



2023 UAE REPORT

# DATA RISK MANAGEMENT

The State of the Market—Cyber to Compliance



Research conducted by:



VansonBourne

# INTRODUCTION

The ability to manage risk is a foundation of a successful organization. Those that do it well can navigate choppy waters while their competitor's struggle. Recent years have seen a succession of heightened risks with contributing factors including a pandemic, geopolitical tensions, and economic turmoil. As a result, organizations are facing a barrage of risks from every conceivable angle. Those that manage them best are the most likely to succeed.

Individual countries and markets approach the topic of risk management differently. As do individual organizations and employee groups.

This report is part of a global research project, focusing on a subsection of 100 executives and practitioners in the United Arab Emirates.

**This report looks to answer the following questions:**

- What are the greatest risks that organizations face in the UAE today? How does this compare to the rest of the world?
- When it comes to data security, how have organizations in the UAE adapted to threats in recent history?
- Do organizations and their employees in the UAE believe themselves to be at risk? How does this translate into action?



# KEY FINDINGS



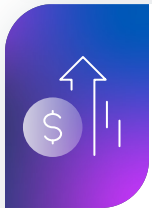
## Economic uncertainty and data security are the top risks for organizations in the UAE.

- Diverging from global trends, risks from economic uncertainty (**38%**) ranked highest for organizations in the UAE, followed by risks from data security (**37%**) and weak sustainability measures (**37%**).
- As a result of risks, **98%** of UAE organizations report actual damage, such as financial and reputational damage.



## The UAE has experienced more successful ransomware attacks than most markets.

- **73%** of organizations in the UAE have experienced a successful ransomware attack in the past two years, which is a substantially higher figure than the global percentage of **65%**.
- **52%** of UAE organizations have experienced loss of data in the same time period.
- The average data loss is **12% to 14%** across all environments measured (on-premises, private cloud, public cloud, and edge) in the same timeframe.



## Organizations in the UAE are responding to data security risk by increasing budgets and staffing.

- To improve data protection across all environments measured, UAE organizations have increased budgets over the past 12 months by **29% to 35%** on average (compared to 28% to 30% globally).
- Staffing of UAE data protection and data security teams has also increased by an average of **14 to 16** people compared to 21 to 22 globally.
- **98%** of UAE organizations believe they have adequate staffing to keep their organization secure.



## Those in the UAE have greater clarity over the source of threats, but underestimate overall risk.

- More organizations report that risk levels have decreased in most areas over the past 12 months. However, they report increased risk from data security, economic uncertainty, and emerging technologies such as AI.
- When presented with individual risk factors, **95%** believe their organization currently experiences risk.
- Organizations in the UAE also have a stronger belief in their resilience. Only **5%** believe their organization won't survive another 12 months compared to 15% globally.

# Economic uncertainty and data security are the top risks for organizations in the UAE.

Managing risk is a cornerstone for every organization around the world. The ability to adapt and navigate barriers to growth is essential for businesses to be able to move forward.

Given this, it's imperative to identify the greatest risks faced by UAE organizations today. When asked, 38% of respondents ranked economic uncertainty—such as financial uncertainty and rising costs—as the greatest risk their organization is experiencing.

Organizations worldwide have been facing rising costs as inflation increases. Raw materials, energy, food, and water—the list is endless as profit margins have been affected. The fact that respondents from the UAE recognize this uncertainty as their greatest risk is not surprising. It may show the pressure the market is facing from a bleak economic outlook.



However, risks from economic uncertainty do not stand alone. A similar number of respondents also highlighted that they are experiencing risks from data security (37%) and from weak sustainability measures (37%). Organizations globally acknowledge cyber risk as a trend, with 46% ranking it as the top risk, demonstrating the ongoing threat posed by cybersecurity breaches.

The high ranking of weak sustainability measures (and notably in contrast to organizations globally) appears to be driven by executives in the UAE, who rank it as the greatest risk (44%) compared to practitioners (30%). With new sustainability laws and regulations coming into place, [and a wider emphasis within the UAE to be Net Zero by 2050](#), those most senior clearly see sustainability practices as their greatest challenge.

However, the top risks outlined here do not tell the whole story. Risk is multifaceted (Figure 1). The results highlight that organizations in the UAE need to understand each type of risk to best protect themselves.

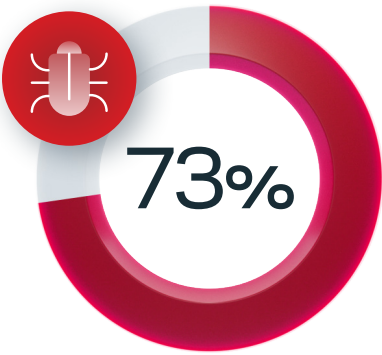


Figure 1. Which of the following are the greatest risks to your organization today? Combination of responses ranked first, second, and third [100]. Data shown only from organizations in the UAE; not all answer options shown.

Each type of risk causes harm, be it to finances or reputation. In fact, 98% of all those surveyed in the UAE report risks have resulted in actual damage to their organizations. Every level of risk that is not managed effectively can cause significant damage, from a loss in key contracts/customers after a cyber breach to fines for not meeting compliance regulations.

Organizations in the UAE appear to be more aware of the risks they face, as well as the resulting damage. Risks can wreak havoc on an organization, a fact that those surveyed understand well. Careful management and mitigation—as well as understanding—are crucial to minimizing threats.

# The UAE has experienced more successful ransomware attacks than most markets.



Almost three-quarters (73%) of organizations in the UAE have experienced a successful ransomware attack in the past two years in which the attacker has gained direct entry or access to the targeted system (Figure 2).

The UAE is clearly under greater threat than other markets; the global average of ransomware attacks in the same time span is 65%. Of the 13 markets surveyed in the research, the UAE is fifth most likely of countries surveyed to have experienced such an attack. There's a clear reward for cyber criminals in a country that is rich in commodities and serves as a huge base for financial service institutions.

Ransomware attacks are not the only type of cyberattacks. And they're not the only event that can lead to data loss. Just more than half (52%) of organizations in the UAE have experienced a loss of data over the past two years from sources other than ransomware attacks.

Furthermore, these data loss events are happening across infrastructure, including cloud environments. The loss averages over the past two years are roughly similar (12% to 14%) for all IT environments measured—on-premises, private cloud, public cloud, and edge.

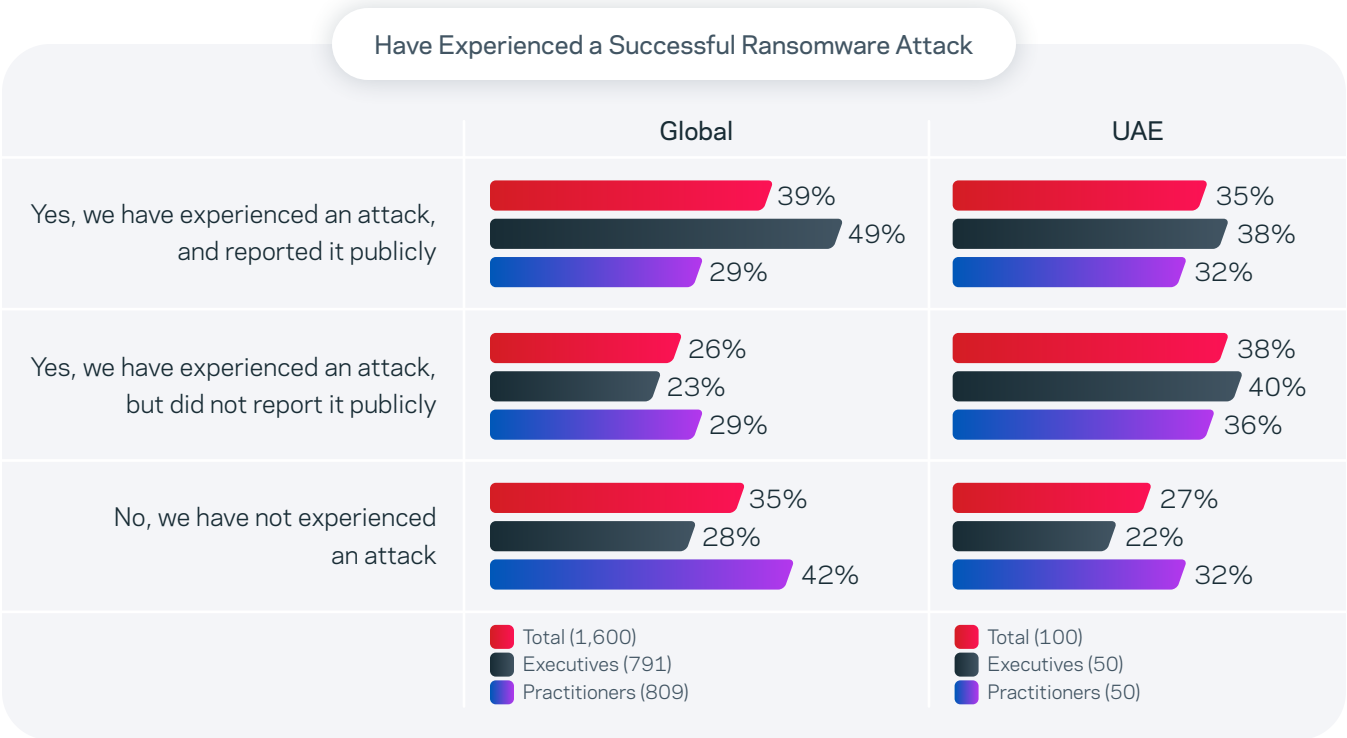


Figure 2. Has your organization experienced a successful ransomware attack in the last two years? [Base sizes in chart] Data split by respondent type, showing data for global and the UAE; not all answer options are shown.

# Organizations in the UAE respond to the level of data security risk by increasing budgets and staffing.

Risks from data security, as mentioned, rank second when it comes to current threats organizations in the UAE face. Given the context around the number of attacks experienced in recent history, it makes sense for organizations to have increased their data protection budgets across all environments measured.

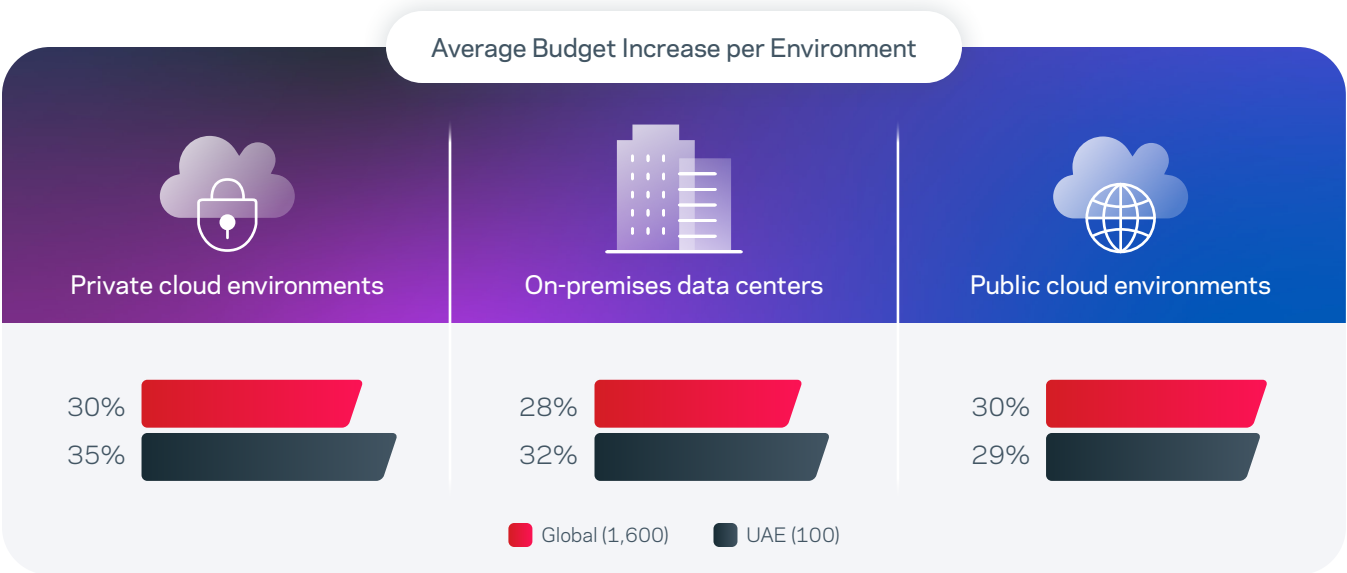


Figure 3. Approximately, how has your organization's budget for data protection changed in the last 12 months over the following environments? [100] Chart shows only the average percentage increase per environment; showing data from global and UAE.

Budgets have increased to a greater extent in the UAE than globally (28% to 30%), showing just how much bolstering data protection defenses have been a focus to those in the UAE (Figure 3).

Organizations in the UAE have also increased their data protection and data security teams by an average of 14 and 16 people, respectively. This increase is lower than the global average (21 and 22), demonstrating how economic turbulence—the market's greatest risk—may have had greater influence.

Given the extra workforce, it is no surprise that 98% of organizations in the UAE believe they have enough staff to keep them secure. Extra employees clearly helps to make respondents feel that their organization is taking the security threat seriously.

Data protection and data security teams are increasing.

# UAE respondents have greater clarity over the source of risks, but underestimate the overall threat.

For organizations in the UAE, risk levels have more likely decreased than increased over the past 12 months. Using risks from competition (meaning price competition or competitor innovation) as an example, 40% of respondents report that risk has decreased in the recent past compared to 32% reporting it has increased.

This pattern is contrary to the global results, in which respondents reported all risk types were more likely to have increased than decreased.

This brings the question: Is the UAE facing less threat compared to other markets?

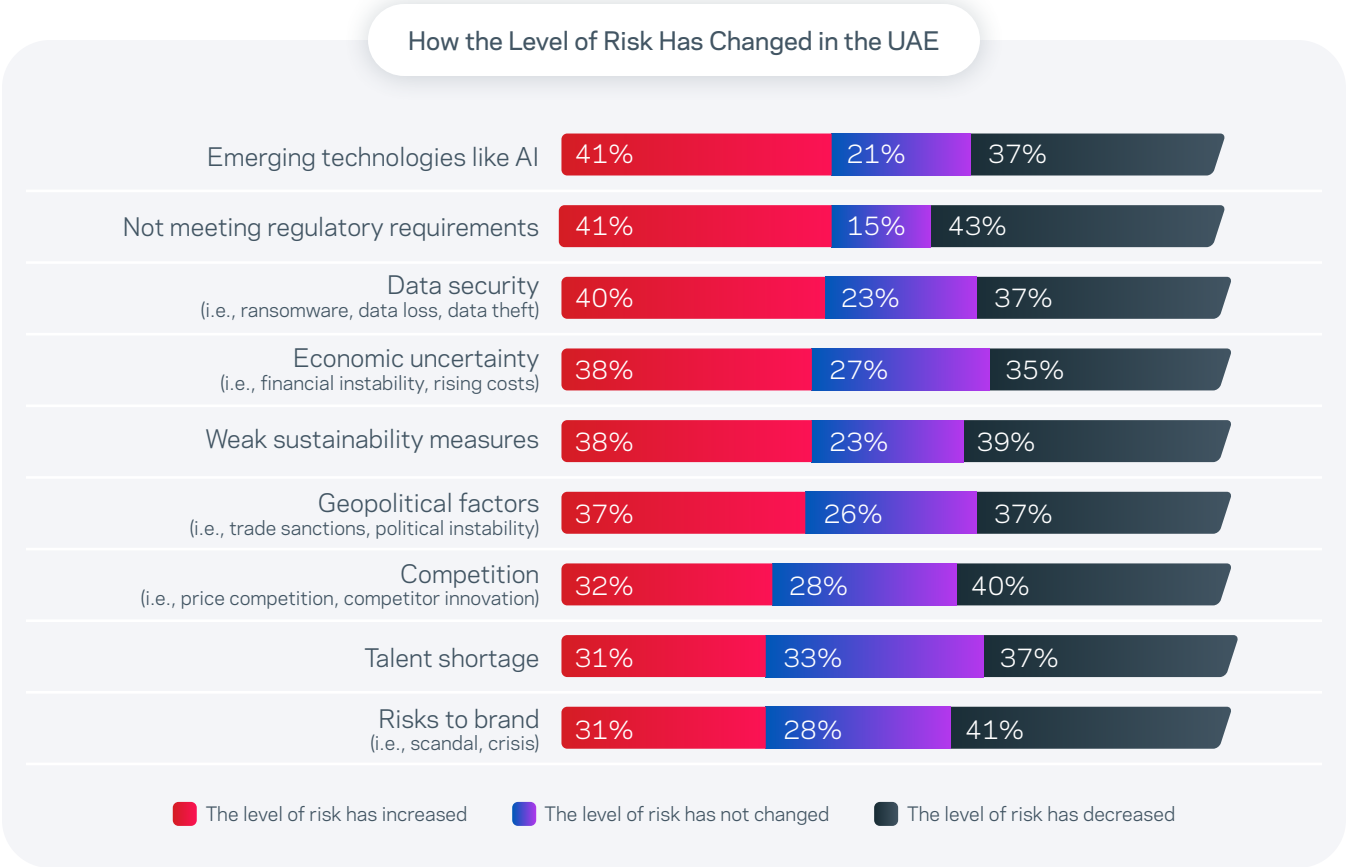
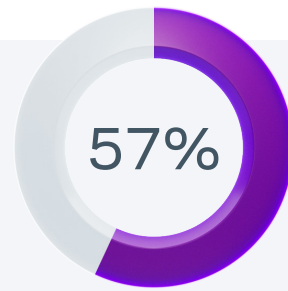


Figure 4. How has the level of risk to your organization over the following categories changed over the past 12 months? [95]. Question only to those who report they experience risks today. Chart shows data only from the UAE and does not include all answer options.

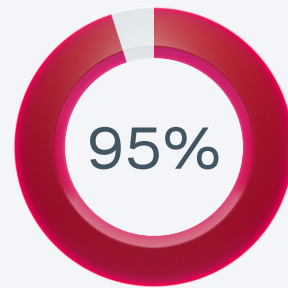
The general pattern of decreasing risks does not apply to all types of risks in the UAE. When it comes to emerging technologies like AI, data security, and economic uncertainty, more respondents are likely to say the risk level has increased. This makes sense as these are the areas respondents in the UAE say pose the greatest threat to their organization today, especially economic uncertainty and data security.

The general threat level is acknowledged by respondents in the UAE, with 57% saying they believe their organization is currently at risk. It appears that organizations in the UAE have greater clarity of the danger posed by different risk types than their global counterparts—only 52% globally said their organization is at risk. And only 5% of respondents in the UAE believe their organization won't survive another 12 months when the global figure stands at 15%.

Despite this, there still appears to be some complacency. When asked later about individual risks, 95% admitted their organization faces risks today, underlining that employees and organizations in the UAE don't consider specific threats when considering their organization's overall risk. It raises the question of whether respondents in the UAE underestimate the level of risk they face.



**believe their organization  
is currently at risk.**



**admitted their organization faces  
risks today when presented with  
an itemized list of risk factors.**

# CONCLUSION

Organizations, it could be argued, are defined by how successful they mitigate and manage risk. Risks vary and constantly change, with new ones emerging on a frequent basis. Navigating uncertainty can significantly impact the outcomes of any business.

The greatest risk faced by businesses in the UAE is that from economic turbulence. This differs from global results, where data security is the greatest risk, highlighting how critical the global economy is to organizations in the UAE. Trade is an important structure in the UAE economy, especially in petroleum and natural gas—tough economic conditions will no doubt impact this market more than others.

However, threats from data security are never too far away. Indeed, organizations in the UAE have been under greater danger of successful ransomware attacks than their counterparts globally. The greater threat posed perhaps explains the fact that data protection budgets have increased across environments.

The general results show a pattern in which organizations in the UAE are generally aware of what their greatest risks are, and where the threat level is increasing. There's a sentiment they're more robust than their counterparts globally. A good place no doubt to be in, but organizations in the UAE must avoid any complacency in the constant risk management battle.

## Research Scope and Methodology

Veritas Technologies commissioned independent market research specialist Vanson Bourne to undertake the quantitative research upon which this report is based. A total of 1,600 business executives and practitioners were interviewed during August and September 2023, with representation from the following regions and individual markets (number of interviews in brackets):

- **Americas (300):** US (200), Brazil (100)
- **EMEA (500):** UK (100), France (100), DACH (100), Nordics (100), UAE (100)
- **APAC (800):** China (200), South Korea (100), Singapore (100), India (200), Japan (100), Australia (100)

All respondents had to be from organizations with more than 1,000 employees and represent a range of private and public sectors. All respondents had to at least influence technology purchasing within their organizations.

Vanson Bourne conducted interviews online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

This executive summary is based on the data from the UAE, with comparisons made to the global data where applicable.

### About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit [www.vansonbourne.com](http://www.vansonbourne.com).



VansonBourne

### About Veritas

Over 80,000 customers—including 91% of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor can match Veritas's ability to execute, with support for 800+ data sources, 100+ operating systems, and 1,400+ storage targets through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at [veritas.com](http://veritas.com). Follow us on X at [@veritastechllc](https://twitter.com/veritastechllc).

**VERITAS™**

United Arab Emirates  
971 8000-35704426  
[veritas.com](http://veritas.com)

For global contact  
information visit:  
[veritas.com/company/contact](http://veritas.com/company/contact)