Shadow IT Detection & Risk Intelligence Dashboard

07.16.2025

—

Asher Livingston
University of New Haven - Master's in Cybersecurity and Networks
West Haven, CT 06516

Overview

This Power BI project systematically identifies and assesses the utilization of Shadow IT tools across various departments within a variety of organization data collected from the Internet. Shadow IT tools refer to applications employed without formal IT authorization, which frequently result in considerable cybersecurity and compliance risks.

The objective is to illustrate the utilization of such tools, evaluate their risk based on Multi-Factor Authentication (MFA) status, Quality Assurance (QA) testing, and Common Vulnerabilities and Exposures (CVE) vulnerabilities, and propose secure alternatives. The dashboard was constructed using manually curated data and is intended for both technical and non-technical decision-makers.

Goals

- Identify unauthorized or unapproved Shadow IT tools
- Visualize tool usage by department and risk score
- Highlight tools lacking security features like MFA and QA testing
- Help cybersecurity teams make data-driven decisions
- Recommend secure alternatives for high-risk tools

Dataset & Specifications

The dashboard utilizes a CSV dataset comprising fields such as Tool Name, Department, Risk Score, QA Tested, Approval Status, and CVE vulnerability information.

The tools were evaluated manually based on cybersecurity indicators. The dashboard comprises bar charts, pie charts, KPI cards, and interactive slicers. It is constructed using Power BI Desktop (version 2.145.1105.0) and incorporates custom DAX measures for calculating key metrics such as "% Untested Tools" and "Average Risk Score."

.

Visual Design & Components

- **Pie Chart**: Shows category distribution of Shadow IT tools
- **Stacked Column Chart**: QA testing status across departments
- **KPI Cards**: Show total tools, % without MFA, average risk
- **Risk Table**: Detailed CVE info and corporate alternatives

Color-coded visuals were used to enhance clarity — green for approved tools, red for high-risk ones. Slicers were added to filter by department and QA status.

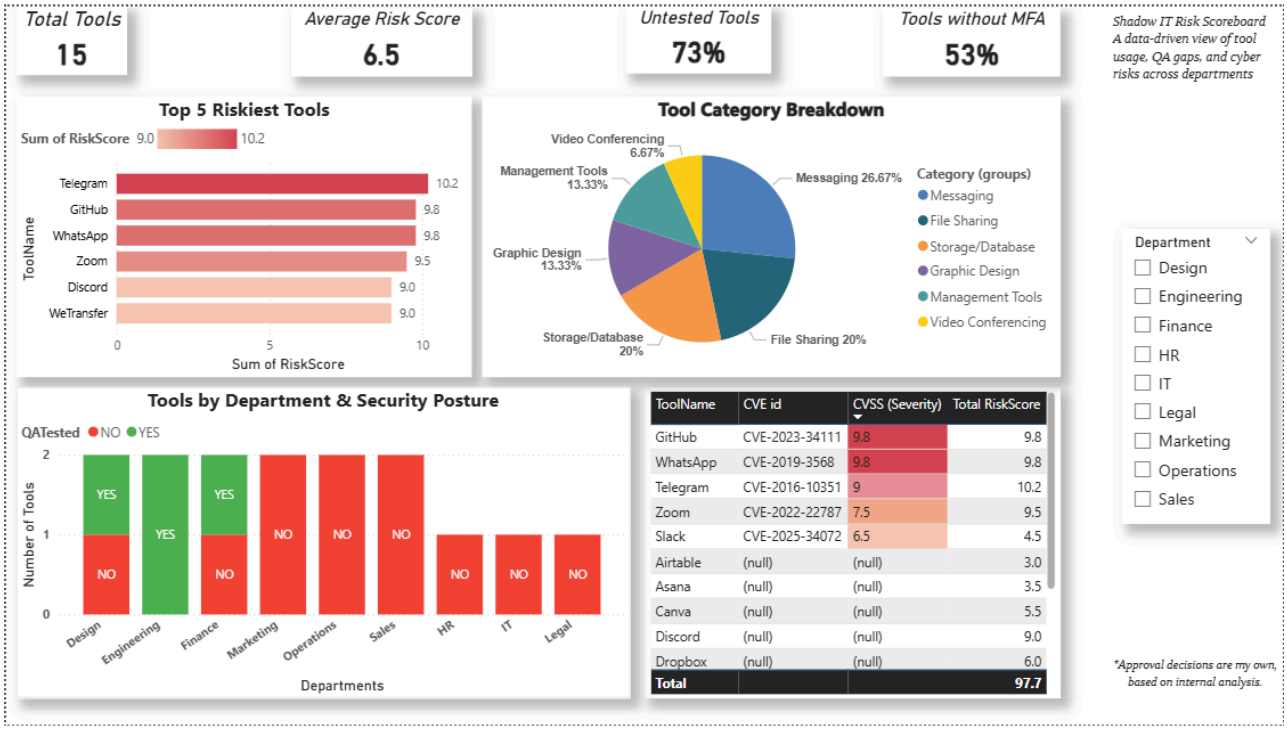
Milestones (timeline-style)

- **Dataset Creation** – July 12, 2025
- **Dashboard Design in Power BI** – July 13–14, 2025
- **Visual Polishing and QA Review** – July 15, 2025
- **Final Documentation** – July 16, 2025

Insights

Sixty-one percent of the tools utilized across various departments have not undergone quality assurance testing, thereby presenting a latent risk. The Sales and Operations departments employ the greatest number of high-risk tools. Messaging platforms, such as Telegram and Discord, are prevalent within the Shadow IT landscape, frequently lacking multi-factor authentication and being disapproved by IT departments. Several tools possess active Common Vulnerabilities and Exposures (CVE) with Common Vulnerability Scoring System (CVSS) scores exceeding 7.5, signifying urgent threats.

Screenshot


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
Top 5 Riskiest Tools
Sum of RiskScore 9.0 10.2
Telegram 10.2
GitHub 9.8
WhatsApp 9.8
Zoom 9.5
Discord 9.0
WeTransfer 9.0
ToolName
0
5
10
Sum of RiskScore
Tool Category Breakdown
Video Conferencing 6.67%
Management Tools 13.33%
Messaging 26.67%
Graphic Design 13.33%
Storage/Database 20%
File Sharing 20%
Category (groups)
Messaging
File Sharing
Storage/Database
Graphic Design
Management Tools
Video Conferencing
Department
Design
Engineering
Finance
HR
IT
Legal
Marketing
Operations
Sales
Tools by Department & Security Posture
QATested NO YES
Number of Tools
Design
Engineering
Finance
Marketing
Operations
Sales
HR
IT
Legal
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
*Approval decisions are my own, based on internal analysis.

Appendix

Dataset Column Description

Column Name	Description
ToolName	Name of the Shadow IT tool used by the department
Category	Function or type of tool (e.g., Messaging, File Transfer, Design, etc.)
Department	Business unit or team using the tool
UserCount	Number of users in the department using the tool
DataSensitivity	Level of data handled by the tool (Low, Medium, High)
MFAEnabled	Whether Multi-Factor Authentication is enabled (Yes/No)
QATested	Whether the tool was tested and approved by the QA process (Yes/No)
ApprovalStatus	Approval decisions are my own, based on internal analysis.
RiskScore	Overall risk score based on security posture (custom scale, 0–12)
CVE_ID	Identifier of any known vulnerability (if applicable)
CVSS_Score	Severity score of the CVE (Common Vulnerability Scoring System, range 0–10)
CVE_Description	Brief summary of the vulnerability or exploit
CorporateAlternative	Approved secure alternative recommended by IT

Key DAX Measures

% Untested Tools

Shows the percentage of tools that have not undergone QA testing.

```
Pct_Untested =
DIVIDE(
    COUNTROWS(FILTER('ShadowIT risk scoreboard', 'ShadowIT risk scoreboard'[QATested] = "No")),
    COUNTROWS('ShadowIT risk scoreboard'),
    0
)
```

Total Tools Without MFA

Counts how many tools do not have multi-factor authentication enabled.

```
No_MFA =
CALCULATE(
    COUNTROWS('ShadowIT risk scoreboard'),
    'ShadowIT risk scoreboard'[MFAEnabled] = "No"
)
```