BITSIGHT | Google

# Cybersecurity Control Insights: An Analysis of Organizational Performance

## Who is this Study for?

**Security professionals:** Inform your cybersecurity strategy with the latest cybersecurity performance insights.

**Board members:** Know what challenges your CISO faces so you can ask the right questions to protect your organization.

**Executives:** Prioritize your budget and workforce to reflect current challenges.

## This study included:

**1** Global Study of Organizational Cybersecurity Performance

**3** Grades per Control per Organization

**9** Industries

**16** Cybersecurity Controls

**100,000** Organizations

BITSIGHT | Google

Have collaborated to study how organizations around the world perform across cybersecurity controls in the Minimum Viable Secure Product (MVSP) framework.

## Our study reveals:

**Control Gaps**

Discover critical areas where organizations are falling short across MVSP controls.

**Positive Progress**

Learn more about the improvements and successes organizations are achieving.

**What's MVSP?**

MVSP is a minimalistic security checklist for B2B software and business process outsourcing suppliers, consisting of 25 controls across four key areas – Business, Application Design, Application Implementation, and Operational.

For example, [2.2] **HTTPS-only** requires that organizations redirect insecure HTTP traffic on port 80 to HTTPS on port 443, and implement Strict-Transport-Security to ensure users default to secure connections on subsequent visits.

## The Study

Bitsight measures the cybersecurity performance of organizations around the world, allowing it to help measure how organizations perform across MVSP controls.

Performance is based on 23 cyber risk vectors, including Patching Cadence, Desktop Software, Mobile Software, and more. Each organization received one of three grades per MVSP control.

**Pass** | **Needs Improvement** | **Fail**

Bitsight risk vectors mapped to 16 MVSP controls and nine industries.

**9 industries:**

Computer Software (CS) | Automotive | Banking | Energy/ Resources | Hospital & Healthcare | Insurance | Retail | Pharmaceuticals | Media/ Entertainment

**16 MVSP controls:**

- [1.1] Vulnerability reports
- [1.2] Customer testing
- [1.3] Self-assessment
- [1.4] External testing
- [1.5] Training
- [1.7] Incident handling
- [1.8] Data handling
- [2.2] HTTPS-only
- [2.3] Security Headers
- [2.5] Security libraries
- [2.6] Dependency Patching
- [2.7] Logging
- [3.3] Vulnerability Prevention
- [3.4] Time to fix vulnerabilities
- [2.8] Encryption
- [4.2] Logical access

**Read the technical white paper to dive deeper into the study's methodology and detailed findings**

Read now →

## Key Findings

### The Good news

In 2023, every industry has:

**1 A high Pass rate[1] for 10 of the 16 MVSP controls we studied:**

[1.1] Vulnerability Reports
[1.2] Customer Testing
[1.5] Training
[1.7] Incident Handling
[1.8] Data Handling
[2.5] Security Libraries
[2.6] Dependency Patching
[2.7] Logging
[3.4] Time to Fix Vulnerabilities
[4.2] Logical Access

Every control with high Pass rates also has low Fail rates, with the exception of [2.6] Dependency Patching and [3.4] Time to Fix Vulnerabilities. All industries have high Pass rates and high Fail rates for [2.6] Dependency Patching and [3.4] Time to Fix Vulnerabilities.

[1]We considered the percentage of organizations in each industry earning each grade for each control as a way to understand industry performance. For example, X percent of organizations in Industry Y earned a Passing grade for Control Z. When we use "Pass rate," "Needs Improvement rate," "Fail rate," or more generally, "rate," we are referring to the rate described here.

**2 ~100%**

**Pass rates across four MVSP controls**

And low Fail rates mapping to Bitsight's Security Incidents risk vector ([1.7]Incident handling, [1.8]Data handling, [2.7]Logging, [4.2]Logical access).

**3 High Pass rates for [1.2] Customer Testing** (A step forward toward a safer third-party digital ecosystem.) **and [1.5] Training** (Human error can result in stolen data and more. Organizations are taking training efforts seriously.)

**From 2020 to 2023:**

- Macro[2] Pass rates rose across every control.
- Macro Fail rates declined across every control except [2.3] Security Headers, with Fail rates for [2.6] Dependency Patching and [3.4] Time to Fix Vulnerabilities declining the most.
- Significant macro improvements in Pass rates across [2.8] Encryption, [1.2] Self-assessment, [1.2] External testing, [3.3] Vulnerability Prevention, by as much as 25 percent marginally.

[2]Each MVSP control has one "macro" Pass/Needs Improvement/Fail rate, representing the average Pass/Needs Improvement/Fail rate for that control across all industries except for CS.

### Areas for Improvement

Organizations across nearly all industries:

**1** Are struggling with controls critical to the health of an organization's vulnerability management program.

**2** The following MVSP controls have either high 2023 Fail rates, low Pass rates, or both, across all industries. Many, if not all of them, are important for vulnerability management:

[1.2] Self-assessment
[1.4] External Testing
[2.2] HTTPS-only
[2.3] Security Headers
[2.6] Dependency Patching
[2.8] Encryption
[3.3] Vulnerability Prevention
[3.4] Time to Fix Vulnerabilities

**3 Organizations now > 2020**

Are Failing to implement [2.3] Security Headers, including those in the CS industry. This could lead to heightened risk of specific vulnerability types (e.g. cross-site scripting and click-jacking).

### State of the Computer Software Industry

CS Pass rates improved across every control just like we observed on the macro front but CS lagged behind macro improvements in all but one control – [2.3] Security Headers (CS improved its Pass rate by 38 basis points more than macro average).

CS Fail rates for [2.6] Dependency Patching and [3.4] Time to Fix Vulnerabilities did not improve as much as the macro average. These controls both map to the same Bitsight risk vector, Patching Cadence. Underperformance in this risk vector is correlated with an increased likelihood of an incident.

**[2.8] Encryption:**

**25%** ↑ Macro Pass rate improvement

**21%** ↑ CS Pass rate improvement


About this study

Bitsight leveraged its internet-wide telemetry of organizations and entity mapping techniques to conduct this study. Bitsight non-intrusively collects unique telemetry into the cybersecurity performance of organizations around the globe, and uses it to create analytics that measure performance over time. The Bitsight Security Rating measures an organization's overall cybersecurity performance. Bitsight risk vectors measure an organization's performance in particular cybersecurity domains (e.g. patching cadence, software updating practices, etc.).

Bitsight and Google collaborated to invent a methodology to measure organizational cybersecurity performance using Bitsight analytics across a specific security checklist, the Minimum Viable Secure Product (MVSP) framework, and to communicate the findings and relevant context to the public. Google played a key role in validating the statistical approach employed in this analysis, including the reasonable mapping of Bitsight telemetry to MVSP controls. Bitsight was not given access to any data owned by Google.


Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES



BITSIGHT