451 Research | Business Impact Brief

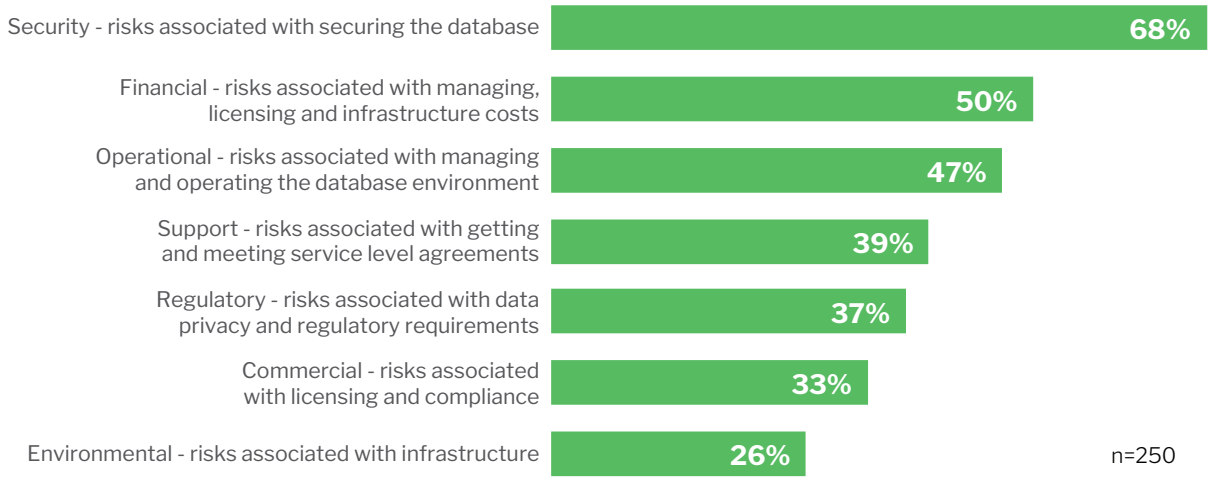
Security tops list as top database management risk, poorly administered security policies a factor

The 451 Take

While there are many risks associated with operating a database, security is one risk that stands out significantly above the rest. According to a recent 451 Research survey (see figure below), 68% of enterprise respondents said that security is their number one concern when it comes to database risks, while 50% of respondents reported financial risks as a major concern as well. And for good reason. Database systems are nearly universally accepted as the vehicle for holding an organization's systems of record. This data may consist of customer data, product data, sales data from products sold and services rendered, employee data, project and development data, and financial data, such as payables and receivables.

Most Worrisome Proprietary/Open Source Database Risks

Source: 451 Research



But database security can be multi-faceted, as suggested by 451 Research's data on database risks. Perhaps the top concern for enterprises is the protection of their data layer, specifically the risk of data breaches and stolen data because failing to properly secure data can have significant consequences. Security lapses can break trust with customers, sever partnerships, cause legal issues, spur governmental compliance incidents, and generally compromise business operations, resulting in penalties and fines.

Securing data is top of mind for enterprises, and many organizations expect that their database inherently comes with enterprise-grade security functionality, whether the database is proprietary or open source software. However, enterprises have indicated that leveraging such inherent enterprise-grade security functionality requires that security policies be properly administered as well. Enterprises confirm that this is not always the case. In fact, 451's research reveals that enterprises are experiencing significant frustration in this regard. While their databases (proprietary or open source) had the necessary enterprise-grade security functionality, organizations reported that their database security was not set up correctly, and vendors were slow to distribute security patches. Additionally, they reported that their administrators were slow to install those patches once received. Moreover, enterprises also reported an increased risk due to access privileges not being managed correctly, such as administrators not being vetted properly and employees not receiving or following the necessary training on critical security behavior, such as password management.

If not dealt with effectively, these database security risks have the potential to disrupt the entire flow of the enterprise. Luckily, there are things that enterprises can do to mitigate these security concerns.

451 Research® | Business Impact Brief

Business Impact

PROTECT THE DATA. With concerns about data breaches and loss, the first action for enterprises is to ensure that the primary data is protected. Perimeter security is necessary, of course, but more importantly, granular security is necessary at both the table level and the row level, including the ability to ensure granular access for certain kinds of commands on rows.

EXPECT ONLY THE BEST SECURITY. Security capabilities can vary widely among the numerous database products available, both proprietary and open source. The reasons for this variance often include immature databases and lack of developmental talent. Regardless, taking security shortcuts in the short run could have severe long-term consequences if not dealt with properly.

TOOLING NEEDS TO MATCH THE SECURITY. Certainly, enterprise-grade database security is important, but the tooling to administer that functionality is equally important. At a minimum, enterprises should expect easy-to-navigate interfaces for administering access policies, monitoring and tuning, as well as tooling for failover and for backup and recovery tasks.

PRIORITIZE DATABASE ADMINISTRATION. An enterprise can have the best database security in the world with the associated tooling, but all databases need some administration, and overlooking this aspect can expose the enterprise to significant risk. Administrators ought to be well trained and qualified and able to functionally administer the database, but they should also be knowledgeable about the enterprise's security policies and strategy.

Looking Ahead

Database security will continue to play an indispensable role in any enterprise, large or small. Choosing the right database is critically important, but so is the tooling and functionality associated with that database and how it can be administered. And while there will always be some security risk, the goal is to minimize it to the smallest degree possible by following security database fundamentals.

With key security measures in place, enterprises will be much more prepared for the future. More importantly, enterprises can count on at least one overriding fact: that database security will continue to change as database attacks become more sophisticated and targeted. As such, enterprises will need to partner with vendors that are keeping up with the latest security trends – security is an ongoing exercise, not a one-time event. Artificial Intelligence and machine learning are expected to play a key role in database security as these technologies become embedded in monitoring, access control, detecting internal and external attacks, applying security patch updates, and even identifying vulnerable areas within the environment.

In the end, regardless of the tooling and methods used, enterprises need to stick to the fundamentals of protecting the data because if data isn't stored properly, enterprises run the risk of legal problems, as well as losing valuable customer support and brand recognition, something that could trickle down to all other facets of the enterprise.