BITSIGHT | Google

WHITE PAPER

Studying Organizational Performance:

Minimum Viable Secure Product (MVSP) Framework

Table of Contents

Organizations continue to struggle with cybersecurity. Cyber vulnerabilities are on the rise, malware incidents continue, and organizations remain exposed to unorthodox risks and threats in cyberspace. These risks have resulted in business disruption, financial loss, reputational harm, and generally add first- and third-party risk to organizations.

Amid heightened interest in cybersecurity disclosure and performance measurement, the private sector is opting to implement its own vision of a security baseline. Organizations are taking it into their own hands to ensure the security posture of their third-party providers. As such, business executives and members of the board are asking how they can better inform their cybersecurity strategies. Across which security controls are organizations improving, and what is the current status of performance across key controls and across industries? This white paper addresses these important questions that security professionals, board members, and executives are all asking.

Cybersecurity Frameworks Aiming to Increase Trust

One framework is the Minimum Viable Secure Product (MVSP) framework, backed by Google, Salesforce, Okta, and others. MVSP is a minimalistic security checklist for B2B software and business process outsourcing suppliers. The goal of this checklist is to ensure that all companies building B2B software or otherwise handling sensitive information adhere to a minimally viable security posture for their product.

What is the MVSP Framework and how does it Help Create Trust?

MVSP consists of 25 controls across four key areas:
Business, Application Design, Application Implementation, and Operational.

MVSP Control Name	Control #
Business controls	
Vulnerability reports	1.1
Customer testing	1.2
Self-assessment	1.3
External testing	1.4
Training	1.5
Compliance	1.6
Incident handling	1.7
Data handling	1.8
Application Design controls	
Single Sign-On	2.1
HTTPs-only	2.2
Security Headers	2.3
Password policy	2.4
Security libraries	2.5
Dependency patching	2.6
Logging	2.7
Encryption	2.8
Application Implementation controls	
List of data	3.1
Data flow diagram	3.2
Vulnerability prevention	3.3
Time to fix vulnerabilities	3.4
Build process	3.5
Operational controls	
Physical access	4.1
Logical access	4.2
Subprocessors	4.3
Backup and Disaster recovery	4.4

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. If intercepted via a man-in-the-middle (MITM) attack, HTTP traffic can be read in plain text. Adopting an HTTPS-only approach can protect organizations from exposing sensitive information, as HTTPS traffic is encrypted and unreadable to an attacker in a position to MITM or observe traffic.

The MVSP framework increases trust between organizations by setting a baseline of security controls that promote a strong security posture.

Summary

The Good News

Notwithstanding there being concerns, organizations performed well across the majority of MVSP controls. **In 2023, every industry had a high Pass rate for 10 of the 16 MVSP controls we studied**. Every control with high Pass rates across all industries in 2023 also has low Fail rates, with the exception of the only two MVSP controls solely mapping to Patching Cadence, the Bitsight risk vector measuring an organization's vulnerability management program. For these two controls — [2.6] Dependency Patching and [3.4] Time to Fix Vulnerabilities — we observe both high Pass rates and high Fail rates across all industries.

What Stood out to Us

In particular, organizations performed very well (near-100% Pass rates and low Fail rates) across the four MVSP controls mapping to Bitsight's Security Incidents risk vector. This indicates that organizations generally protect themselves from what Bitsight calls Breach Security Incidents and General Security Incidents, although they may not perform well across controls critical in reducing the likelihood of a breach, like those mapping to Patching Cadence.

We were particularly surprised to see high Pass rates for [1.2] Customer Testing and [1.5] Training. The former is a step forward toward a safer third-party digital ecosystem, where organizations welcome customer testing of their applications and environments. This is especially important given the need for non-production data to stay out of production environments amid high-profile attacks targeting enterprise storage and transfer solutions.

High Pass rates for the latter control, [1.5] Training, is also an important development. Human error remains a popular way attackers compromise internal systems and access, steal, and exfiltrate sensitive data. Our research indicates that organizations are taking training efforts seriously, and we suspect this will continue yielding benefits.

Macro Improvements Underway

Macro[1] Fail rates declined from 2020 to 2023 across every control except [2.3] Security Headers, with similar results for the Computer Software (CS) industry. On the macro front, Fail rates for [2.6] Dependency Patching and [3.4] Time to Fix Vulnerabilities declined the most — marginally by nearly 4% — indicating that although many organizations are Failing these controls, improvement is underway. CS improved in this sense but at less than half the rate.

Industries are also improving Pass rates across key controls. We observed significant macro and CS improvements across [2.8] Encryption, [1.3] Self-assessment, [1.2] External testing, [3.3] Vulnerability Prevention, by as much as 25% marginally.

[1] 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 all industries are struggling with controls critical to the health of an organization's vulnerability management program. This represents an important issue amid a rising count of vulnerabilities, especially those considered "known exploited" by the United States Cybersecurity and Infrastructure Security Agency (CISA). 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:

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

But that's not the end of the story. Some controls with high Fail rates also had high Pass rates. 2.6 Dependency Patching and 3.4 Time to Fix Vulnerabilities are two of these controls, indicating that although many organizations Pass these controls, many others Fail the very same controls.

A Note on Security Headers

More organizations now, compared to 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).

We expected CS to outperform in most respects but that is not what we observed. CS's stagnation — and at times underperformance — may be attributed to many factors, including workforce challenges, rising asset inventories, lacking cybersecurity tools, and more. CS organizations tend to have more extensive IT footprints for which it is difficult to manage cyber risk.

How Bitsight Evaluated MVSP and Detailed Findings

The following sections illustrate our evaluation methods and findings in detail, explaining how we came to the conclusions described in the Summary section and more.

Methodology

Mapping Bitsight Risk Vectors to MVSP Controls

Bitsight measures the cybersecurity performance of organizations around the world, allowing it to help measure how organizations perform across MVSP controls. Performance spans 100,000 organizations from around the world and is based on 23 cyber risk vectors, including Patching Cadence, Desktop Software, Mobile Software, and more.

Bitsight mapped its risk vectors to 16 of the MVSP controls and reported performance in 2023 and over time, most recently considering March 2023. The 16 mappings are not unique in that some controls map to the same risk vectors. The complete mapping methodology is as follows:

MVSP Controls	Bitsight Risk Vectors	Mapping Category	Reasoning
1.1 Vulnerability reports 1.2 Customer testing	Patching Cadence, Server Software	Mapped to same risk vectors	Patching Cadence and Server Software provide evidence as to how many externally visible systems are affected by vulnerabilities and how quickly the company has resolved any issues (patches). They also record evidence of out-of-date versions (OS, Platform) within the network.
1.3 Self-assessment 1.4 External testing 3.3 Vulnerability Prevention	Desktop Software, DKIM, Insecure Systems, Mobile Application Security, Mobile Software, Open Ports, Patching Cadence, Server Software, SPF, TLS/SSL Certificates, TLS/SSL Configurations, Web Application Headers	Mapped to same risk vectors	Self-assessments, External testing and Vulnerability prevention efforts cover out-of-date versions of desktop software, email controls, mobile application development, encryption configurations, certificate management, service and port exposure, cross site scripting and other vulnerabilities for web applications.
2.6 Dependency Patching 3.4 Time to fix vulnerabilities	Patching Cadence	Mapped to same risk vectors	Patching Cadence provides evidence relevant to dependency and supersedence relationships between patches and Windows products, and between patches and other patches. It also measures the time to fix confirmed vulnerabilities.
1.7 Incident handling 1.8 Data handling 2.7 Logging 4.2 Logical access	Security Incidents	Mapped to same risk vectors	Security Incidents and Data Breaches provide evidence of security incidents that have been publicly disclosed and insight into incident management practices.
2.8 Encryption	TLS/SSL Certificates, TLS/SSL Configurations,	Mapped to unique risk vectors	SSL Certificates and SSL Configurations provide evidence about how data in transit is encrypted, indicating if industry standard testing and best practices are followed.
2.2 HTTPS-only	TLS/SSL Certificates, TLS/SSL Configurations, Web Application Headers	Mapped to unique risk vectors	SSL Certificates, SSL Configurations and Web Application Headers provide evidence about secure HTTP communications.
2.3 Security Headers	Web Application Headers	Mapped to unique risk vectors	Web Application Headers provides evidence as to how an organization is maintaining HTTP Security headers, as well as preventing cross site scripting (XSS) and other vulnerabilities.
2.5 Security libraries	Botnet Infections, Malware Servers, Open Ports, Potentially Exploited, Spam Propagation	Mapped to unique risk vectors	These risk vectors cover compromised endpoints and provide evidence of missing, misconfigured, or out-of-date anti-virus and/or anti-malware, as well as security-related design and implementation flaws.
1.5 Training	Botnet Infections, File Sharing, Malware Servers, Unsolicited Communications, Potentially Exploited, Spam Propagation	Mapped to unique risk vectors	These risk vectors provide evidence of how users are trained to interact with phishing attacks, infections and adware.

Performance Metrics

An organization's performance on an MVSP control is equal to the weighted sum of its performance across the Bitsight risk vectors to which the control is mapped, using the same risk vector weights as the Bitsight headline rating algorithm. More rigorously:

For an MVSP control mapped to n risk vectors and an organization in the p_i percentile for risk vector R_i, we compute the MVSP control score as:

$$Score = \sum_{i=1}^{n} w_i p_i$$

Where w_i is the normalized weight of R_i with Bitsight Security Rating weight W_i, and where W_j is the Bitsight Security Rating weight for the jth risk vector from R_i to R_n. We compute the normalized weight, w_i, to:

$$w_i = \frac{W_i}{\left(\sum_{j=1}^{n} W_j\right)}$$

Scores are then mapped to one of three grades, as follows:

Score	Grade
90-100	Pass
40-90	Needs Improvement
Less than 40	Fail

The following sections illustrate our evaluation methods and findings in detail, explaining how we came to the conclusions described in the Summary section and more.

Detailed Findings

We studied performance across 16 MVSP controls for nine industries:

- Computer Software
- Automotive
- Banking
- Energy/Resources
- Hospital & Healthcare
- Insurance
- Media/Entertainment
- Pharmaceuticals
- Retail

We then considered the percentage of organizations in each industry earning each grade for each control as a way to understand industry performance. For example, X% 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.

Performance in 2023 is Mixed

Industry performance is rather homogeneous in 2023 such that each industry has roughly the same rate of Pass, Needs Improvement, and Fail grades for a given control under measurement. A rate is considered high if it is above the average of that rate (Pass, Needs Improvement, or Fail) across all controls and industries. With limited exceptions, here's an overview of the results applying to all industries:

THE GOOD

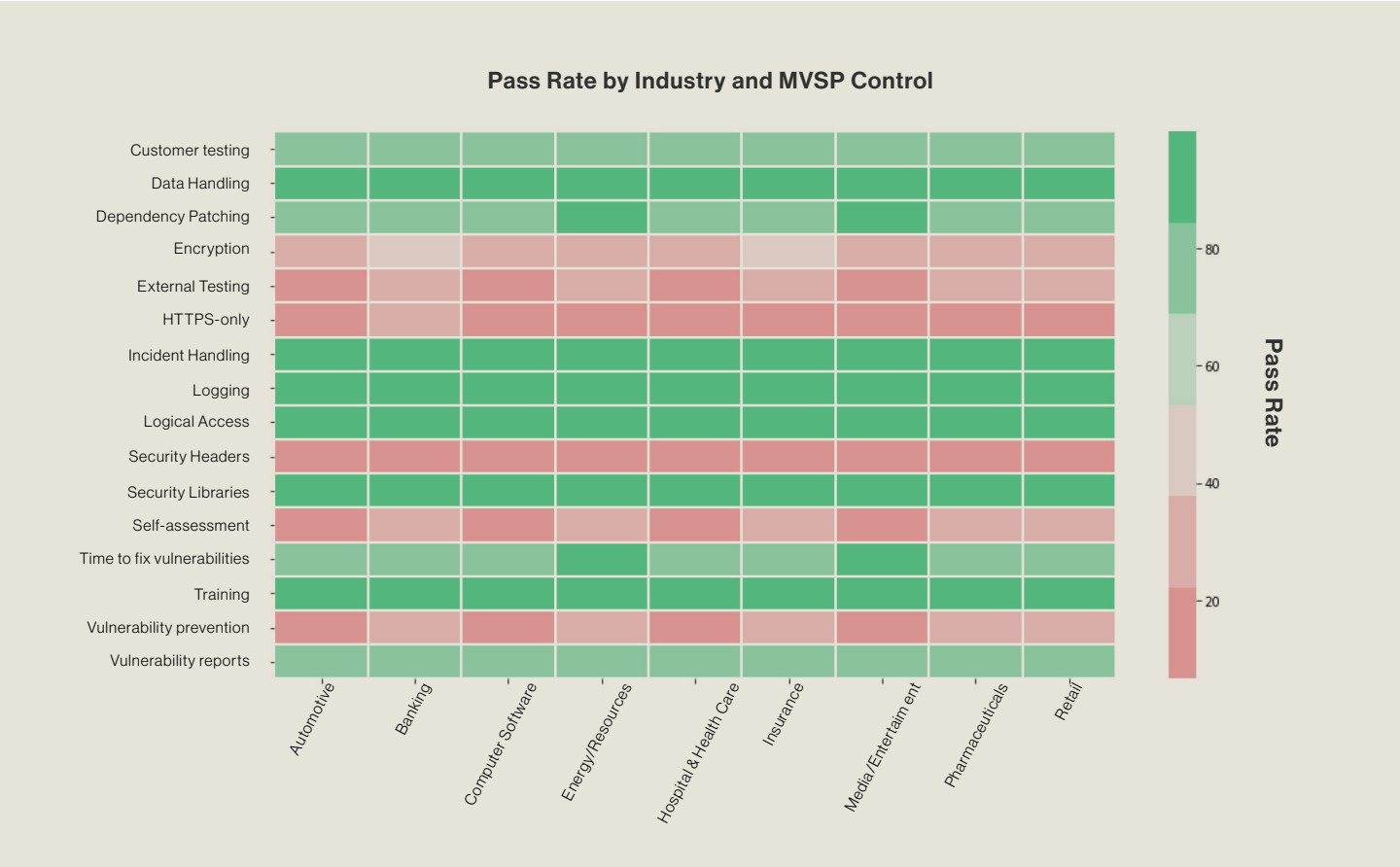
1. Near-100%Pass rates

- [1.8] Data Handling[2]
- [1.7] Incident Handling[2]
- [2.7] Logging[2]
- [4.2] Logical Access[2]

[2] These MVSP controls map to the same Bitsight risk vector (Security Incidents).

2. High Pass rates, in addition to controls under “Near-100% Pass rates”

- 1.2 Customer Testing[3]
- 1.1 Vulnerability Reports[3]
- 2.6 Dependency Patching[4]
- 3.4 Time to Fix Vulnerabilities[4]
- 2.5 Security Libraries
- 1.5 Training



3. Low Fail rates

In addition to the controls under “Near-100% Pass rates:”

- 1.2 Customer Testing
- 1.1 Vulnerability Reports
- 1.4 External Testing[5]
- 1.3 Self-assessments[5]
- 3.3 Vulnerability Prevention[5]
- 2.5 Security Libraries
- 1.5 Training

The Fail rate for all industries is less than 25% across all controls, except for 2.3 Security Headers, where the Fail rate exceeds 25% for all industries except banking.

[3]These MVSP controls map to the same Bitsight risk vectors (Patching Cadence, Server Software).
[4]The above MVSP controls map to the same Bitsight risk vector (Patching Cadence).
[5]These MVSP controls map to the same Bitsight risk vectors (Desktop Software, DKIM, Insecure Systems, Mobile Application Security, Mobile Software, Open Ports, Patching Cadence, Server Software, SPF, TLS/SSL Certificates, TLS/SSL Configurations, Web Application Headers).

Share of Organizations Receiving each Grade by Industry and MVSP Control

Share of Organizations Receiving each Grade by Industry and MVSP Control

4. Low rates of Needs Improvement

In addition to the controls under "Near-100% Pass rates:"

- [1.2] Customer Testing
- [1.1] Vulnerability Reports
- [2.6] Dependency Patching
- [3.4] Time to Fix Vulnerabilities
- [2.5] Security Libraries
- [1.5] Training

AREAS FOR IMPROVEMENT

1. Low Pass rates

- [1.4] External Testing
- [1.3] Self-assessment
- [3.3] Vulnerability Prevention
- [2.8] Encryption
- [2.2] HTTPS-only
- [2.3] Security Headers

2. High Fail rates

- [2.6] Dependency Patching
- [3.4] Time to Fix Vulnerabilities
- [2.2] HTTPS-only
- [2.3] Security headers
- [2.8] Encryption

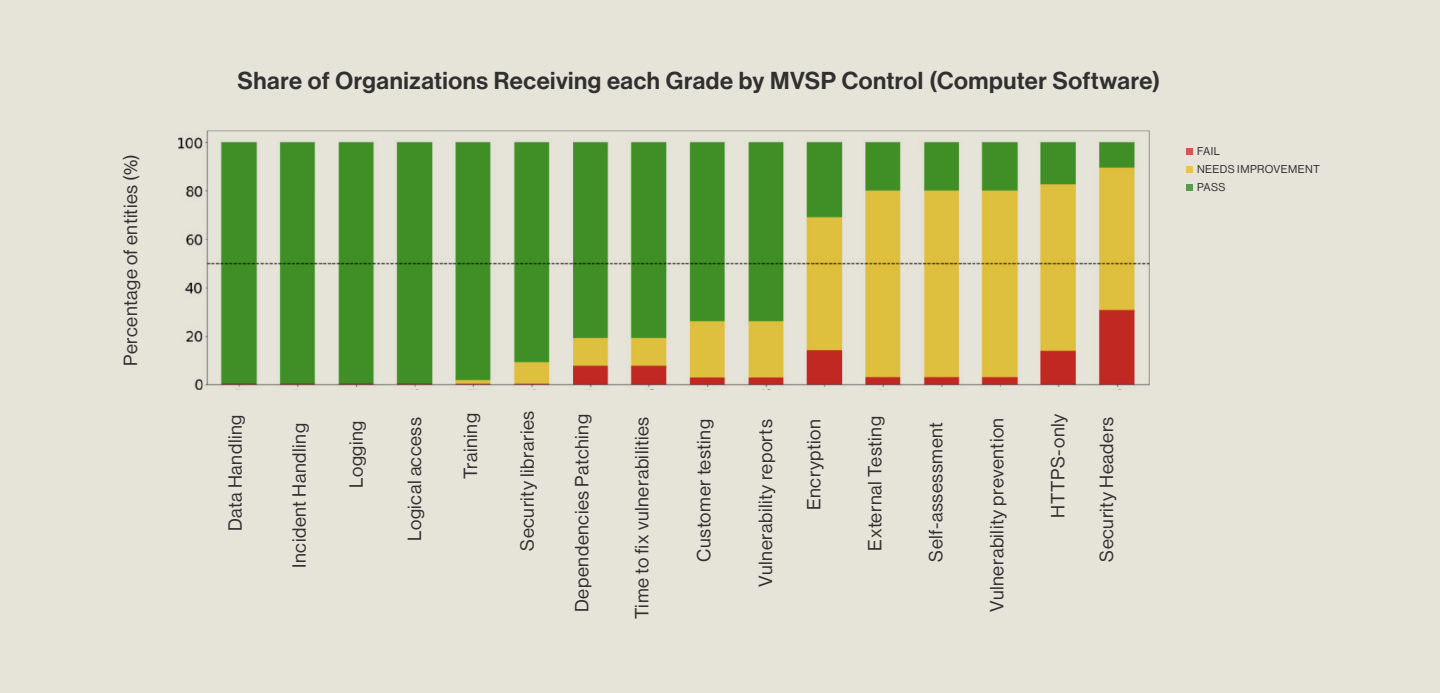
3. High rates of Needs Improvement

More than 50% of organizations across all industries in 2023 were graded as Needs Improvement for the following MVSP controls:

- [1.4] External Testing
- [1.3] Self-assessment
- [3.3] Vulnerability Prevention
- [2.2] HTTPS-only
- [2.3] Security headers
- [2.8] Encryption

COMPUTER SOFTWARE PERFORMANCE IN 2023 SIMILAR TO OTHER INDUSTRIES

Let's examine a snapshot of the CS industry's performance in 2023. Each industry looks very similar to this breakdown, with the exception of Banking, which boasts a higher Pass rate and lower Fail rate for [2.2] HTTPS-only and [2.3] Security Headers; and a higher Pass rate for [1.3] Self-assessment and [3.3] Vulnerability Prevention.



But as little difference as there is in 2023 between CS and all other industries, there are some stark differences between the two when considering changes from 2020 to 2023.

Organizational Performance over Time

We measured the net change from 2020 to 2023 in Pass and Fail rates across all industries but CS, and for CS alone. We refer to the former rates as "macro" rates. What we found surprised us.

MACRO PERFORMANCE

Macro improvements were broad, with consistent declines in Fail rates and increases in Pass rates.

Pass Rates

Computing the differences between average Pass rates for each control from 2020 to 2023, we found that Pass rates improved for every single control, sometimes by as much as 25 marginal percentage points. The largest marginal improvements were identified in the following controls:

- 1.4 External Testing (+ 17%)
- 1.3 Self-assessment
- 3.3 Vulnerability Prevention
- 2.8 Encryption (+ 25%)
- 2.2 HTTPS-only (+ 14%)

Fail Rates

For our macro average, all Fail rates declined from 2020 to 2023 across all but one control, indicating broad improvement with one exception. The Fail rate for 2.3 Security Headers rose by a marginal 11%, indicating a relatively high increase. The largest marginal declines in Fail rate were observed across the following controls:

- 3.4 Time to Fix Vulnerabilities (- 4%)
- 2.6 Dependency Patching
- 1.1 Vulnerability Reports (- 3%)
- 1.2 Customer Testing
- 2.8 Encryption (-2%)

Macro Marginal Net Change (2020-2023)

MVSP Control	Fail	Pass
1.2 Customer testing	-3.18	9.13
1.8 Data Handling	-0.19	0.08
2.6 Dependency Patching	-3.84	8.27
2.8 Encryption	-2.27	25.25
1.4 External testing	-1.09	16.87
2.2 HTTPS-only	-1.93	14.16
1.7 Incident handling	-0.19	0.08
2.7 Logging	-0.19	0.08
4.2 Logical access	-0.19	0.08
2.3 Security Headers	11.28	2.52
2.5 Security libraries	-0.39	6.34
1.3 Self-assessment	-1.09	16.87
3.4 Time to fix vulnerabilities	-3.84	8.27
1.5 Training	-0.22	2.83
3.3 Vulnerability prevention	-1.09	16.87
1.1 Vulnerability reports	-3.18	9.13

COMPUTER SOFTWARE PERFORMANCE VS. MACRO IMPROVEMENTS

Fail Rates

For controls critical to vulnerability management, we observed CS lagging behind macro[6] improvements in Fail rates. CS Fail rates for 2.6 Dependency Patching and 3.4 Time to Fix Vulnerabilities did not improve as much as the macro average; however, CS's Fail rate for 2.3 Security Headers rose by less than the macro average.

Underperformance in Controls Critical to Vulnerability Management

We were surprised that CS Fail rates — an industry we expected to be the leader in improvements — lagged behind macro improvements in controls critical to vulnerability management. 2.6 Dependency Patching and 3.4 Time to Fix Vulnerabilities map to the same Bitsight risk vector, Patching Cadence, which is a measure of an organization's vulnerability management program. Patching Cadence is a critical element of an organization's vulnerability management program.

All other changes in CS Fail rates are largely consistent with macro changes.

Pass Rates

For Pass rates, all industries (less CS) and CS experienced universally positive changes; from 2020 to 2023, we observed Pass rates rising. However, **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). The controls where CS lagged its peers the most are:

- 1.4 External Testing (-3%)
- 1.3 Self-assessment
- 3.3 Vulnerability Prevention
- 1.1 Vulnerability Reports (-2%)
- 1.2 Customer Testing
- 2.5 Security Libraries (-3%)
- 2.2 HTTPS-only (-2%)

Computer Software Marginal Net Change (2020 - 2023)

MVSP Control	Fail	Pass
1.2 Customer testing	-2.78	7.13
1.8 Data Handling	0.01	0.03
2.6 Dependency Patching	-1.47	6.64
2.8 Encryption	-2.16	21.03
1.4 External testing	-0.71	14.13
2.2 HTTPS-only	-1.38	11.74
1.7 Incident handling	0.01	0.03
2.7 Logging	0.01	0.03
4.2 Logical access	0.01	0.03
2.3 Security Headers	10.25	2.90
2.5 Security libraries	-0.21	3.80
1.3 Self-assessment	-0.71	14.13
3.4 Time to fix vulnerabilities	-1.47	6.64
1.5 Training	-0.16	1.73
3.3 Vulnerability prevention	-0.71	14.13
1.1 Vulnerability reports	-2.78	7.13

Difference between CS and Macro Rates

MVSP Control	Fail	Pass
1.2 Customer testing	0.40	-2.00
1.8 Data Handling	0.20	-0.05
2.6 Dependency Patching	2.37	-1.63
2.8 Encryption	0.11	-4.22
1.4 External testing	0.38	-2.74
2.2 HTTPS-only	0.55	-2.42
1.7 Incident handling	0.20	-0.05
2.7 Logging	0.20	-0.05
4.2 Logical access	0.20	-0.05
2.3 Security Headers	-1.03	0.38
2.5 Security libraries	0.18	-2.54
1.3 Self-assessment	0.38	-2.74
3.4 Time to fix vulnerabilities	2.37	-1.63
1.5 Training	0.06	-1.10
3.3 Vulnerability prevention	0.38	-2.74
1.1 Vulnerability reports	0.40	-2.00

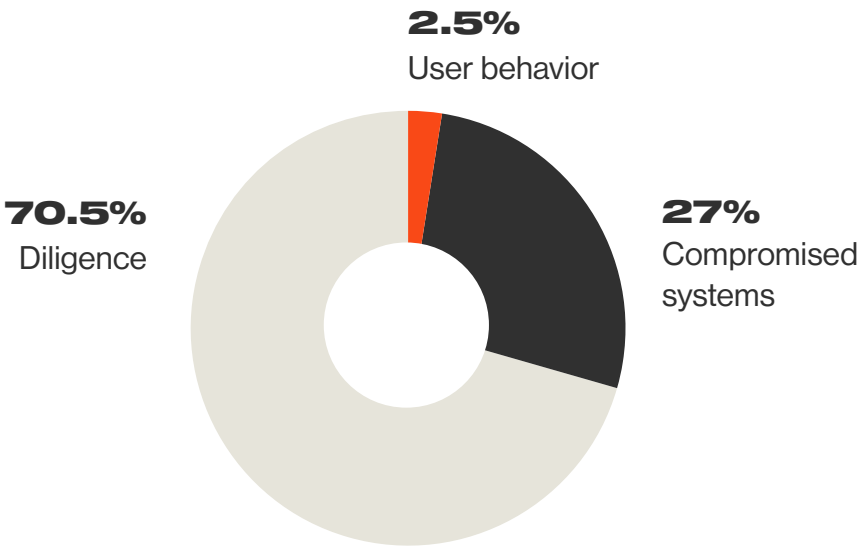
Fail: negative values are good | **Pass:** positive values are good.

[6] The above "Macro" refers to the average rate for a control across all industries except for CS.

Bitsight Ratings Methodology

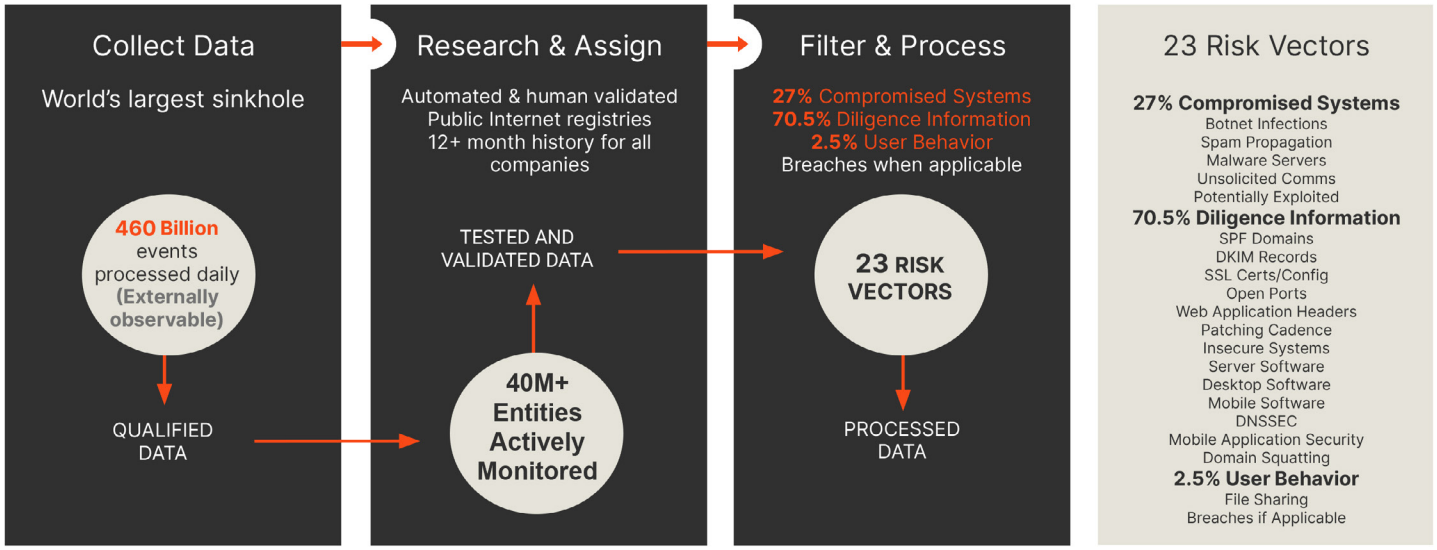
The Bitsight Security Rating is based on 23 weighted risk vectors, including Patching Cadence, Botnet Infections, and more. The risk vectors are organized into three main categories – Diligence, Compromised Systems, and User Behavior.

What makes a Security Rating?



Breaches have a negative impact on Security Ratings only if they occur

The process of collection to processing is as follows:



Each risk vector is weighted according to the below chart, with risk vectors associated with Diligence heavily weighted in the Rating. Due to Patching Cadence's high correlation with cybersecurity incidents — including ransomware and breach — this risk vector is weighted at 20%.

Compromised Systems	Botnet Infections	27%	
	Spam Propagation		
	Malware Servers		
	Unsolicited Communications		
	Potentially Exploited		
Diligence	SPF Domains	-2.78	70.5%
	DKIM Records	0.01	
	Mobile Software	-1.47	
	Server Software	-2.16	
	Insecure Systems	-0.71	
	Desktop Software	-1.38	
	Web Application Headers	0.01	
	Open Ports	0.01	
	TLS/SSL Certificates	0.01	
	TLS/SSL Configurations	10.25	
	Patching Cadence	-0.21	
User Behavior	File Sharing	27%	

Contributors

Noah Stone, Senior Manager, Bitsight (Author)
Moctar Sankara, Data Analyst, Bitsight (Analyst)
Chris John Riley, Staff Security Engineer, Google (Co-author)
Dirk Göhmann, Technical Writer, Google (Co-author)

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