Shadow IT Detection & Risk Intelligence Report

Author: Asher Livingston

Program: M.S. Cybersecurity & Networks – University of New Haven

Date: July 16, 2025

Project Summary

This study examines the unauthorized utilization of software tools,commonly referred to as Shadow IT, across various organizational departments. These tools are frequently adopted without formal approval from the IT department, resulting in significant security concerns, such as the absence of Multi-Factor Authentication (MFA),lack of Quality Assurance (QA) testing, and exposure to high-risk vulnerabilities,as indicated by Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS) metrics.

Utilizing Power BI, the project visualizes usage patterns, risk scores, and the approval status of diverse applications.The dashboard provides cybersecurity teams and decision-makers with actionable insights to mitigate Shadow IT risks and advocate for secure alternatives.

Tool & Risk Overview

The dataset was meticulously curated and encompasses fields such as tool name, category, department, user count, data sensitivity, CVEs, and MFA/QA/Approval status. Each tool was assigned a risk score based on its security posture. Tools such as Dropbox, Telegram, and Discord were identified as having severe vulnerabilities and a lack of protective controls.

Departmental Patterns & Risk Posture

Analysis revealed that departments like **Sales, Operations, and Engineering** use the highest number of unapproved or insecure tools.

- Over **60%** of the tools were **untested (QA)**
- **53%** of tools lacked **MFA**
- **4 tools** had **CVSS scores above 8.0**, including active CVEs
- Messaging tools like **Discord** and **Telegram** showed high-risk behavior and were disapproved

Recommendations

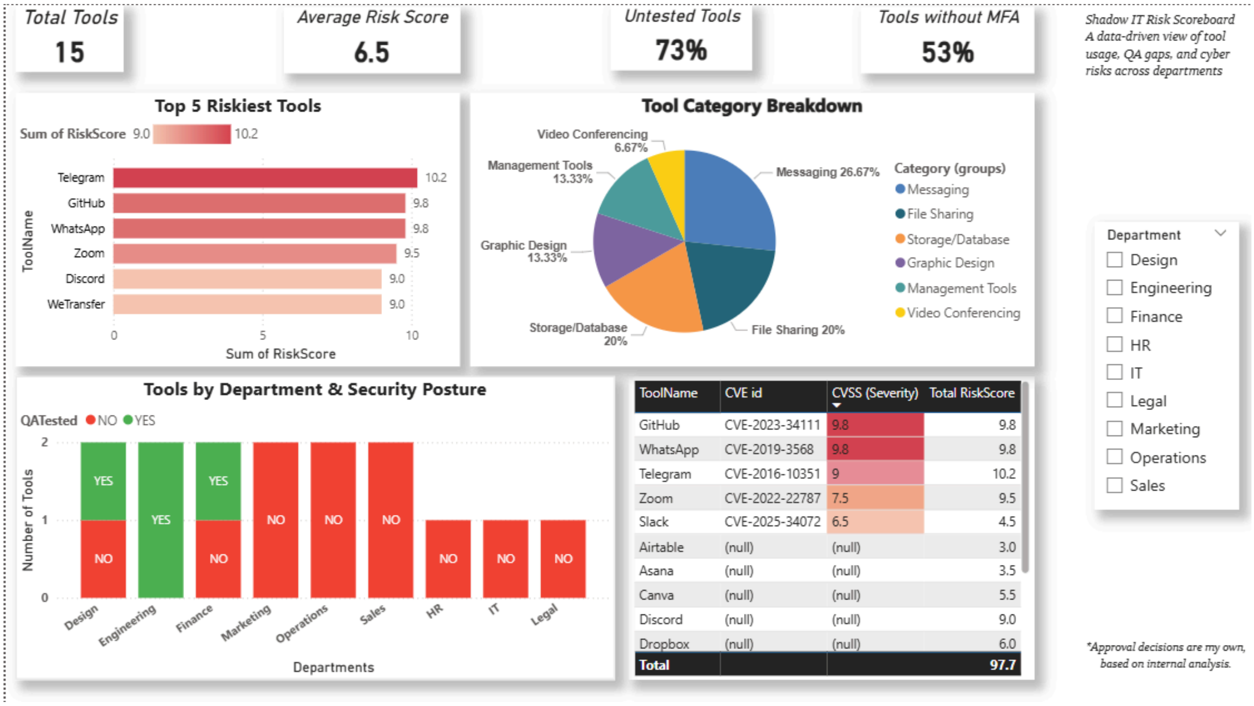
Implement organization-wide requirements for multi-factor authentication (MFA).Replace tools that are rejected or deemed high-risk with approved corporate alternatives, such as Microsoft Teams and OneDrive. Conduct mandatory quality assurance (QA) testing prior to the deployment of any tools.Monitor the adoption of tools through a Shadow IT detection framework.

Power BI Dashboard Design

- **KPI Cards**: Total Tools, MFA %, QA %, Avg Risk
- **Pie Chart**: Distribution by Tool Category
- **Stacked Column Chart**: QA testing across departments
- **Risk Table**: CVEs, CVSS scores, and safer replacements
- **Slicers**: Dynamic filtering by QA, Approval, Department, and MFA

Color-coded visuals were used to distinguish secure vs. insecure tools, with green for approved, red for rejected, and neutral tones for pending.

Final Dashboard Snapshot



Total Tools 15

Average Risk Score 6.5

Untested Tools 73%

Tools without MFA 53%

Shadow IT Risk Scoreboard A data-driven view of tool usage, QA gaps, and cyber risks across departments

ToolName	CVE id	CVSS (Severity)	Total RiskScore
GitHub	CVE-2023-34111	9.8	9.8
WhatsApp	CVE-2019-3568	9.8	9.8
Telegram	CVE-2016-10351	9	10.2
Zoom	CVE-2022-22787	7.5	9.5
Slack	CVE-2025-34072	6.5	4.5
Airtable	(null)	(null)	3.0
Asana	(null)	(null)	3.5
Canva	(null)	(null)	5.5
Discord	(null)	(null)	9.0
Dropbox	(null)	(null)	6.0
Total			**97.7**

Department

- ☐ Design
- ☐ Engineering
- ☐ Finance
- ☐ HR
- ☐ IT
- ☐ Legal
- ☐ Marketing
- ☐ Operations
- ☐ Sales

**Approval decisions are my own, based on internal analysis.*

Technology Used

- Power BI Desktop v2.145.1105.0
- DAX for custom metrics (e.g., % Untested Tools, Avg Risk Score)
- Manually structured CSV dataset with real-world security mapping

Conclusion

This project underscores the critical necessity of monitoring Shadow IT across various departments and developing governance strategies to mitigate associated risks. The dashboard not only identifies high-risk tools but also facilitates proactive risk mitigation by recommending safer, approved technologies.