threats in Network Architectures	CIS 461 (IT Security Risk Mgmt)	May 2021	CIS 461- Graded In-class team-based labs to design, construct NW Architectures to ID cyber vulnerabilities	CIS 461: In-class labs to construct NW Architectures and Infrastructures were first introduced as a step-by-step in class lab. Drawing NW Architectures are then assigned as individual homework (HW) and then	78%	Understanding NW Architectures and Infrastructures is key in revealing potential NW cyber attacks vulnerabilities. Will implement: * More graded Individual construction	Spring, 2022

			-Related subject matter (SM) on Quizzes,Exams	as an in-class, team NW Architecture exercise. Individual team members still submitted NW Architectures labs that were not well designed against NW cyber attacks. While students have had course material to identify a range of Cyber threats, including specific NW Client and Server attacks, DoS attacks and Web attacks, there was a lack of correctly identifying potential cyber threats, vulnerabilities associated with specific NW architectures. This lack of correctly identifying potential cyber threats in NW Architectures was demonstrated in Quiz and exam results		of NW Architectures. * This will assure that each team member is proficient in constructing NW Architectures using MS-Visio, "draw.io" applications * More team-based exercises of NW Architecture with embedded cyber threats will be developed to help develop individual proficiency.	

Program-Level Learning Outcome #2: Demonstrate appropriate analysis, application of CD (Cyber Defense) tools, methodologies to address and defend Info Systems from cyber attacks

Related PLO Assessment Indicator	Course That Can Formally Assess This PLO	When Was This PLO Last Assessed?	Methods, Metrics, Rubrics Used To Assess Indicator? (Include Copies of Methods)	Results of the PLO Assessment Indicator	Average Performance Score for this PLO Assessm't	Recommended Changes for Improvement	Next Period When PLO Will Be Assessed
Clear understanding of capabilities of a range of NW cyber defense (CD) tools	CIS 461 (IT Security Risk Mgmt)	May, 2021	CIS 460-Quizzes, exams questions on related subject matter lectures, and videos, to increase their understanding of range of NW cyber defense (CD) tools and their relative, capabilities	Once students identified specific types of cyber attacks and their relative effects, it was challenging for students to correctly understand which I.T. and cyber defense (CD) tools should be used. Many students found understanding the wide range of CD tools and their relative capabilities overwhelming... as many students had still not mastered the identification of different *categories* of cyber threats (e.g., Malware vs. Network, Server attacks, vs. Database breaches vs. Web attacks, etc.).	75%	Additional in-class Lecture material, related videos will * provide a range of illustrations to better assist students in understanding different categories of CD tools, safeguards, * Specific lectures on Cyber Sec via NW devices, Security via Hardware and Security (via Software), * Additional labs using 1-2 CD safeguards from each CD categories will increase better understanding of relative capabilities of different CD safeguards	Spring, 2022
Correct and specific application of range of CD tools, methods to address, specific cyber attack type	CIS 460 (Cyber Security,Defense)	May, 2021	Graded in-class and take home labs on correct application of a range of tools for PW cracking, Crypto ID, PW	Becoming proficient in *understanding* how specific *capabilities* of a various of I.T. and CD safeguards would address specific cyber attack types was challenging	74%	To better help students match the best/ most effective I.T., CD safeguards, to address a specific cyber attack types: * more in class	Spring, 2022

			hash ID, web exploitation, scanning, cyber threats challenges Quizzes, Exams on related labs on correct application of best CD tools to identify types of Cryptos, Stego, Password (PW) hash types for NW and Web exploits, attacks using specific Kali Linux tools. Used the following Kali tools: (John the Ripper, nmap, Ophrack,Hashcat, Dirbuster, Burpsuite, etc.)	Student struggled to *first* correctly identify various cyber attack types and then correctly *match* that cyber attack type with the most appropriate cyber security tool /safeguard. This mismatch indicates a need for better understanding the many aspects of a particular cyber security attacks and attack vectors before prescribing the best CD safeguards		examples, and team labs to explore the range of I.T., CD safeguards * individual labs will be designed to better match the more effective CD safeguards, with a range of cyber attack types	
Correct placement of Network devices as I.T. safeguards in a NW Architecture	CIS 461 (IT Security Risk Mgmt)	May, 2021	CIS 461-graded Individual, Team-based labs, relating to best placement of CD devices (*Proxies, Firewalls,Routers IDS, IPS, Honeypots*), to address variety of NW threats in NW Architectures, Infrastructures	Students found it challenging to be proficient in the best placement of *Network devices* (*Routers*, *Switches*, *Proxies, Load Balances, DMZs*) as CD safeguards to address NW threats due to poorly designed, vulnerable NW Architectures. Students often confused	77%	Additional Lectures, videos, in-class labs on * the best application of NW devices in Architectures for NW security Infrastructures * vs NW devices placed to improve performance *Team exercises to enhance I.S. security via DMZs and restricted system access	Spring, 2022

			to reduce cyber vulnerabilities	recommending NW devices for Architectures that improved NW *performance* but did not increase NW *cyber security*. Students often did not perceive a clear conceptual difference between NW performance and NW security. Long Answer exam questions clearly demonstrated this shortcoming to understanding this difference between devices to enhance NW cyber security vs. NW performance			
Correct application of NW tools to address and defend from cyber threats	CIS 289 (Networking Concepts)	Fall, 2020	Individual Graded Quizzes, Exams, in-class and take home labs (at least 12) on challenges in Wireshark, *aircrack-ng* tool, related quiz, exam questions,	Proficiency in Network Assessment tools such as Wireshark, nmap and other Kali Linux utilities to sniff packets, scan ports is critical to ID and address potential cyber threats. After several in-class Wireshark labs, student developed proficiency with *individual* take-home labs across a variety of *pcap* files depicting potential cyber threats. Kali Linux Network analysis tools such as nmap and aircrack-ng required more in-class	84%	* More Wireshark and Kali "aircrack-ng" in-class labs to demo the range of capabilities * More demos on the use of the Wireshark Statistics and Analysis utilities * More instructional guides on the wide range of Kali *nmap* commands for various network scanning and network information discovery	Fall, 2021

				demos and exercises. However students showed great interest in developing these NW analysis tools to identify potential cyber threats			

Program-Level Learning Outcomes #4: As team project members, the ability to develop and communicate Threat-Vulnerability-Asset (TVA) grids, and IT solutions for cyber attack and vulnerability risk analysis

Related PLO Assessment Indicator	Course That Can Formally Assess This PLO	When Was This PLO Last Assessed?	Methods, Metrics, Rubrics Used To Assess Indicator? (Include Copies of Methods)	Results of the PLO Assessment Indicator	Average Performance Score for this PLO Assessm't	Recommended Changes for Improvement	Next Period When PLO Will Be Assessed
Develop and Integrate all the components of a Threat Vulnerability Asset (TVA) grid	CIS 460 (IT Security Risk Mgmt)	May, 2021	Teams submit graded Project progress Milestones to identify the 3components of the TVA grid and insure team project progress CIS 460 teams have graded TEAM exercises to correctly ID specs for recommended CD safeguards.	From the required submitted TVA project "milestones" (Milestones #1, #2, #3) team members found it challenging to correctly identify their target organization's critical assets, threats and current IT safeguards. The underperformance of even one TVA team member in identifying any of the 3 TVA grid components affected the entire team's correct recommendation for the most appropriate CD, IT safeguards. Individual quiz and exam scores: ID'd Individual under-performance to	78%	The construction of an accurate TVA grid was critical to both CIS 460 TVA field studies, it will be important to: * develop *individual* proficiency to correctly identify the 3 components of TVA grid, * more individual labs using Asset, Threat Matrices to identify critical assets, threats and effectiveness of the current IT safeguards, * more in-class team based labs to build a more accurate team based identification of 3 TVA grid components. * more take home labs working with Asset and	Spring, 2022

				correctly ID an organization's critical assets, threats to those assets and current IT safeguards Individual TVA project team members fell short of in accurate ID of their technical TVA I.T. safeguards resulting in inaccurately estimating the technical vulnerabilities.		Threat Matrices for team members to work together to better integrate and develop a more accurate TVA grid *More time by Instructor assessing team project Milestones	

Summary and Comments on Program Assessment Report for Selected Cyber Security, Program-Level Learning Outcomes (PLOs)

For AY 2020-2021, the following Program-Level Learning Outcomes (PLOs) were assessed:

PLO #1: Demonstrate the ability to understand and recognize the nature and range of Cyber Threats, Exploits, Attacks

PLO #2: Demonstrate appropriate analysis, application of CD (Cyber Defense) tools, methodologies to address and defend Info Systems from cyber attacks

PLO #4: As team project members, the ability to develop and communicate Threat-Vulnerability-Asset (TVA) grids, and IT solutions for cyber attack and vulnerability risk analysis

Assessment Results

PLO #1 - Avg. approx. 77-78%
PLO #2 - Avg. approx. 74- 84%
PLO #4 - Avg. approx. 78%

Future PLO Assessment

1. Assess PLO #1 every academic year
2. Assess PLO #2 every academic year
3. Assess PLO #5 every academic year

Created by CCSER Sept 2020, Revised April, 2021, Revised May, 2021

Cyber Security Program PLOs x Curriculum Map

Program-Level Learning Outcomes (PLOs)	CIS 315	CIS 350	CIS 289	CIS 271	CIS 401	CIS 460	CIS 461	CIS 462
1. Demonstrate the ability to understand and recognize the nature and range of Cyber Threats, Exploits, Attacks	I	I	I,R			R, A (SPR-2021)	R, A (SPR-2021)	R, A (Fall-2020)
2. Demonstrate appropriate analysis, application of CD (Cyber Defense) tools to address and defend Info Systems from cyber attacks			I, R, A (2020)		R	R, A (SPR-2021)	R, A (SPR-2021)	R, A (Fall-2020)
3. Understand best application of Info Security Models, Cyber Sec Planning and Policies to analyze, integrate appropriate cyber security methodologies into viable solutions	I	I	I	I	R	R	R, A (SPR-2021)	R
4. As team project members, the ability to develop and communicate Threat-Vulnerability-Asset (TVA) grids, and IT solutions for cyber attack and vulnerability risk analysis						I, R,A (SPR-2021)	I, R,A (SPR-2021)	I, R,
5. Demonstrate ability to develop Disaster Recovery, Bus Continuity and Risk Mitigation Strategies and solutions within financial, ethical and cyber Law boundaries					R	I, R	I, R,A (SPR-2021)	I, R

I = Introduced, R= Reinforced, A = formally assessed

Created by CCSER Sept 2020, Revised April, 2021, Revised May, 2021

CIS 460-Cyber Security & Defense

TVA FIELD Project Evaluations

SPRING, 2021

Team No____________ Company Analyzed________________________

Team Members

	ANALYSIS of TVA REQUIREMENTS for TEAM PROJECT PRESENTATION	**EXTRA PTS**	**MAX SCORE**	**TEAM SCORE**
1	**ID of Target Organization**		**////////////**	
2	**Clear ID of Organization Mission**		**3**	
	Mission Statements, Org Charts, Process Charts etc			
3	**Architecture, Infrastructure of Organization**		**5**	
4	**IDENTIFICATION of organization's most critical assets, processes,activitie**		**5**	
	- use of Pironti Metrics **+2**			
	-Used CIS 461 ASSET Ranking Matrix ? **-2**			
4A	**Prelim RANKING TABLE, Criteria for Critical Assets, Processes**		**5**	
	Use of Industry Benchmarks?			
5	**IDENTIFICATION of Potential Cyber Threats, Exploits, Attacks**		**5**	
	Needed column for reasons for ranking			
6	**Generation of ranking TABLE, criteria used to prioritize cyber THREATS cyber exploits, attacks**		**5**	
	Use/ reference to Industry Benchmarks?			
	-Used CIS 461 THREAT Ranking Matrix ? **-1**			

	Good Identification of Existing IT Safeguards				
7	**ID of the resulting vulnerabilities- development of TVA GRID**		**5**		
	2nd Post TVA grid		**5**		
	-No TVA grid = -10 pts !				
8	**Recommendation of new or improved cyber defenses and IT safeguards**		**5**		
	some discussion of recommended safeguards				
9	**Generation of approximate COST ESTIMATES and ROSIs**		**5**		
	Adjusted for "Probabilities" of Attack?				
	Used INDUSTRY Benchmarks for Cost and Attack estimates?				
10	**Lessons learned from TVA Field Project**		**2**		
		0	**50**		of 50

ADDITIONAL CONSIDERATIONS

Guidelines for CIS 460
TEAM “THREAT-VULNERABILITY-ASSET” (TVA) TEAM FIELD PROJECT

SPRING, 2021

Instructor: Dr. Roberto Mejias, Ph.D.

The Threat-Vulnerability-Asset (TVA) analysis project is designed to give you and your project team the opportunity to investigate and analyze your selected organization’s critical assets, the cyber-threats facing those critical assets, the current (if any) IT safeguards in place, and the related cyber vulnerabilities from the triangulation of these three (3) components. Your TVA project team must also recommend appropriate IT safeguards and cyber-defense measures to protect your selected organization's information system (IS) security and their IT resources.

Complete List of Pueblo Licensed Businesses **https://www.pueblo.us/Archive.aspx?AMID=81**

Teams will identify and consult with any local or regional organization, corporation, department or project regarding a TVA analysis of their I.S. operations. Your selected organization may be private, public, governmental or non-profit. The CIS 460 TVA team project requires the completion of the following components (in this order):

1. **Identification** of a real organization / department / project. Your team must gain **consent** from their management regarding the undertaking of a TVA analysis for their organization. ***(An “Intro Letter” will be posted on the course Blackboard (BB) site that your team should take with you.***

Feel free to recommend that your selected organization’s Manager or CIO call me for verification),

2. Clear **Identification** of your selected organization’s **“mission”** (i.e., *what is the purpose, operational goals of that organization*)? Important: Include mission statements, org charts, business process charts, etc. to support this requirement,

3. Provide a Graphic of existing **Network Architecture** *and* **Infrastructure** *(Recommend using MS Visio or "Draw.io" (open source diagramming software)).*

4. **Identification** and **approx ranking** of the organization’s ***most*** **critical assets, processes** and **activities** that support the organization’s mission and core operations,

5. **Identification** of the potential cyber **threats**, **exploits, attacks** that threaten the confidentiality, integrity and availability (C.I.A.) of your organization's most critical assets, processes, activities,

6. **Generation** of a **ranking criteria to prioritize** these identified cyber security threats/exploits/ attacks from *most probably* threat to *least probable* threats,

7. **Identification** and analysis of your organization's *current* **IT safeguards** and **cyber-defenses** designed to protect your organization's critical IT resources and key processes,

Team Threat Vulnerability Asset analysis Project (contin.)

8. **1st TVA Grid**: Identification of the current **vulnerabilities** from the intersection of these 3 components (triangulation) on a TVA grid: most *critical assets*, most probable *cyber-threats* and current *IT safeguards*,

9. **2nd TVA Grid:** Recommendation of new or improved **cyber defenses** and **IT safeguards** (*e.g., more firewalls, AV protection, encryption, IDS, SETA, etc*.) that could prevent or mitigate the cyber-threats and vulnerabilities identified from your TVA grid,

10. Generation of *approximate* **cost estimates** and **ROSIs** *(return on security investments)* for your recommended IT controls and cyber defense devices, designs, hardware, etc.

11. The **Lessons learned** from your team experience with this TVA Field Project.

In a real-life cyber-attack "incident", TVAs are developed immediately after a breach or unauthorized access of data has occurred. Thereafter, an "Incident Report" or "Disaster Recovery" report is usually submitted to IT management within 3-5 days of the security breach or intrusion. Your team will have 9-10 weeks to develop your TVA analysis.

5 TVA Project Milestones (*Must* Include Course #(CIS 460), MS #. Team #, Team Member Names)
The above 11 TVA Field Project requirements will be accomplished via **five (5) TVA Project Milestone progress reports.** Milestones #1 through #4 may be 2-3 pages long detailing the progress of your TVA team project. Milestone #5 is your team's final TVA team's PPT presentation to the class.

Milestone #1: Identification of the **organization** your team selected for your TVA Project. Identify your selected organization's **mission** and its major **core activities** (e.g., *retail sales, customer service, manufacturing, DB support, revenue generating activities*). In other words, why does this company exist and what does this organization "do" as their business model? **(10 pts.)**

Milestone #2: Identification of related **IT architecture** and n**etwork infrastructure** and related information (**include Arch drawings!**). If your selected company does not have an IT architecture, **your team must develop one for them! (10 pts.)**

Milestone #3: ***Part 1***: Identification of **ALL critical assets, processes, technology resources** (e.g., *company's R&D, key employees, secret processes, unique intellectual property (IP), customer database records, unique software, their website, etc*.) that directly support their organizational mission and core activities. Include a copy of your Team's Project Gantt chart using MS Project **(10 pts.).**
Part 2- Identification and PRELIM **ranking** of your **organization's critical assets. (10 pts.)**
(Do not need an Excel ID-Ranking Matrix- Use Best Ranking Estimates)
Note: Be sure to identify and include at least 2-3 technology assets for MS #2. (Note: these assets, processes and resources will not yet be "ranked" at this stage of the TVA project).

Milestone #4: *Part 1*: Identification and **ranking** of the **potential cyber-threats** to these most critical assets, processes.
Part 2: Identification of the **existing IT safeguards** that your organization has in place to mitigate the threats to these critical assets.
(Do not need Excel ID-Ranking Matrix- Use Best Estimate)
Part 3: Generation of a **1st TVA Grid worksheet. (10 pts.)**

Milestone #5: Submission and class presentation of your Team's TVA final analysis with all 12 TVA components described above. Final presentation includes

- final identified vulnerabilities,
- final recommended IT safeguards to reduce potential vulnerabilities.
- final cost estimates and ROIs for your recommended new IT safeguards,
- **Final TVA Grid worksheet** along with "Lessons Learned. **(50 pts.)**

Note; Each Team Milestone must contain, CIS 460 course #, Milestone #, Team # and names of Team member contributing!

Grading of the TVA Team Project:

The team TVA project and related Milestones will constitute significant percentage of your overall course grade as indicated in your course syllabus. Your team will be expected to present a professional, well-prepared and informative presentation that provides interesting TVA insights for our class members and demonstrates a valuable learning experience in Cyber-defense for you as a team.

Confidential Peer Evaluations

All team members will be given a "*Confidential Peer Evaluation***"** sheet to evaluate the relative contribution of each member within your group. **Team members receiving negative peer evaluations will be penalized (-10) TVA project points per negative evaluation. (-5 pts. if not submitted)**

Additional Team Presentation Requirements

1. All TVA Project Milestones must have (as a cover sheet) their **Team Number**, **Team name** (if applicable) and names of all the team members ***for each milestone submitted***. Milestones may be submitted late at 50% credit, but all milestone must be submitted regardless.

2. All team class presentations must use a professional presentation software interface (e.g., MS Power Point. Prezi, etc©). Presentation should be between 20-25 slides maximum, *(Note; No "Final Project Paper" is required).*

3. Presenting teams must prepare **handouts** or electronic copies (in PDF format) of their TVA project presentations for all student members! (***Double check with your organization to permit this dissemination)***

4. **A hard copy and electronic copy of your Team TVA project presentation should be transmitted to Dr. Mejias for posting on BB** *(-5 pts. if electronic copy not submitted).*

5. **Teams shall also provide Dr. Mejias a digital picture of your talented team members (*with names under each person*) for posterity** *(-10 pts if not submitted)*

Good luck CIS 460 students! Get involved and learn from this Threat-Vulnerability-Asset (TVA) analysis Project. This team project will provide valuable analysis, insights, tools, and TVA experience for you and your organization(s) when Info Security breaches occur. And they WILL occur!

However, there is a 25 pt. penalty for not being present (for whatever reason!) at your team's final TVA project presentation*.*