5-2023

An Application Risk Assessment of Werner Enterprises

Nathan Andres

An Application Risk Assessment

Conducted by

Nate Andres, Redmond Reed, Abdoul Latoundji,

Andrew Fisher and Sara Kroft

University of Nebraska at Omaha

On

Werner Enterprises Inc.

5/15/2023

Professor Greg Hoff

Cyber Security Capstone 2023

Table of Contents

Abstract

Risk assessments provide a systematic approach to identifying potential risks that could negatively impact an organization's operations, financial performance, and reputation. Using a risk assessment, companies can evaluate potential risks and vulnerabilities, prioritize them based on their potential impact, and develop strategies to manage and address these risks effectively.

Werner Enterprises Inc. is a nationally known trucking company headquartered in Omaha, Nebraska. Our cybersecurity capstone project motivation was to partner with Werner to produce an assessment of known application risks in a functional way that can be repeated for all of Werner's applications. To achieve this, we created a risk equation that utilizes the vulnerabilities and risks of applications and their impact on Werner to develop an overall risk score for each application. The ideal outcome of this risk assessment is to provide findings and recommendations to improve Werner's overall application security posture, as well as provide meaningful data for future analysis.

While ideally, we would have been able to assess the risk score of every application used by Werner, our team had to work within a limited time constraint. Therefore, our team assessed a list of twenty-five applications. With our risk equation and assessment described throughout this report, Werner can use this information to continue risk assessments on all remaining applications with relative ease. The applications determined as in-scope for this assessment were divided evenly among our group members. While a rough outline of the analysis guidelines was used, there are still several notes in each application that could be subject to bias. Threat likelihood analysis was performed in a similar manner, so some threat ratings may be subject to bias.

Our risk equation quantifies a point score for external and internal vulnerabilities, threats, data classification, mission critical applications, and recovery time objective. Using the data collected via open-source intelligence and meetings with application owners, we calculated a risk score for the twenty-five applications in-scope.

Our entire application risk assessment has been coordinated alongside the National Institute of Technology and Standards (NIST) 800-53 R5 report on properly conducting risk assessments. Additionally, all recommendations and implementations have been suggested alongside the NIST Cybersecurity Framework (CSF) 2.0 draft, a continuation of the CSF 1.1 framework created to guide corporations along an improved, standardized security posture.

Introduction

The goal of this capstone project was to classify the applications of Werner by examining their application owners, entitlements, business impact analysis (BIA) criticality, and data classification to objectively determine application risk and report our conclusions. By determining and reporting application risk, we sought to bring clarity to Werner's application security posture and recommend improvements. This will ideally bring Werner closer to appropriate cybersecurity standards and frameworks, such as the upcoming National Institute of Standards and Technology (NIST) cybersecurity framework (CSF 2.0) (NIST, 2023). Due to the sensitive nature of the information on vulnerabilities, parts of this report have been redacted and would require a non-disclosure agreement for all non-Werner associates to view the restricted report.

Werner Enterprises Inc. is a transportation and logistics company based in the United States. Headquartered in Omaha, Nebraska with over 8,000 trucks, 24,000 trailers, and 13,000 employees, Werner is strategically designed to provide superior support and keep America moving (Werner Enterprises, 2023). As a company classified as critical infrastructure under the transportation systems sector in the United States (CISA, 2023), the security of Werner remains of high importance within the evolving area of cybersecurity.

This project was conducted from January 2023 to May 2023 by undergraduate cybersecurity students at UNO, namely Nate Andres, Redmond Reed, Abdoul Latoundji, Andrew Fisher, and Sara Kroft.

System Scope

The scope of our application risk assessment includes a list of all applications below along with their basic descriptions. The applications were collected from Werner's Okta environment using internal data classification methods. Applications have been listed alphabetically for convenience.

Application List

The applications included in this report (and their descriptions) are as follows:

- Azure DevOps:
    - A cloud-based set of development tools and services offered by Microsoft to help software development teams plan, develop, test, and deploy software applications.
- ClearSight:

  - A claims administration system in which associates can enter claims, adjusters manage claims & payouts, and payments can be managed.
- Drive Werner Pro:
  - An application for Werner drivers to submit bills to get paid and verify their bills.
- ERS
  - An application that is used to check on breakdowns with Werner drivers and log them in the system.
- GitHub:
  - A web-based platform for version control and collaboration that allows developers to store, manage, and track changes to their code.
- KnowBe4:
  - A security awareness and training platform that is used to educate and test associates on digital security.
- Lucidchart:
  - A cloud-based visual workspace that allows users to create and collaborate on diagrams, flowcharts, mind maps, and other visual representations.
- MasterMind:
  - A transportation management system that intakes all customers' requests and processes them to completion.
- Microsoft Office 365:
  - A subscription service that provides access to Microsoft Office applications and other productivity tools and services such as email, file storage, and communication tools.
- MuleSoft:
  - An integration platform as a service that provides a platform to build application and serves as an integration builder between applications.
- Okta:
  - An identity and MFA provider for Werner which upholds nearly all security standards and authentication company-wide.
- Palo Alto Networks:
  - A next-generation firewall that manages and maintains secure access across the enterprise (and contains 8 different firewall clusters of at least 2 firewalls).
- Remediant:

    - An application that limits the lateral movement of user (admin) accounts with administrative access through the network and provides just-in-time (JIT) admin access to that resource.
- Salesforce Roadmaster:
    - A database working across multiple departments to improve processes and data automation; focused on anything related to Roadmaster schools.
- Salesforce Werner Corporation:
    - A database working across multiple departments to improve processes and data automation; focused on day-to-day operational data.
- ServiceNow:
    - Serves as a ticketing, issue tracking, and escalation platform for technical issues.
- SharePoint:
    - An internal source of current events and other useful information for employees, both new and seasoned.
- Snowflake:
    - A central data repository with several sources of input data from various Werner apps.
- TeamViewer:
    - An industry standard remote-control application used by the Werner support team.
- Werner EDGE:
    - A self-service application for third-party carriers to perform actions themselves (booking freight, preferences).
- Werner Store:
    - Hosts the Werner public product catalog available for purchase.
- Workday:
    - A central HR system housing personal identifiable information (PII) for all employees.
- Workiva:
    - A compliance tracking and remediation platform for the Finance, Risk, and Accounting departments.
- Workplace:
    - An employee social platform allowing employees to share experiences from work or home with each other.
- Zoom:
    - An industry standard remote conferencing software used for daily communications company-wide.

Limitations

Applications were divided by group member, and while a rough outline of the analysis guidelines was utilized, there remains several notes in each application that could be subject to bias. Threat likelihood analysis was performed similarly, so some threat ratings may be subject to bias.

No concrete industry standard guideline was used alone for the purpose of this audit. The analysis done was a combination of several different security guidelines adapted for our specific use case.

Time constraints for this project limited how many applications were able to be reviewed, but future reviews should be expected to be more efficient now that a process has been created. Ideally, all applications would have been reviewed in this risk assessment, but because of time, only twenty-five were considered.

Process Narrative

All members of the Werner capstone team and their professors signed a non-disclosure agreement (NDA) to gain permission to use sensitive security information related to Werner's applications and their vulnerabilities. The team then pulled a list of twenty-five applications from Werner’s Okta environment.

We performed a preliminary analysis of the audited applications, checking for common auditing pitfalls. The team established boundaries for what data was to be analyzed and what should be left alone. Only two group members were authorized to access some data.

Once boundaries were established, we started applying the NIST framework to gather data and began reporting on initial findings that were supported by this framework. Preliminary research was conducted to outline a risk equation for future work (like applying a security framework).

We expanded on the preliminary analysis of the applications to include common issues, including unapplied patches, non-compliance, and versioning. During this time, application owner meetings were held for further clarification on data classification, roles, mission critical applications (MCAs), and dependencies to complete the application chart. All data from these meetings were compiled and used to begin research into application risks.

Finally, we generated the final risk equation based on the data derived from all sprints, along with open-source intelligence, and calculated the risk for each application using this equation.

Overall, the process involved a comprehensive approach to auditing and assessing application risks while adhering to strict data security protocols through NDAs and establishing clear data analysis boundaries. The team worked closely with application owners and used a variety of tools and frameworks to identify and mitigate potential security issues.

Risk Equation

Our risk calculation equation was created using a variety of traditional risk tools. First, we used the basic structure of identifying assets and threats, identifying vulnerabilities, assessing the likelihood of threats and their impact, and assigning scores to these factors. With this basic structure, we modified a risk equation (Risk = Likelihood x Impact) to include our defined structure using the data collected in our findings. This final risk score was then automated in an Excel spreadsheet to complete our risk equation. The equation is calculated below as follows:

Likelihood (out of 10): Vulnerabilities + Threat

- Vulnerabilities: External + Internal
    - External: 2.5 - (Security Scorecard (SSC) + Domain Health (DH))
        - SSC = score / 80
        - DH = {passed / (errors + warnings + passed)} / 80
    - Internal: Single Point of Failure (SPOF) + Admin Single Point of Failure (ASPOF)
        - SPOF = 1.25 if yes, 0 if no
        - ASPOF = 1.25 if yes, 0 if no
- Threat: For each risk, we assign a score out of 5 (1 is the lowest threat), then find the average of these scores.
    - Example: If Risk 1 is 1/5, Risk 2 is 3/5, and Risk 3 is 5/5, the total of these is 9/5. Then the average is found by dividing 9/5 by 3, which would be 3/5.

Impact (out of 10): DC + MCA + RTO

- Data Classification (DC): LEGAL = 4, RESTRICTED = 3, INTERNAL = 2, PUBLIC = 1
- Mission Critical Application (MCA): 2 if yes, 1 if no
- Recovery Time Objective (RTO):

- < 4 HRS = 4 points
- 4 – 8 HRS = 3 points
- 9 – 24 HRS = 2 points
- > 24 HRS = 1 point

Total Risk Score: (Likelihood x Impact) / 100

Findings

Data was collected for all applications in scope but cannot be disclosed in this report due to data sensitivity. The data collected for all applications included application name, internal access count, external access count, recovery time objective (RTO) in hours, data classification level, mission critical applications (MCA), security scorecard scores (SSC), company domain health, dependencies, and any single points of failure (SPOFs). These fields were generally abbreviated, and the table was alphabetized.

Application Risks

Using the risk equation and data findings described above, we calculated the risk score for each application and listed them in our restricted report from highest risk to lowest risk. Under these risks, there were details regarding how the risks were calculated. Four areas of risk that were evaluated included Werner specific risk, transportation specific risk, application type specific risk, and application specific risk. Unfortunately, due to the sensitive nature of the data, these findings cannot be disclosed.

Recommendations

The following recommendations for this application risk assessment are an addendum to the findings that were listed above by the capstone team. As an Honors student at UNO, Nate Andres has been tasked with additional work on top of the process of the capstone team to highlight the academic standards of the Honors program. As such, the following recommendations are a representation of this work and has been solely completed by Nate Andres. The goal of these recommendations is to create suggestions for future implementation at Werner to improve Werner's application security posture. Ideally, these recommendations will be implemented with the new and upcoming NIST CSF 2.0 framework used as an ideal corporate security standard.

Unfortunately, these findings cannot be disclosed due to data sensitivity. All recommendations were associated with NIST CSF 2.0 draft framework core fields, primarily from the platform security (PR.PS)

field where applications are managed with data security (PR.DS) and technology infrastructure resilience (PR.IR) to protect the confidentiality, integrity, and availability of systems (NIST 2023). Additional CSF 2.0 core frameworks include proper identity management, authentication, and access control (PR.AA), as well as organizational security awareness and training (PR.AT) (NIST, 2023). The framework and core fields described above are currently only available in draft form and has not been publicly released as an official cybersecurity framework. The use of this framework draft has been used for the future implementation of security at Werner. The standards above were used to justify and recommend the improved security of applications to Werner to improve their organizational application security posture.

References

Andress, J., & Leary, M. (2017). Building a Practical Information Security Program. *Syngress*, 23-34.

Baxter, K. (2022). *TMS and Cybersecurity.* Retrieved from InTek Freight and Logistics: https://blog.intekfreight-logistics.com/tms-cybersecurity

Cimpanu, C. (2019). *How MuleSoft patched a critical security flaw and avoided a disaster*. Retrieved from ZDNet: https://www.zdnet.com/article/how-mulesoft-patched-a-critical-security-flaw-and-avoided-a-disaster/

CISA. (2023). *Transportation Systems Sector*. Retrieved from Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector

CVE. (2023). *CVE List.* Retrieved from https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=microsoft

CVE Details. (2023). *TeamViewer: Security Vulnerabilities.* Retrieved from https://www.cvedetails.com/vulnerability-list/vendor_id-11100/product_id-19942/Teamviewer-Teamviewer.html

LookingGlass. (2019, March 27). *Three Common Threat Actors and the One You Might Not Know About*. Retrieved from LookingGlass Cyber Solutions: https://lookingglasscyber.com/blog/threat-intelligence-insights/three-common-threat-actors-and-the-one-you-might-not-know-about/

LucidWorks. (2022). *Log4j Vulnerabilities*. Retrieved from https://support.lucidworks.com/hc/en-us/articles/4415649244055-Log4j-vulnerabilities-CVE-2021-44228-CVE-2021-45046-CVE-2021-45105-and-CVE-2021-44832

MuleSoft. (2021). *Apache Log4j2 Vulnerability.* Retrieved from https://help.mulesoft.com/s/article/Apache-Log4j2-vulnerability-December-2021

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from National Institute of Standards and Technology: https://doi.org/10.6028/NIST.CSWP.04162018

NIST. (2023). *Cybersecurity Framework*. Retrieved from National Institute of Standards and Technology: https://www.nist.gov/cyberframework

NIST. (2023). *Risk Management Framework (RMF)*. Retrieved from National Institute of Standards and Technology: https://csrc.nist.gov/projects/risk-management/about-rmf

Okta. (2022, November 30). *What is Okta and What Does Okta Do?* Retrieved from Okta Help Center: https://support.okta.com/help/s/article/what-is-okta?language=en_US

Pariseau, B. (2023). *Azure Pipelines vulnerability spotlights supply chain threats*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/news/365534205/Azure-Pipelines-vulnerability-spotlights-supply-chain-threats

Werner Enterprises. (2023). *About Werner*. Retrieved from Werner Enterprises: https://www.werner.com/about/