Risk, Threat, and Vulnerability Management Academic Level : Bachelor Paper details Deliverables 10 Page security assessment report (SAR) Transcript Many companies and agencies conduct IT audits to test and assess the rigor of IT security controls in order to mitigate risks to IT networks. Such audits meet compliance mandates by regulatory organizations. Federal IT systems follow Federal Information System Management Act (FISMA) guidelines and report security compliance to US-CERT, the United States Computer Emergency Readiness Team, which handles defense and response to cyberattacks as part of the Department of Homeland Security. In addition, the Control Objective for Information Technology (COBIT) is a set of IT security guidelines that provides a framework for IT security for IT systems in the commercial sector. These audits are comprehensive and rigorous, and negative findings can lead to significant fines and other penalties. Therefore, industry and federal entities conduct internal self-audits in preparation for actual external IT audits, and compile security assessment reports. Step 1: Conduct a Security Analysis Baseline In the first step of the project, you will conduct a security analysis baseline of the IT systems, which will include a data-flow diagram of connections and endpoints, and all types of access points, including wireless. The baseline report will be part of the overall security assessment report (SAR). You will get your information from a data-flow diagram and report from the Microsoft Threat Modeling Tool 2016. The scope should include network IT security for the whole organization. Click the following to view the data-flow diagram: [diagram and report

] Include the following areas in this portion of the SAR: 1. Security requirements and goals for the preliminary security baseline activity. 2. Typical attacks to enterprise networks and their descriptions. Include Trojans, viruses, worms, denial of service, session hijacking, and social engineering. Include the impacts these attacks have on an organization. 3. Network infrastructure and diagram, including configuration and connections. Describe the security posture with respect to these components and the security employed: LAN, MAN, WAN, enterprise. Use these questions to guide you: a. What are the security risks and concerns? b. What are ways to get real-time understanding of the security posture at any time? c. How regularly should the security of the enterprise network be tested, and what type of tests should be used? d. What are the processes in play, or to be established to respond to an incident? e. Workforce skill is a critical success factor in any security program, and any security assessment must also review this component. Lack of a skilled workforce could also be a security vulnerability. Does the security workforce have the requisite technical skills and command of the necessary toolsets to do the job required? f. Is there an adequate professional development roadmap in place to maintain and/or improve the skill set as needed? g. Describe the ways to detect these malicious code and what tactics bad actors use for evading detection. 4. Public and private access areas, web access points. Include in the network diagram the delineation of open and closed networks, where they co-exist. In the open network and closed network portion, show the connections to the Internet. 5. Physical hardware components. Include routers and switches. What security weaknesses or vulnerabilities are within these devices? 6. Operating systems, servers, network management systems. a. data in transit vulnerabilities i. endpoint access vulnerabilities ii. external storage vulnerabilities iii. virtual private network vulnerabilities iv. media access control vulnerabilities v. ethernet vulnerabilities.

7. Possible applications. This network will incorporate a BYOD (bring your own device) policy in the near future. The IT auditing team and leadership need to understand current mobile applications and possible future applications and other wireless integrations. You will use some of this information in Project 2 and also in Project 5. The overall SAR should detail the security measures needed, or implementations status of those in progress, to address the identified vulnerabilities. Include: 1. remediation 2. mitigation 3. countermeasure 4. recovery Through your research, provide the methods used to provide the protections and defenses. From the identification of risk factors in the risk model, identify the appropriate security controls from NIST SP 800-53A and determine their applicability to the risks identified. The baseline should make up at least three of the 12 pages of the overall report. When you have completed your security analysis baseline, move on to the next step, in which you will use testing procedures that will help determine the company's overall network defense strategy. Step 2: Determine a Network Defense Strategy You've completed your initial assessment of the company's security with your baseline analysis. Now it's time to determine the best defenses for your network. Start by reading a publication by the National Institute of Standards and Technology, NIST-SP-800-115 Technical Guide to Information Security Testing and Assessment, and outline how you would test violations. Identify how you will assess the effectiveness of these controls and write test procedures that could be used to test for effectiveness. Write them in a manner to allow a future information systems security officer to use them in preparing for an IT security audit or IT certification and accreditation. Within this portion of the SAR, explain the different testing types (black box testing, white box testing). Include these test plans in the SAR. The strategy should take up at least two of the 12 pages of the overall report. Click the following link to learn more about cybersecurity for process control systems: Cybersecurity for Process Control Systems After you've completed this step, it's time to define the process of penetration testing. In the next step, you'll develop rules of engagement (ROE). Step 3: Plan the Penetration Testing Engagement Now that you've completed your test plans, it's time to define your penetration testing process. Include all involved processes, people, and timeframe. Develop a letter of intent to the organization, and within the letter, include some formal rules of engagement (ROE). The process and any documents can be notional or can refer to actual use cases. If actual use cases are included, cite them using APA format. This portion should be about two pages of the overall 12-page report. After you have outlined the steps of a penetration testing process, in the next step you will perform penetration testing. During the testing, you will determine if the security components are updated and if the latest patches are implemented, and if not, determine where the security gaps are. Step 4: Conduct a Network Penetration Test You've defined the penetration testing process, and in this step, you will scan the network for vulnerabilities. Though you have some preliminary information about the network, you will perform a black box test to assess the current security posture. Black box testing is performed with little or no information about the network and organization. To complete this step, you will use industry tools to carry out simulated attacks to test the weaknesses of the network. Your assessments within the lab will be reported in the SAR. See attached LAB Example and answer Lab Questions Using the tutorial above, respond to the following questions (and put in your lab report): 1. Perform three advanced searches, state what you were searching for, and then take a screenshot of each search. 2. For each of the searches, why did the results change? How can you combine the searches to narrow the results? 3. How can the search techniques above be used by both black and white hat hackers? 4. What type of information would you look for when performing information gathering? 5. What is the difference between active reconnaissance and passive reconnaissance? 6. Research two other search engines and provide the details to conduct the same type of information gathering. Provide the search results, what you searched for, and a screenshot. 7. You were conducting information gathering of a company website; however, no search engine provided any details. After reviewing the website, you saw an email address with a different domain than that of the website. How can this be used? Step 5: Complete a Risk Management Cost Benefit Analysis You've completed the penetration testing, and now it's time to complete your SAR with a risk management cost benefit analysis. Within this analysis, think about the cost of violations and other areas if you do not add the controls. Then add in the cost for implementing your controls. When you have finished with the cost benefit analysis, which should be at least one page of your overall report, move to the final step, which is the completed SAR. As part of the final assignment, remember that you will need to create a slide presentation as part of the executive briefing, and submit that along with the SAR. Step 6: Compile the SAR, Executive Briefing, and Lab Report You have completed comprehensive testing in preparation for this audit, provided recommended remediations, and developed a set of recommendations. Now you are ready to submit your SAR and executive briefing.