Central Washington University Software – Lockdown Browser –

Security Assessment

Information Security Services

Prepared by Ben Sharman, Student Technician, 4/8/19

Contents

Information Security Services 1

Executive Summary 3

Objective 4

Scope 4

Background Information 4

Questions to be answered by Risk Assessment 4

Vulnerabilities 5

Vulnerability 1 5

Threat 5

Likelihood 5

Impact 5

Risk 5

Vulnerability 2 5

Threat 5

Likelihood 5

Impact 5

Risk 5

Assumption & Constraints 6

Uncertainties 6

Summary of Results 6

Time Frame 6

Risk Model 7

Risk Tolerance 7

Recommendations 7

Appendix A: References 8

Appendix B: Participants 9

Appendix C: NIST SP 800-30 10

Tier 1 and 2 Risk Assessments 10

Tier 3 Risk Assessments 10

Appendix D: Risk Assessment Matrix 11

Executive Summary

Central Washington University has been using the software Lockdown Browser, by Respondus, to proctor online tests and quizzes in order to mitigate the ability for students to cheat. One vulnerability of this application is that it may be invasive and provide an opportunity to introduce malicious code to a student's computer. This could lead to an inability for the student to use their device. This should be avoided because this software is used to aid students in success of test taking.

Another vulnerability of the application may be caching or storage of information of the students. Some students have the concern that the application is always running in the background and caching their information. This however is not the case, some parts of the system are running so that way when the application is clicked, it will open, but it does not store data without the action of a student.

The risk of using lockdown browser is moderate. This is because if the application is compromised then this could lead to student data being lost. This is applicable to both vulnerabilities. The overall probability of either happening is low.

Some recommendations for the use of this software is to download it from the link in Canvas to ensure that students are getting the correct software. This can be downloaded on an external site, which means students run the risk of downloading a counterfeit software which may lead to malicious code. The link in Canvas is part of our licensing so it is free and safe to use for students.

In conclusion, Lockdown browser is a safe product to use if used correctly. It does not cache student data and will not run in the background. The risks and vulnerabilities have been evaluated and should not be high enough to concern students.

Objective

The objective of this assessment is to answer a concern brought forward by a student. This is also used to look at the security measures used by the software. The university has been using this software for almost seven years. At the request of Multimodal, a security review of the Lockdown Browser was conducted to determine if it is still an adequate software to use.

Scope

This assessment will take place on the Central Washington University campus. Research will be conducted to identify the possible security risks the lock down browser may have. CIS Security Controls will be used as a reference to identify potential vulnerabilities and where that vulnerability originates. The main goal of this is to understand each control to its fullest extent and better understand how to best mitigate security assessment.

Background Information

The Lockdown browser has been implemented for the use of students taking test outside of class or online. This program helps teachers and instructors ensure an honest test environment for students and allows faculty members to create quizzes for use in canvas. This program can record a student while taking the exam, notify the instructor about suspicious behavior while in use, it is easily integrated within learning management systems (i.e. Canvas), and it is fully automated. Personal data is collected from the student on an as needed basis, but this only occurs during an early shutdown before a test is submitted.

Questions to be answered by Risk Assessment

- How do you like the software?
- What are some advantages to the software?
- What are some complications that you have seen with the software?
- Is there any student feedback that you have heard, good or bad?
- Have you heard of the software logging information from users and or running in the background?
- Have you thought of any other software's that could replace lockdown browser?
- What do you do as an Admin for this software?
- How often is the software updated?
- How long does our license last?
- How long have we had our license for?

Vulnerabilities

Vulnerability 1

The first vulnerability for this software is the software may store student data. There is a possibility the application runs in the background and potentially stores user data (ExamSoft, 2019).

Threat

If this program is does store data from the user then there is a threat to the individual's privacy as well as any sensitive data captured.

Likelihood

The likelihood of this happening is possible.

Impact

The impact of a student's data being compromised due to use of software required by the university is significant as it could cause damages to the student but also the organizations reputation.

Risk

The risk related with this is moderate because it is possible and the impact would be significant if the data is compromised.

Vulnerability 2

The second vulnerability is that the program may be invasive to the user's computer and could introduce a virus to their computer (ExamSoft, 2019). This could lead to viruses being introduced to their computer and impact their ability to take tests using the Lockdown Browser.

Threat

The threat associated with this vulnerability is the Lockdown Browser can introduce viruses onto the user's computer. This is a concern because it jeopardizes the security of student's personal computers.

Likelihood

The likelihood of this occurring is unlikely if the student is downloading the version of the software in canvas, but has a reported possibility. Some university users that have been interviewed said they have never experienced this problem, but after research there are still cases of students reporting this as a problem.

Impact

The impact, if this threat occurs, is significant. If there is a virus that has been introduced on the user's computer, then it can impact their productivity and ability to use their computer for every day work. There could also be impact to the university's reputation.

Risk

The risk related to this threat is moderate because it is unlikely and could have significant impact.

Assumption & Constraints

Assumptions for the use of the Lockdown Browser are that it is an appropriate tool for the use of instructors for online tests. There are some good features of the browser that allow the instructor to ensure honesty during the duration of the test. One of these factors is the ability to record students taking the test. The other is being able to receive notifications about specific activity related to a student taking that test.

Some constraints that may hinder the effectiveness of the software are the backlash from students and the administrative uses for taking tests. Another possible constraint is the budget. Depending on which department is purchasing the product, their budget may not support the financial ability to supply the software for the campus. The cost of this software is $5,045 for the 12,000 students on campus. This fee is an annual fee. This price does not seem to be too expensive but depending on the budget and the department it may affect their fiscal budget.

Another constraint, some students have had problems with downloading the software. There is a link within canvas that has CWU's personal license with the software for download. If student tries to download the software from online, then there may be some problems when opening quizzes in Canvas. It is recommended that students use the link within Canvas to download the software.

Uncertainties

Some uncertainties that come with the use of the Lockdown browser are that there is no way to see what the program is doing in a hibernated state, but on a windows machine, task manager will show the user if the program is running or not. There are assumptions that the Lockdown browser is running in the background but it is not definite. There is also no way to see if it saves data from other applications while it is installed on the user's computer. With this software, it is important to ensure the confidentiality of student information as well as their privacy. Another uncertainty is there are no results on how the software impacts the user's computer and if the software limits the accessibility of the user's computer.

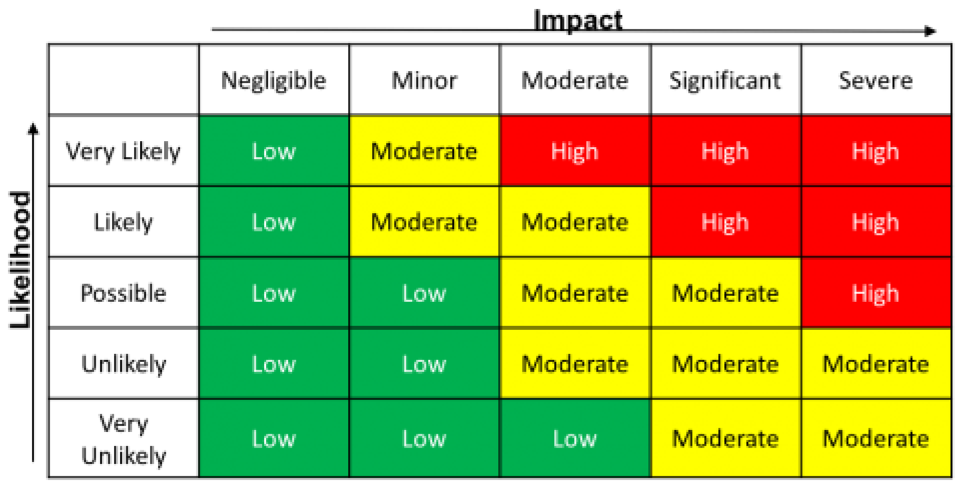
Summary of Results

To summarize the Lockdown browser is not a high-risk solution. While there are concerns user data being stored by the program while not in use the likelihood of this is low. There is the possibility the software could introduce malicious software to a user's device, but this is unlikely.

Time Frame

The timeframe of this assessment is to outlive the use of the Lockdown Browser product. There is still the possibility that Central Washington could decide to use another system. Central Washington University has decided to pilot a system called TopHat, and this would be used to add a mobile feature to test taking while using a locked down browser. This Assessment will withhold during the time that the Lockdown browser is in use on the Central Washington University campus.

Risk Model


Impact
Likelihood

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

Risk Tolerance

The risk tolerance related to this software is fairly high. There is no information stating that student or user information is at risk. The software running in the background in a hibernated state does not seem to impact the data on the user's computer (Examsoft, 2019).

Recommendations

Recommendations while using Lockdown Browser is to make sure that the anti-virus is up-to-date and to check when closing the software that it fully closed. If the software is acting up and is causing concern, it may be a good idea to delete the program and download it again. Another possible recommendation is to update the software on a regular basis to ensure that there are no hidden bugs that need to be fixed.

A recommendation is that the administrative team for the Lockdown browser should include a warning or disclaimer when downloading the software from canvas. There should also be a clear explanation of what the software can and cannot do to put students at ease about the privacy of their device while the Lockdown browser is installed. This would help make students aware about the system and what it does.

APPENDICIES

Appendix A: References

Breckon, D. (2019, April 8). Lockdown Browser Security Assessment [Personal interview].

Examsoft. (2019). The Risks of Using Lockdown Browsers. Retrieved February 10, 2019, from https://examsoft.com/resources/blog/the-risks-of-using-lockdown-browsers

Hollingsworth, F. (2019, April 8). Lockdown Browser Security Assessment [Personal interview

Respondus. (n.d.). Retrieved February 10, 2019, from https://www.respondus.com/products/lockdown-browser/

Appendix B: Participants

Ben Sharman (Composer)

Jamie Schademan (IS Manager)

Kellon Benson (Information Security Analyst)

Forrest Hollingsworth (Interviewee)

Delayna Breckon (interviewee)

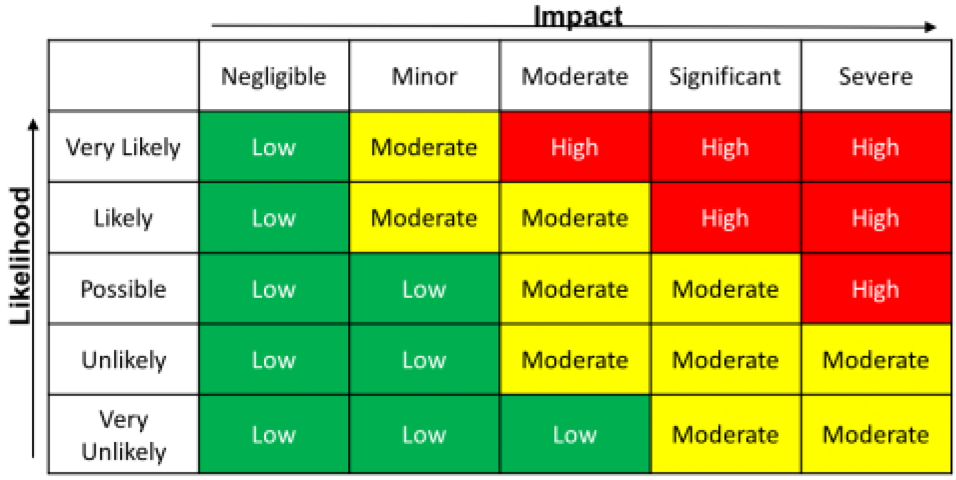
Appendix C: NIST SP 800-30

Per NIST Special Publication 800-30, (Appendix K):

Tier 1 and 2 Risk Assessments must include: Organizational governance structures, or processes associated with the assessment (e.g., risk executive [function], budget process, acquisition process, and systems engineering process, enterprise architecture, information security architecture, organizational missions/business functions, mission/business processes, and information systems supporting the mission/business process).

Tier 3 Risk Assessments must identify: the information system name, and location(s), security categorization, and information system (i.e., authorization) boundary.

Appendix D: Risk Assessment Matrix



Impact
Likelihood

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate