WHITEPAPER

United Arab Emirates Cybersecurity:

Supply Chain Threat Report

SecurityScorecard

Introduction

This research presents an analysis of the cybersecurity landscape of the top 30 companies in the United Arab Emirates (UAE) by revenue. Companies were ranked based on various factors, such as: **network security, potential malware infections,** 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.

BREACH LIKELIHOOD

Companies with an F rating have a

13.8X GREATER

likelihood of a data breach than companies with an A.

Key Findings:

While all companies in this data set demonstrate relatively strong cybersecurity, all of them have a relationship with a breached entity. A deeper dive into the data reveals:

1. **43%** have a cybersecurity score of A
2. **10%** have a cybersecurity score of a C or below
3. **73%** have a breached entity in their third-party ecosystem
4. **73%** have a breached entity in their fourth-party ecosystem

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

The cyber threat landscape of the UAE

Companies and institutions around the globe face the constant threat of cyberattacks, due to the growing attack surface, third and fourth parties, remote work, and the current geopolitical climate. Attackers are increasingly aware of organizations' vulnerabilities, which is why it's crucial for companies of all sizes and in all industries to conduct regular security assessments through the eyes of a hacker.

Our analysis of the top 30 companies in the UAE by revenue shows areas for improvement. This report looked at companies in the following sectors: energy, financial, manufacturing, transportation, utilities, and technology.

Results

Overall scores

1. **43%** of companies received the highest cybersecurity ratings — an A.

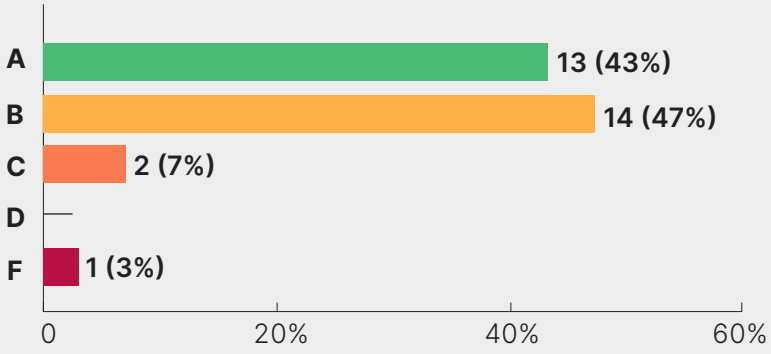
2. **47%** received a B score.

3. **10%** of these UAE companies have a C rating or below.

Notably, however, 43% of companies have an A cybersecurity rating and have not experienced a breach for a year. This group consists primarily of energy and financial firms.

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.

Top 30 UAE Companies Score Distribution



"Our data indicates that whilst the UAE's largest companies have respectable ratings, there have been large data leaks from their third party suppliers, demonstrating that more must be done to protect their cybersecurity supply chain. When it comes to security there can be no room for errors and our extensive knowledge as a leader in cyber risk ratings will be on display in Dubai this year."

Steve Cobb
CISO, SecurityScorecard

Cyber resilience linked to GDP

On the whole, the top 30 companies in the United Arab Emirates exhibit strong cybersecurity postures; this is in line with SecurityScorecard's recent research identifying a strong correlation between a country's cyber risk exposure and GDP. At the World Economic Forum in Davos this year, SecurityScorecard presented the Cyber Resilience Scorecard, which found that a nation's economic prosperity is closely tied to its ability to navigate the complex landscape of cyber threats.

According to the report, the Middle East, North America, the Pacific, as well as Northern, Western, and Central Europe have the highest security scores in the world. **Bottom line: regions with higher per capita GDP tend to exhibit better cybersecurity hygiene and lower cyber risk**. Considering that the UAE has one of the highest rankings of GDP per capita, it is presumably better equipped to invest in resilient and safe infrastructure and to implement and maintain active security programs to combat the ever-evolving nature of cyber threats. Wealthier countries such as the UAE may also be more likely to use licensed software that is kept up to date with security patches.

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 73% of these companies have a breached entity in their third-party ecosystem, and 73% have a breached entity in their fourth-party ecosystem. This threat highlights the importance of identifying and assessing the security posture of all Nth parties in a company's digital ecosystem.

Several of the companies analyzed in this report are holding companies with dozens of subsidiaries serving multiple sectors. Many of these industries — such as telecommunications, critical manufacturing, energy, and technology — are interconnected, resulting in a complex matrix of risk interdependencies that policy-makers and business executives around the world are attempting to address with laws, policies, and risk management strategies.

Securing critical infrastructure is key

More than half of the companies listed in this report (57%) represent critical sectors: energy, telecommunications, critical manufacturing, and healthcare. For society to function smoothly, 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."

"Third-party data breaches are a problem for many large organizations globally, but with clear guidance and the right cyber tools, they can be drastically reduced. SecurityScorecard is at the forefront of cyber risk assessment across the Middle East, offering comprehensive ratings that enable organizations worldwide to understand, improve, and communicate their cybersecurity posture and provide in-depth insights into the risk profile for critical suppliers."

Jan Bau
VP, EMEA

Recommendations

For many UAE companies, improving cybersecurity hygiene should be a top priority. Though the majority of companies received high cybersecurity ratings, nearly three quarters have experienced a third-party breach and the same number have experienced a fourth-party breach. To mitigate risk and enhance overall cybersecurity posture, we recommend the following actions:

Focus on application and network security: All 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 10% of companies in the UAE with cybersecurity ratings of a C or below require more 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.

Regardless of the score, 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

Trust and transparency are paramount in cybersecurity. Nevertheless, many organizations struggle to assess their cybersecurity precisely. Our analysis of the top companies in the UAE by revenue 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 solutions stand as a proactive commitment to cybersecurity. We firmly believe that every company in this analysis 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 the top UAE companies by revenue from 20 January 2023 to 20 January 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