RESEARCH REPORT

Japan's Nikkei 225 Index:

The State of Cybersecurity in Japan

Security Scorecard

Contents

Introduction

This research presents an analysis of the cybersecurity landscape of the **Nikkei 225** index. Companies were ranked based on various factors, such as network security, potential malware exploits, and patching cadence.

To measure cyber risk, SecurityScorecard delivers standardized "A to F" letter grades that measure and validate organizations' security posture and supply chains in real time. Validation of SecurityScorecard scores using statistical analysis demonstrates that companies with an F rating have a 13.8x greater likelihood of a data breach than companies with an A.

Key Findings

While Nikkei 225 companies generally perform well, SecurityScorecard found that **30% have cybersecurity scores that are a C — and 7% earned failing grades of a D or F.**

- 63% of **Nikkei 225** companies received high cybersecurity ratings (A or B), 30% scored a C, and 7% received failing grades (D or F).
- **Transportation companies** demonstrated the lowest ratings, with 47% at a C or below.
- **Financial companies excelled** with only 10% with a C or below.
- 10 companies in the **Nikkei 225** experienced a domain hack in the last year - 9 of which were in the **manufacturing sector**.
- **Utility companies** experienced the most third-party breaches (100%) while manufacturing companies had the fewest (83%).
- Notably, 40 companies with an A grade remained breach-free over the past year.

The Nikkei 225 Cyber Threat Landscape

Nikkei 225 companies and institutions face the perpetual threat of cyberattacks, and recent global events only serve to heighten their risk. Attackers are often more aware of a company's vulnerabilities than the company itself, which makes security assessments crucial.

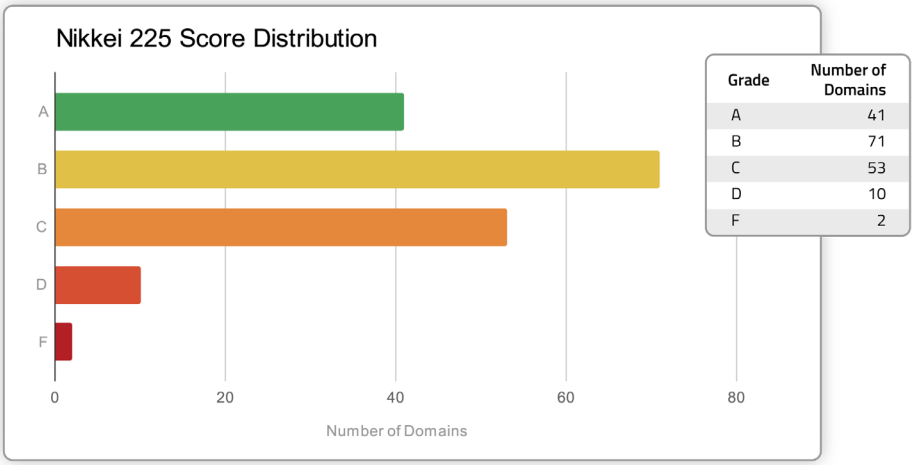
Our cybersecurity study among firms in the **Nikkei 225** clearly shows areas for improvement. This report examined companies in the following sectors: financial, manufacturing, healthcare, utilities, and transportation.

Results

Overall scores

Overall, 63% of companies in the index received the highest cybersecurity ratings — an A or B. However, 30% of companies had an average performance, scoring a C, and 7% of the **Nikkei 225** failed outright — earning a D or F.

SecurityScorecard Cybersecurity Ratings can be compared to financial credit ratings. Just as a poor credit rating is associated with a greater probability of default, a poor cybersecurity rating is associated with a higher probability of sustaining a data breach or other adverse cyber event.



Grade	Number of Domains
A	41
B	71
C	53
D	10
F	2

Supply chain risks extend beyond third parties

While third parties typically receive most of the supply chain scrutiny, fourth-party vendors also create significant risk. SecurityScorecard research shows that 83% of companies in the manufacturing sector had a domain affected by a third-party breach, and 85% had a domain affected by a fourth-party breach. This threat highlights the importance of identifying and assessing the security posture of all of the companies that serve third-party vendors to avoid incidents.

The importance of securing critical infrastructure

This research shows that 47% of transportation companies scored a C or below, and 100% of utility companies experienced a third-party breach. These companies make up part of the national critical infrastructure, which is the backbone of society. For society to function, the public needs to trust that these services and institutions are safe. Companies in these sectors would benefit from the recommendations below. For further guidance and best practices, please read SecurityScorecard's 2023 report, "Addressing the Trust Deficit in Critical Infrastructure."

Recommendations

For many **Nikkei 225** companies, cybersecurity improvement should be a top priority. While 63% of companies in the index received high cybersecurity ratings (A or B), 30% scored a C, and 7% faced failing grades (D or F). To mitigate risk and enhance overall cybersecurity posture, we recommend the following actions:

Focus on application and network security: All Nikkei 225 companies should prioritize improving application and network security. These two aspects are fundamental to safeguarding against a wide range of cyber threats.

High-Risk Companies: The 7% of **Nikkei 225** companies with failing scores require urgent attention. In addition to improving application security and network security, these high-risk companies should place special emphasis on:

- **DNS Health:** Ensure the health and integrity of your Domain Name System (DNS) configurations. Misconfigurations in this critical component can lead to vulnerabilities.
- **Endpoint Security:** Strengthen the security of all endpoints, including laptops, desktops, mobile devices, and BYOD devices. Identifying and addressing vulnerabilities in these endpoints is crucial.
- **Patching Cadence:** Establish a consistent and timely patching cadence for your systems, software, and hardware. Frequent updates help mitigate known vulnerabilities.

We recommend that the 12 high-risk companies undergo a thorough evaluation to identify and mitigate weaknesses.

Regardless of the score, all **Nikkei 225** companies need to know not only their score, but the factors that influence it. Any **Nikkei 225** company can obtain a detailed report on their score for free from SecurityScorecard.

Conclusion

Trust and transparency are paramount in cybersecurity. Nevertheless, many organizations struggle to assess their cybersecurity precisely. Our analysis of the Nikkei 225 index underscores the critical significance of these principles.

Cybersecurity assessment is an ongoing process. Security Ratings empower cybersecurity leaders with the insights they need to make well-informed decisions, fortify their security posture, and foster collaboration in the face of an escalating risk.

Amidst the evolving threat landscape, Security Ratings and third-party monitoring tools stand as a proactive commitment to cybersecurity. We firmly believe that every Nikkei 225 company has the potential to attain cybersecurity resilience and contribute to a safer, more collaborative world.

Methodology

A dynamic threat landscape requires real-time risk assessment. Cyber risk must be evaluated based on up-to-the-minute data. SecurityScorecard gathers significant amounts of non-intrusive data on the cybersecurity performance of companies around the world. Using this data, we're able to score companies' cyber defenses. We produce an overall score, graded A-F, based on ten factors that are predictive of a security breach.

Analysis Period: The report covers the cybersecurity posture of **Nikkei 225** companies from November 20, 2022, to November 20, 2023.

What are Security Ratings?

SecurityScorecard provides organizations with a comprehensive view of security posture for companies, including third- and fourth-party risk.

Security Ratings are entirely evidence-based; everything is scored on an underlying and transparent observation, based on scans of the entire IPv4 space. Correlated with incidence data, SecurityScorecard factors provide insight that can help organizations focus on areas that need the most attention to reduce their risk exposure. Here are the ten factors:

Network Security checks for open ports (such as SMB and RDP), insecure or misconfigured SSL certificates, database vulnerabilities, and IoT vulnerabilities.

DNS Health checks for misconfigurations, such as Open Resolvers, and checks for recommended configurations for DNSSEC, SPF, DKIM, and DMARC.

Patching Cadence measures the frequency of updates for an organization's identified services, software, and hardware.

Endpoint Security measures the versions and exploitability of laptops, desktops, mobile devices, and BYOD devices that access an organization's networks.

IP Reputation signals are collected by SecurityScorecard's sinkhole system, which ingests millions of malware signals from commandeered Command and Control (C2) infrastructures from all over the world. Identified infected IP addresses are mapped back to impacted organizations.

Hacker Chatter is collected from underground and dark web locations discussing targeted organizations and IP addresses.

Information Leak consists of compromised credentials that have been exposed as part of a data breach or leak, keylogger dumps, pastebin dumps, database dumps, and other information repositories.

Social engineering involves measuring the use of corporate accounts in social networks, financial accounts, and marketing lists.

Cubit Scores are calculated using SecurityScorecard's proprietary threat algorithm that measures a collection of critical security and configuration issues, such as exposed administrative control panels.

About SecurityScorecard

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating.

For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1707
International: +1(646) 809-2166