2011 Downtime and Data Loss Vulnerability Index Benchmark

Presented by

About this study

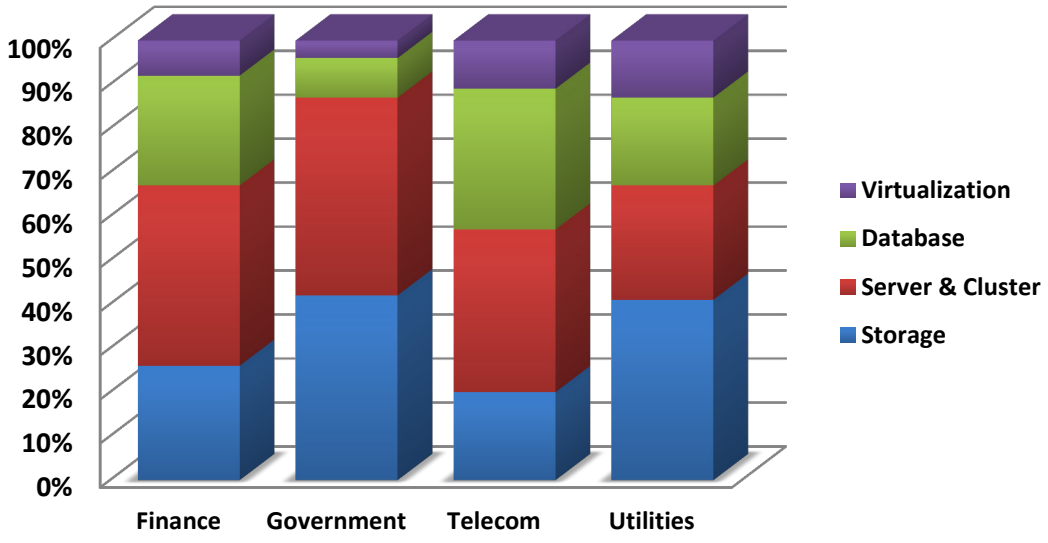
The statistics presented in this study are based on data gathered over 12 months (September 2010 to August 2011) from 88 organizations based in Europe and the US. The data was collected using Continuity Software's AvailabilityGuard™, an automated DR and HA testing and monitoring software that scans the entire IT infrastructure and identifies potential downtime and data loss vulnerabilities before they impact business operations.

Where are HA/DR risks found?

Overall, High Availability (HA) and Disaster Recovery (DR) risks are most prevalent in the storage and server layers, although some variations are exhibited among companies in different sectors. Financial services and government organizations have more risks identified in the server & cluster layer. Telecommunication companies have pretty even distribution of risks in all layers, while for utilities storage is the greatest risk area.

The number of HA/DR risks identified in the virtualization layer is relatively low, since most organizations are still shying away from running high-complexity business-critical application in a virtual environment. As organizations gain more confidence in their cloud implementations, we can expect an increase in the portion of applications running in the virtual environment as well as the risks associated with the virtualization layer.

Distribution of identified risks by area and industry



Industry	Storage	Server & Cluster	Database	Virtualization
Finance	33%	41%	18%	8%
Government	42%	45%	9%	4%
Telecom	26%	31%	32%	11%
Utilities	41%	27%	19%	13%

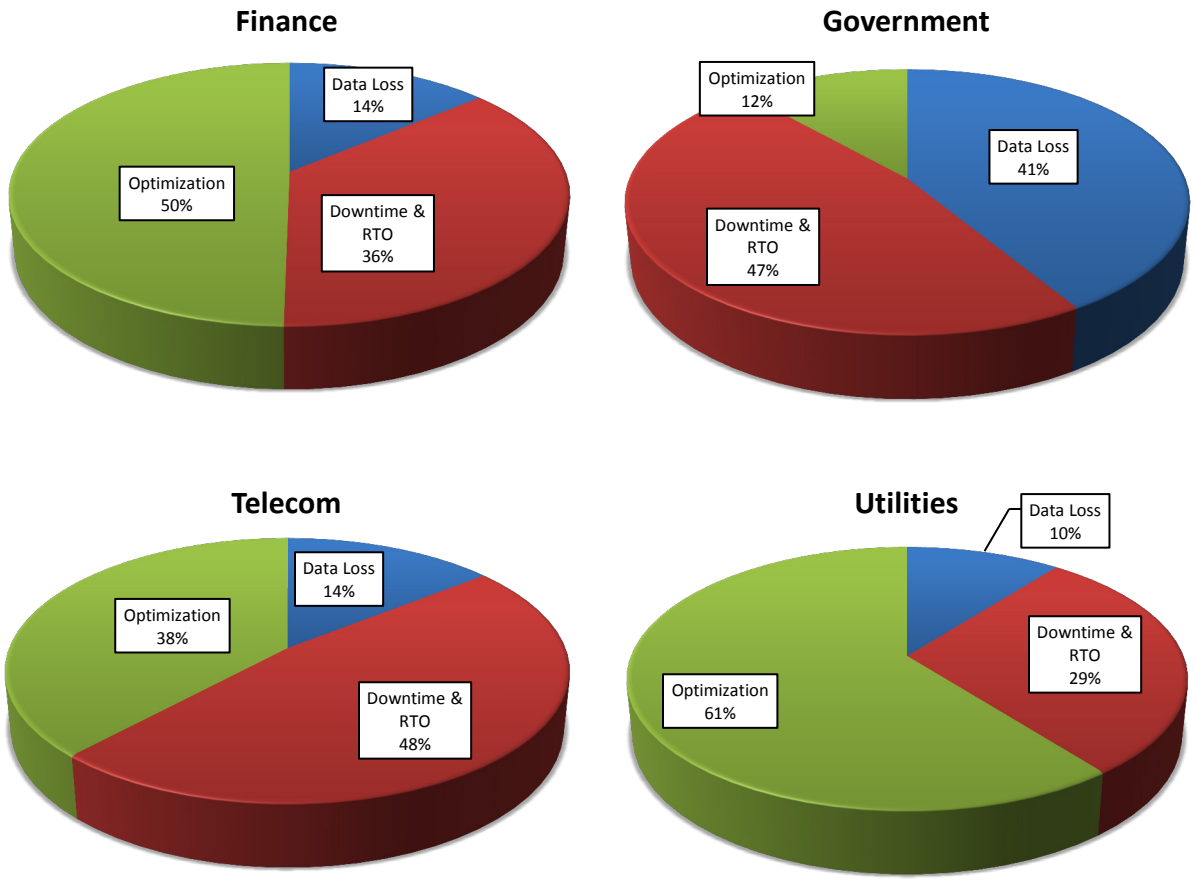
What types of HA/DR risks are found?

The data shows that government organizations exhibit a higher proportion of downtime and data loss risks than commercial businesses. As many as 47% of the risks identified in government organizations could lead to downtime and Recovery Time Objective (RTO) violations, and 41% could result in data loss.

These figures are significantly higher than those found in the private business sectors. Among these, utilities seem to do the best job of minimizing downtime and data loss risks (29% and 10% respectively), with the majority of the identified items (61%) pointing to issues that may compromise efficiency and resource utilization but would not hinder the service level provided.

Among private sector companies, telecommunication organizations lag behind other industries in containing downtime and data loss risks (48% and 14% respectively), compared to 38% and 14% respectively for finance organization.

Ticket distribution by risk category, per industry



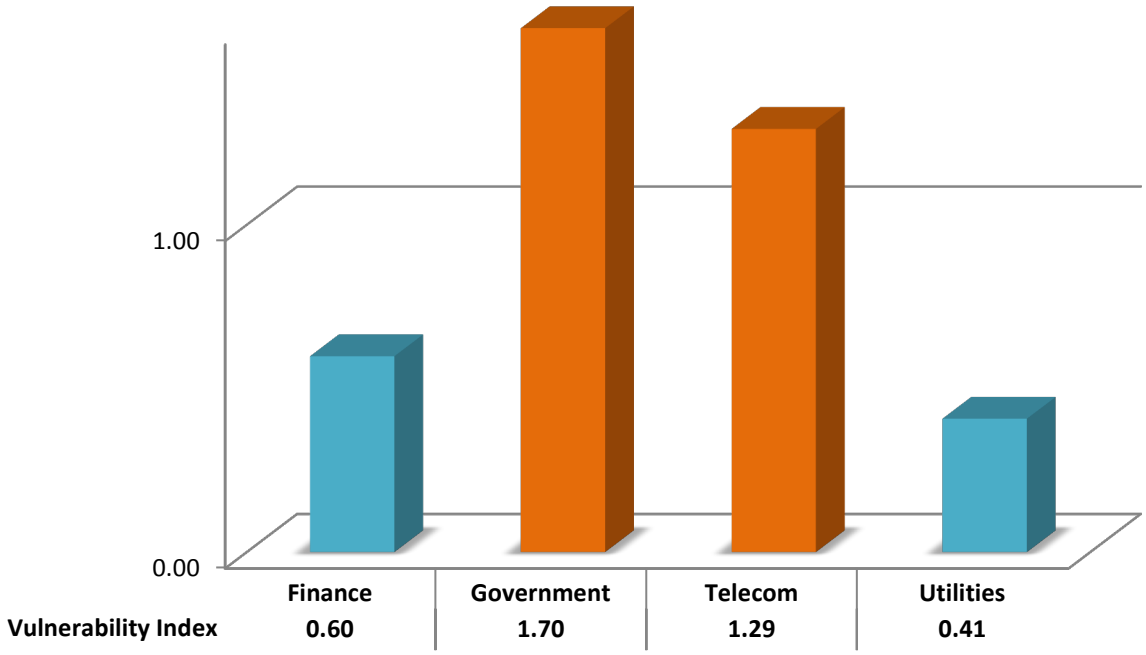
The table below shows the most common issues found within each category per industry.

Sector	Top DP/DR risk	Top HA risk	Top RTO risk	Top Optimization issue
Finance	RPO SLA breach	SAN I/O multipath redundancy issues	Incomplete access to storage on DR	Suboptimal database file layout on file systems and storage volumes
Government	Storage replication group configuration errors	SAN I/O multipath redundancy issues	Incorrect DNS Settings	Suboptimal database file layout on file systems and storage volumes
Telecom	Database log shipping out of sync	Cluster configuration errors	Network file systems inaccessible / missing	No database transaction log file mirroring
Utilities	Storage replication group configuration errors	Incorrect / missing mapping of storage to nodes	Insufficient resources to carry production load	MS-SQL configuration BP violations

The Continuity Software Vulnerability Index

The Vulnerability Index benchmark compares the level of risk found in each sector on a normalized scale. It takes into consideration the number of risks found per organization in each sector as well as the severity of these risks. A Vulnerability Index score greater than one means the sector's level of risk is above average, while a score lower than one represents a below average risk level.

As can be seen in the chart, **the telecom and government sectors exhibit above-average risk levels** (1.70 and 1.29 respectively), **while finance and utility organizations have below-average Vulnerability Index scores** (0.60 and 0.41 respectively).



In Conclusion

Despite ongoing efforts to eliminate HA/DR risks, organizations in all sectors still exhibit a significant number of incidents that could lead to downtime and data loss.

Maybe even more alarming is the fact that many organizations simply don't know what risks exist in their environment. Lacking the tools to automatically monitor risks on an ongoing basis, these organizations rely on infrequent and incomplete manual tests, limiting their ability to accurately account for and address downtime and data loss risks that can impact business operations.

To see how AvailabilityGuard can help you identify the vulnerabilities that can put your organization at risk, sign up for a 48-hour assessment of your environment.

Disclaimers and notices

The results presented in this publication are based on a limited data set are not warrantied to accurately represent any data beyond the data set used.

This publication is subject to change without notice. While every precaution has been taken in the preparation of this publication, Continuity Software assumes no responsibility for errors or omissions.