IDG

WHITE PAPER

7 Guidelines for Hyper-Availability in the Digital Financial Services Enterprise

FINANCIAL SERVICES ORGANIZATIONS FACE INCREASING pressure to comply with rapidly evolving regulatory requirements for data integrity and security. In addition, valuable stored data continues to grow at exponential rates.

Meanwhile, customers expect around-the-clock access to their account information from their computers and mobile devices. In fact, many banks have developed customized mobile applications that enable 24.7.365 account transactions, including deposits and transfers of funds.

Considering the highly sensitive nature of financial information, the effects of lost or compromised data can be detrimental for firms, investors and customers.

IT leaders in financial services must adopt an intelligent data management strategy, to incorporate: backup and recovery of all application and workloads, protection and management of data across multi-cloud environments, orchestration and optimal use of resources, and automated backup, migration, security and recovery capabilities. Financial services firms will lose customers if there are any doubts about the security or reliability of account information. Enabling the Hyper-Available Enterprise is critical.

SPONSORED BY:

VEEAM

The threat landscape

Customers increasingly require non-stop access to account information, and financial services are natural targets for cybercriminals. In one of the most eye-opening examples, Bangladesh Bank in 2016 suffered an $81 million bank heist when hackers used Society for Worldwide Interbank Financial Telecommunication (SWIFT) credentials to request that more than three dozen criminal money transfers be sent to bank accounts set up in the Philippines, Sri Lanka and in other locations throughout Asia. This theft not only caused serious threats to Bangladesh Bank's reputation, it also raised integrity issues worldwide about the SWIFT network, which had previously been considered totally reliable.

More recently (October 2017), the SWIFT system of NIC Asia Bank was compromised by a cyber attack, in which hackers made $4 million worth of fraudulent transfers.

"Banks are attacked daily, sometimes hundreds or thousands of times," said James Chessen, executive vice president of the American Bankers Association's Center for Payments and Cybersecurity, in a Nov. 7, 2017 story in *American Banker*. "There's this constant battle, with hactivists, hostile nations or whomever trying to get access to information or work their way into a bank."

The 2017 Cost of Cyber Crime Study by Accenture and Ponemon Institute reports that, on average, a company suffers 130 breaches per year. The study found that the financial services industry pays the highest annualized cost of cyber crime: $18 million.

Hyper-Availability in the age of compliance

Financial services firms also need to comply with national and, in some cases, international standards. For example, publicly traded banks and insurance companies must adhere to Sarbanes-Oxley requirements for protecting, securing and retaining information. In addition, the Basel Accords include strict rules on how to protect bank IT departments through proper disaster recovery (DR) solutions, and they require DR tests at least annually.

Regulatory compliance requires clear visibility into data availability processes and procedures, with automated auditing and reporting. The impact of noncompliance is untenable, because financial services firms would be exposed to the possibilities of major fines and damage to brand reputation.

Encryption and data access security are essential for maintaining the privacy of account information, and availability of all systems must be guaranteed. Financial services organizations need to ensure zero downtime because clients demand instant access to their account information, and data must be retained long-term to address regulatory compliance and document the integrity of financial transactions. Data from remote and branch office locations should be centrally consolidated and archived to protect customer privacy and ensure the continuous availability of historical account information.

IT's impact on financial services

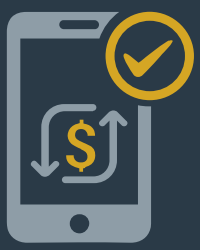
Banks and insurance companies are increasingly dependent on applications for business success, and critical data and applications must be secure and constantly available through multiple channels.

Financial services organizations are continually developing innovative applications to differentiate themselves in increasingly competitive, multichannel markets. They are conducting more transactions online, and therefore collecting more data on each account that they, in turn, have to maintain, archive and protect. Through big data analytics, banks and insurance companies are providing customers with richer and more immersive online and mobile experiences.

The explosive growth of data is placing major resource demands on IT while forcing financial services organizations to invest more in storing and archiving enterprise data, and implementing best practices for DR. As financial services firms wrestle with how to securely and cost-effectively store the growing volumes of information and recover from any natural or unnatural disasters, they are increasingly using cloud resources to augment internal infrastructure.

Rapidly expanding data growth rates are severely affecting enterprise IT budgets. According to the IDC Financial Insights Worldwide Semiannual IT Spending Guide, the financial services industry leads overall global IT spending, largely driven by digital transformation efforts. Investing in the availability of ever-increasing data volumes is crucial to the long-term viability of any financial services institution.

Alongside this data growth is the concept of digital transformation, which is allowing banks and insurance companies to increasingly adapt to or drive disruptive changes in their business processes.



FINANCIAL SERVICES ORGANIZATIONS ARE CONDUCTING MORE TRANSACTIONS ONLINE, AND THEREFORE COLLECTING MORE DATA ON EACH ACCOUNT THAT THEY, IN TURN, HAVE TO MAINTAIN, ARCHIVE, AND PROTECT.

"DIGITAL TRANSFORMATION IS NOT JUST A TECHNOLOGY TREND, IT IS AT THE CENTER OF BUSINESS STRATEGIES ACROSS ALL INDUSTRY SEGMENTS AND MARKETS."

—Robert Parke
group vice president of IDC

Financial services firms are leveraging digital competencies to innovate new business models, products and services that enhance the customer experience while improving operational efficiencies and organizational performance. According to IDC, worldwide spending on digital transformation technologies will grow to more than $2.1 trillion in 2019, with a compound annual growth rate of 16.8% from 2014 to 2019.

Digital transformation is also helping financial services firms manage risks more effectively. For example, in the event of a natural disaster, banks and insurance companies that have implemented geographically distributed backup and recovery sites can protect their digital information and ensure their business continuity to enterprise and consumer customers.

"Digital transformation is not just a technology trend, it is at the center of business strategies across all industry segments and markets," says Robert Parker, group vice president of IDC. It represents "a critical opportunity for companies to redefine their customers' experience, achieve new levels of enterprise productivity and create competitive advantage. Enterprise investments in digital transformation will constitute the majority of growth in technology markets over the next five years, making it a priority for technology vendors as well."

Reduced downtime and data retention

Hyper-Availability of enterprise data and long-term data retention are essential elements of business success for financial services organizations. Customer account information is now accessible at any time, from any device, and no customer will tolerate slow performance or network downtime. Partners throughout the financial services ecosystem will similarly refuse to conduct business regularly with banks and insurance companies that do not reliably deliver uninterrupted access to shared data.

Financial services firms increasingly conduct business through digital channels, and the cost of downtime is skyrocketing. IDC estimates that the mean cost of one hour of downtime for an organization with between 1,000 and 4,999 employees is approximately $225,000. Consequently, businesses cannot tolerate the same levels of unplanned downtime they could before they started on their digital transformation journeys.

Even planned backup activities create the potential for customer retention and revenue problems. "Backup to tape was taking 48 hours, and recovery could take hours or days," says Andrew Connelly, IT operations manager at Capfin. "For example, if our SQL environment were to fail, our company could be offline for days as we restored from tape, which could massively affect revenue. We never want to experience a situation like that."

Because brand reputation is critical for customer retention, the window of downtime for banks and insurance companies is close to zero. For example, HSBC suffered a cyber attack that prevented customers from accessing their accounts for several hours. This incident was particularly difficult for the bank's reputation, because it had suffered two other outages in recent years.

"We are very serious about providing our customers with the service they deserve," says Larry Walker, vice president and data processing officer at Chelsea Groton Bank. "However, we can't wait on customers and provide extraordinary service if the virtual machines (VMs) supporting our customer call center, email and document imaging system are unavailable. They must be available when we need them."

Guidelines for data protection, backup and availability

Technical requirements for financial institutions and insurance companies are changing rapidly, and ensuring the continuous availability of mission-critical data is essential for profitable operations. IT leaders in these environments must assess their data availability solution options and enable intelligent data management, using these critical factors as guidelines:

1. **DATA PRIVACY MUST BE MAINTAINED:** As customer information becomes accessible through any device, encrypting secure traffic flows is required to secure customer information

2. **BACKUP AND RECOVERY OF ALL WORKLOADS MUST BE GUARANTEED:** Customers and business partners expect 24.7.365 availability for all applications and data with complete visibility, and financial services firms should embrace zero-downtime tolerance policies

3. **DATA RECOVERY SHOULD BE STREAMLINED AND SECURED:** Exposure of confidential data can result in business-crippling fines and a disastrous impact to the brand. Financial services organizations must be able to implement granular data recovery, have the ability to search data resources, and focus on immediately recovering mission-critical data. Banks and insurance companies must also develop and implement low recovery point and time objectives. Ideally, data recovery should be implemented within less than 15 minutes for recovering all applications and data, with complete visibility into recovery processes and end-to-end encryption to protect the data

4. **CONSIDER AN AVAILABILITY SOLUTION THAT ENSURES PROTECTION AND MANAGEMENT OF DATA ACROSS MULTI-CLOUD ENVIRONMENTS:** Every comprehensive availability strategy must include an off-site infrastructure, whether managed internally or by a trusted service provider. IT should evaluate whether to extend availability to the cloud to avoid the cost and complexity of building and maintaining off-site infrastructure for backing up data and enabling secure and timely disaster recovery

5. **IMPROVE MANAGEMENT OF DATA WITH CLEAR, UNIFIED VISIBILITY AND CONTROL INTO USAGE, PERFORMANCE ISSUES, AND OPERATIONS:** Aggressive retention standards, growing customer demands and increasing IT-infrastructure complexity make it challenging for financial services firms to adequately safeguard the growing amount of sensitive information they're required to store and protect. It is important to deploy resource optimization and configuration tracking to evaluate the performance of the infrastructure, ensure best practices for data management are implemented and enable around-the-clock real-time monitoring and alerting

6. **SAVE MONEY BY SIMPLIFYING AND AUTOMATING DR:** Banks and insurance companies are required to comply with demanding standards and regulations. One of the most challenging requirements is to consistently execute annual DR testing, which can be both expensive and labor-intensive. DR should be simplified to guarantee recovery point and time objectives of less than 15 minutes for recovering all applications and data, and to provide proof of compliance through automated reporting

7. **MANAGE BRANCH FACILITIES THROUGH A SINGLE PANE OF GLASS:** The centralization of data from remote and branch office locations consumes significant bandwidth and resources for financial services organizations. It is crucial to centralize server management for multiple locations into a single view and empower IT administrators to manage assigned VMs without allowing multitenant reporting to compromise the remainder of the data

Learn more

Veeam is the global leader in Intelligent Data Management for the Hyper-Available Enterprise. Veeam Hyper-Availability Platform is the most complete solution to help customers on the journey to automating data management and ensuring the Hyper-Availability of data. We have more than 307,000 customers worldwide, including 75 percent of the Fortune 500 and 58 percent of the Global 2000. Our customer satisfaction scores, at 3.5X the industry average, are the highest in the industry. Our global ecosystem includes 57,600 channel partners; Cisco, HPE, and NetApp as exclusive resellers; and nearly 19,800 cloud and service providers. Headquartered in Baar, Switzerland, Veeam has offices in more than 30 countries.

To learn more on how to achieve Hyper-Availability for your financial enterprise, visit this web page.