REPORT

The Middle East's Top 100 Companies:

Cybersecurity Threat Report

SecurityScorecard

Introduction

Critical Infrastructure is one of the most valuable and vulnerable areas in the Middle East's economy with persistent attacks on these systems potentially having a catastrophic impact on national security and economies. With growing unrest in parts of the region, it is more important than ever that companies implement strong security measures. To examine the risks in this area, our report analyzes the cybersecurity of the top 100 companies in the Middle East by market capitalization over the last year.

As the saying goes, "What you can't measure, you can't improve." Years after the ransomware attack that disrupted the Colonial Pipeline, there is still no standard framework for measuring cyber risk. This gap leaves organizations uncertain about their cybersecurity posture and how to address vulnerabilities effectively. SecurityScorecard fills this void with an A-to-F rating system based on continuous threat intelligence data, providing an instant snapshot of a company's cybersecurity status.

Just as a poor credit rating signals a higher risk of default, a poor cybersecurity rating indicates a greater likelihood of a data breach or other cyber incident. This is crucial: companies with an F rating are 13.8 times more likely to face a breach compared to those with an A. In today's world, a low cybersecurity score poses risks comparable to a poor credit rating.

Financial entities such as banks, insurance companies, and investment firms will all need to ensure that the Middle Eastern financial sector is able to maintain and monitor resilience during severe third-party operational disruptions.

Coupled with the EU's Digital Operational Resilience Act (DORA) deadline looming on 17th January, 2025, all financial companies looking to do business in Europe face an urgent cybersecurity challenge. Despite the high stakes, many organizations lack effective ways to measure their risk, effectively leaving them exposed and 'flying blind.'

Companies with an A rating are

13X LESS LIKELY

to suffer a cyber incident than those with an F

Key Findings:

SecurityScorecard evaluated the Middle East's top 100 companies based on critical cybersecurity factors such as network security, malware infections, endpoint security, patching cadence, application security, and DNS health. The findings reveal significant vulnerabilities:

- Only **2%** have suffered a direct breach in the last year (compared to **18%** of European companies)
- Only **14%** had a C rating or below (the average for Europe is 36%)
- Only **19%** of the top 25 companies by market cap have a rating of C or below and **5%** of the bottom 25 companies
- The Utilities sector is the strongest, with all companies scoring a B or higher, unlike the Telecommunications sector, where 86% had a C rating or below
- **84%** had a breach in their third-party ecosystem in the last year (less than Europe at 98%)
- **84%** had a breach in their fourth-party ecosystem in the last year
- **100%** of the Middle Eastern companies with an A grade have not been breached in the last year (demonstrating the importance of having an A grade)

Results

Overall scores

1. **29%** received an A
2. **51%** received a B
3. **16%** received a C
4. **2%** received a D
5. **2%** received an F

Grade	Breach Likelihood
A	1x
B	2.9x
C	5.4x
D	9.2x
F	13.8x

The average global cost of a data breach is $4.5M.

IBM Security, Cost of Data Breach Report 2023

Sector Overview

Supply chain cyber risk

Supply chain vulnerabilities provide an easy entry point for adversaries to access organizations and networks. No matter how much organizations invest in security, they remain only as secure as their weakest link. This means even well-protected companies face risks from third- and fourth-party weaknesses.

Previous SecurityScorecard research found that 98% of companies have a relationship with a third party that has been breached. In this report, sectors with the lowest security ratings have the most complex attack surfaces due to the sheer number of their third, fourth, and nth party vendors.

> "The supplier ecosystem is a highly desirable target for ransomware groups. Third-party breach victims are often not aware of an incident until they receive a ransom note, allowing time for attackers to infiltrate hundreds of companies without being detected. Governments worldwide are set to enforce stricter security regulations in 2025 that place accountability on organizations and their suppliers, demanding higher security standards across the board making monitoring and understanding a company's flaws will become essential."
>
> - **Ryan Sherstobitoff**
> **Senior Vice President of Threat Research and Intelligence**

Utilities

The Utilities sector stands out as the most secure in the Middle East, with no companies scoring a C rating or lower. Coupled with the lack of direct breaches in the last year, it demonstrates a very strong cybersecurity posture in the sector.

Energy

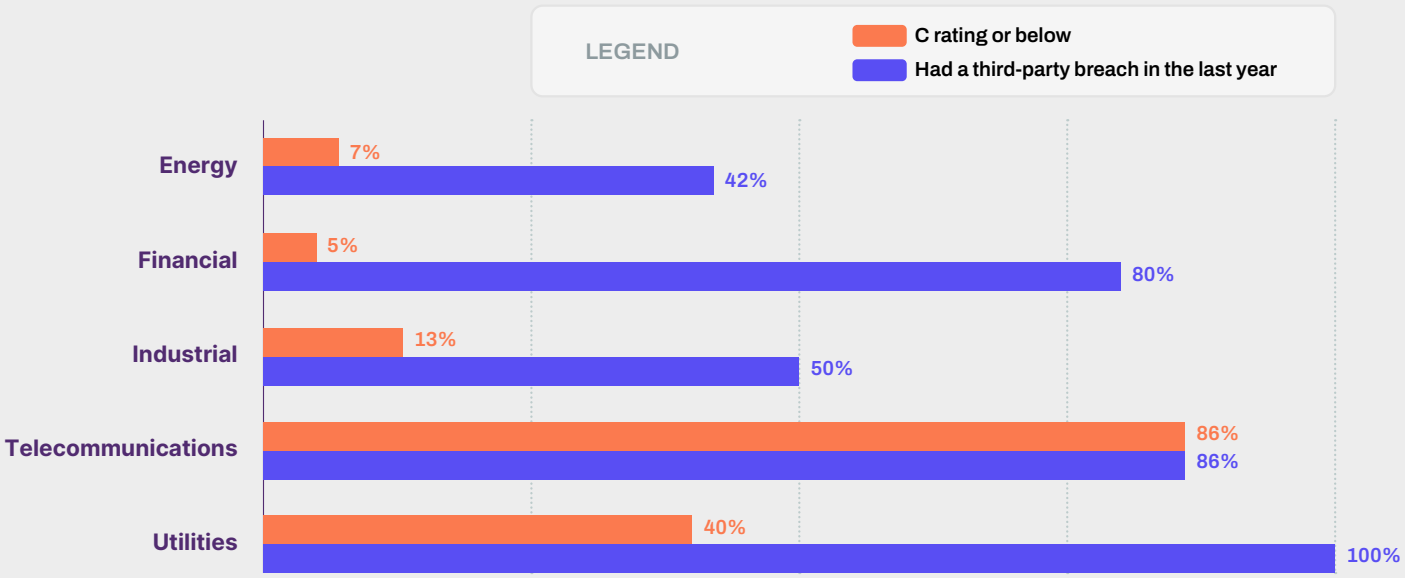
The energy sector has strong overall security ratings, with only 7% receiving a C rating or below. This is expected, given the significant economic value tied to the sector. In comparison, 75% of energy companies in Europe had a C rating or below, highlighting the Middle East's stronger security posture. Notably, none of the energy companies in the Middle East experienced direct breaches in the past year.

The Energy sector is an integral part of critical infrastructure making them a prime target for nation-state attacks and other threat actor groups. The energy sector's growing dependence on third-party vendors highlights a critical vulnerability — its security is only as strong as its weakest link. Our recent Energy research shows that this rising reliance poses significant risks. 67% of North American Energy Sector breaches were linked to software and IT vendors. It's time for the industry to take decisive action and strengthen cybersecurity measures before a breach turns into a national emergency.

Telecommunications

The telecommunications sector is the weakest in the Middle East, with 86% receiving a C rating or below, compared to 33% in Europe. This industry faces particularly complex attack surfaces due to its extensive networks of third-party vendors, partners, and service providers.

Scores by Sector



Score comparison by region

Cybersecurity challenges go beyond national borders and individual networks, making it a global issue. Collaboration between governments, industries, and organizations is essential to strengthen collective defense.

This report examines the top 100 companies in the Middle East, with comparisons to past analyses of European companies. The Middle East showed stronger cybersecurity overall, with only 14% rated C or below, compared to 36% of Europe's top 100 companies.

SecurityScorecard's recently released Global Third-Party Cybersecurity Breach Report underscores why these findings are so pressing. The report reveals that 75% of third-party breaches target the software and technology supply chain, a trend reinforced by recent high-profile breaches involving SolarWinds, Log4j, and MOVEit.

Cyber risk concentration: A growing concern

According to the Global Cyber Resilience Scorecard, ten threat actor groups are responsible for 44% of global cyber incidents—with the C10p cybercrime group being the most prolific perpetrator of third-party breaches.

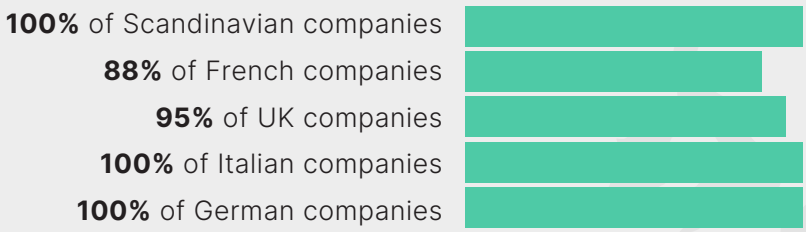
The fact that a few groups are behind such significant disruptions raises serious concerns about concentrated risk in the global economy. "Redefining Resilience: Concentrated Cyber Risk in a Global Economy," with knowledge contributions from McKinsey and Company, looked at this very issue. A striking finding is that just 15 companies dominate 62% of the global technology market.

Because of their large influence, these companies have greater potential to inflict third-party harm on their customers due to their extremely large market share and vast attack surfaces. These vulnerabilities are the root of many recent, high-profile supply chain attacks that have crippled critical industries. One example of this is the cyberattack on Change Healthcare, a major medical claims processor in the United States. The February 2024 attack forced Change Healthcare to disconnect over 100 systems, pushing many providers to the brink of closure.

Benchmarking across Europe

Top 100 Companies breached in the last year

Companies with an A grade that have not been breached in the last year



Companies with a breached entity in their third-party ecosystem

"The scale and value of the Middle East's energy and financial sectors cannot be underestimated globally and requires a very robust cybersecurity protocol, not least because of mounting unrest in parts of the region. The urgency for harmonization has reached a tipping point. In response to mounting challenges, there will be a growing push for greater regulatory harmonization in 2025. Governments, international organizations, and industry bodies will unite to create consistent standards and frameworks that can be adopted globally, particularly among the United States, Canada, Australia, and across Europe.

Third-party risk management is a key component of any robust cybersecurity program, and the companies represented in this report would benefit by making it a priority. The sectors and organizations in Europe (and in Europe as a whole) need to do more now if they are going to be ready for the implementation of DORA [Digital Operational Resilience Act] by January 2025 as well as the NIS2 directive.

"The rise of data breaches across Europe demonstrates that European companies need to make third-party risk management (TPRM) an integral component of not only their security program but of their vendor selection process as well.

SecurityScorecard can help with this effort by providing ratings to evaluate prospective vendors and monitor existing vendors to hold them accountable."

- Jeff Le
VP, Global Government Affairs & Public Policy at SecurityScorecard

Supply chain risk extends beyond third parties

While third parties typically receive most of the supply chain scrutiny, fourth-party vendors also create significant risk.

This report shows that 84% of the companies have a breached entity in their third-party ecosystem. Further analysis also shows that 84% of the Middle East's top companies have a breached entity in their fourth-party ecosystem. These threats underscore the importance of identifying and assessing the security posture of all Nth parties in a company's digital ecosystem.

The potential impact of these breaches is evident. The MOVEit exploit, discovered in spring 2023, primarily affected third- and fourth-party vendors, demonstrating how vulnerabilities in widely used software can disrupt entire supply chains. This incident continues to impact operations and impose financial strain, with projected costs exceeding $65 billion USD.

Further market capitalization insights

Our analysis shows that the top 50 companies by market capitalization (over $22 billion) have lower security ratings than the 50 companies with smaller market capitalization. On average, 19% of the highest-value companies have a C rating or below, compared to only 5% of lower-value companies with the same rating. This demonstrates that any company—regardless of size, industry, or revenue—can be a target for cybercriminals if its defenses are weak.

Globally, however, there appears to be a correlation between a country's cyber risk exposure and its GDP. The aforementioned Cyber Resilience Scorecard found that a nation's economic prosperity is closely tied to its ability to navigate the complex landscape of cyber threats.

The Middle East, North America, the Pacific, as well as Northern, Western, and Central Europe have the highest security scores in the world. In other words, regions with higher per capita GDP tend to exhibit better cybersecurity hygiene and lower cyber risk.

Securing critical infrastructure is key

A significant portion of the companies in this report are part of critical sectors such as utilities, telecommunications, transportation, and finance. Public trust in the safety of these essential services is vital for society to function seamlessly. Companies in these sectors should take note of the following recommendations to strengthen their cybersecurity posture. For more comprehensive guidance and best practices, refer to SecurityScorecard's 2023 report, "Addressing the Trust Deficit in Critical Infrastructure."

Recommendations

To reduce risks and strengthen cybersecurity stance, SecurityScorecard recommends the following actions for Middle Eastern organizations:

Focus on application and network security: Prioritize improving application and network security. These two aspects are fundamental to safeguarding against a wide range of cyber threats.

High-risk companies: The 41% of companies with cybersecurity ratings of a C or below 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.

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

Conclusion

Assessing cybersecurity accurately is a persistent challenge for many organizations. Our analysis of the top 100 companies in the Middle East highlights the importance of reliable security evaluations. Trust and transparency are essential for maintaining strong defenses, yet many companies struggle to gauge their true risk levels.

Security ratings play a key role in equipping cybersecurity leaders with the information they need to make better decisions and enhance their security measures. In an environment where cyber threats are growing in complexity, proactive measures like security ratings and third-party monitoring are critical for resilience.

The findings in this report show that every company, regardless of size or industry, can strengthen its cybersecurity posture. By prioritizing ongoing assessment and collaboration, these companies can better protect their operations and contribute to a safer digital ecosystem.

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.

The report covers the cybersecurity posture of the top 100 companies in the Middle East by market capitalization from 28th August 2023 to 28th August 2024.

Appendix

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.

To learn more and create your free account, visit SecurityScorecard.com

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.io