

WHITE PAPER:

A Guide to Managed IT Services for Financial Services Organizations

As the Banking Industry evolves, outsourcing to technology experts may be the key to staying ahead of the competition.





EXECUTIVE SUMMARY

The financial services industry is in a period of profound transformation. The rise of digital-only competitors, cryptocurrencies, and digital ledger technologies, along with evolving financial markets, have increased regulatory complexities. Accelerating risks from cybercrime and fraud also present retail banking, credit unions, investment, insurance, and venture capital firms with an array of challenges.

In nearly every instance, the industry is addressing these challenges through the application of emerging technologies. In a recent global study, 96 percent of financial services professionals surveyed by the Norton Rose Fulbright law firm agreed that financial technology, or fintech, is a strategic priority for their institutions.

Cloud-based infrastructure, artificial intelligence, predictive analytics, and process automation are all essential to the industry's ongoing digitalization efforts. However, although such solutions can help streamline processes, reduce risks, and enhance the customer experience – time cost, and complexity present obstacles to effective implementation.

Worldwide IT spending in the financial services industry has reached nearly \$600 billion annually, according to Gartner, but a good deal of that is going toward maintaining legacy technologies. Analysts say nearly half of all banking systems worldwide remain heavily dependent on decades-old mainframe platforms running COBOL applications for processing deposits, check-clearing services, ATM transactions, and servicing mortgages.

The resources required to maintain these legacy technologies make it difficult for IT teams to take on the challenges of digital transformation – especially if and when this transformation must take place across hundreds or even thousands of disparate locations in a consistent fashion. Nearly 85 percent of financial services CIOs reported they've had digital transformation projects canceled, delayed, or reduced in scope because of the limitations of their legacy infrastructure.

As a result of these limitations, financial institutions are increasingly adopting managed IT services to support their efforts to modernize their technology infrastructure. In this white paper, we'll take a closer look at some of the new challenges facing financial services firms, and why organizations should partner with a qualified managed services provider (MSP) to address them.

THREE TRENDS DRIVING TRANSFORMATION OF FINANCIAL SERVICES ORGANIZATIONS

Banking has been around for centuries, so the industry has had to evolve and reinvent itself countless times to meet changing conditions. Here are three key trends driving the latest evolution:

- **New Competition**

The dependence on legacy technologies and traditional business models is putting financial institutions at a competitive disadvantage. Shifting demographics mean that younger, more tech-savvy consumers make up a growing proportion of the customer base, and these consumers aren't particularly interested in doing business at a physical location.

More than three-quarters of Americans now prefer to do their banking digitally via mobile apps or websites, according to an Ipsos-Forbes consumer survey. An Accenture study estimates that by 2025, conventional banks will lose up to \$280 billion in business to fintech startups such as neobanks — digital-only banks that use cloud-based infrastructure to offer a complete range of services through mobile and web channels without any physical branches or offices.

- **Financial Fraud and Cybercrime**

Large U.S. financial services and lending firms are experiencing an average of 2,320 fraudulent attacks each month, according to a recent study from LexisNexis Risk Solutions. The cost of that fraud has increased by nearly 10 percent since 2020. According to the study, every dollar lost to fraud costs financial services firms \$4 in fees, fines, interest, labor, investigation, and recovery expenses.

Most of these crimes are accomplished through cyberattacks, including ransomware, phishing, state-sponsored threats, and advanced persistent threats. Analysts say financial services firms are 300 times more likely to be the victim of a cyberattack than other organizations, and the average cost of financial services cybercrime is 40 percent higher than in all other industry sectors.

- **Compliance Challenges**

Given the nature of financial services organizations and the amount of risk involved in their day-to-day business, it's no surprise that banking is among the most regulated industries. The financial compliance framework includes hundreds of laws and regulations governing various financial services, and they are continually being updated and revised. According to one study, banking regulations change every 12 minutes, on average.

As much as 15 percent of a financial institution's entire workforce is dedicated to regulatory compliance, according to a McKinsey study. Meanwhile, Citigroup estimates that annual global spending on regulatory compliance is \$270 billion, which represents roughly 10 percent of their total annual expenses.

NECESSARY TECHNOLOGY ENHANCEMENTS

From the development of wire transfers in the late 1800s to automated teller machines a century later, the financial services industry has always embraced technologies that could improve efficiency and enhance profitability. Here are some of the technologies driving current modernization efforts:

- **Zero Trust Networks**

Zero trust security frameworks require all users and devices, whether inside or outside the organization, to be authorized, authenticated, and continually validated before being granted access to network resources. This is critical for supporting the increased use of cloud-based applications and mobile banking platforms. It's important to support zero trust networks with a highly reliable, highly available network that is monitored 24/7/365 with round the clock service and support to ensure smooth operation.

- **Cloud Applications and Infrastructure**

The cloud enables financial institutions to modernize quickly with dependable, scalable, and cost-efficient systems that allow them to get out of the business of managing massive, in-house systems. More than 80 percent of financial services companies report they are deploying cloud technology, according to a Google study. Additionally, cloud-based applications for mobile payments, market analysis, portfolio balancing, compliance management, and advanced analytics enable more automation and enhanced security.

- **Artificial Intelligence**

AI-powered digital assistants are enabling new forms of customer engagement. These tools capture, process, and analyze data about financial products and market conditions as well as customers' transaction history, investment goals, and risk tolerance to enable faster and smarter investment decisions. Additionally, AI-driven data analysis is being used for process automation, market analysis, fraud detection, credit scoring, claims management, and more.

- **5G Broadband Cellular**

The faster speed, lower latency, and higher data capacity of 5G networks will allow banks and other financial services organizations to launch a number of new customer services while also addressing existing gaps in their operations. According to PwC analysts, the technology could create more than \$40 billion in productivity gains for U.S. financial services firms by 2030.

- **Digital Signage & Wi-Fi to Enhance Retail Banking Customer Experience**

When customers DO venture into a branch office, they both expect and demand the type of environment they are used to in other retail environments. This means welcoming communication and critical information provided via digital signage deployments, as well as reliable customer wi-fi to access apps and other customer loyalty programs. In fact, the customer experience has been elevated to the expectation of customized greetings and offerings. To achieve this, retail banking locations need to partner with experts who can not only deploy but continuously maintain these technologies and systems

- **Governance, Risk and Compliance Management**

GRC solutions automate many essential IT security and compliance management processes. These tools create a cohesive approach to policy and compliance, IT governance, and internal auditing across multiple business units, and provide improved visibility into risks, threats, and vulnerabilities.

TECHNOLOGY CHALLENGES FACING FINANCIAL SERVICES ORGANIZATIONS

No industry is more deeply affected by the true cost of network downtime than financial services. Network reliability is critical for moving massive amounts of data across global financial markets, corporate data centers, branch locations, and ATMs in near real time. Highly available, highly reliable, secure networks are a must. However, resource constrained IT teams are challenged to effectively manage these complex networks. According to research from the Digital Banking Report, more than 70 percent of banking executives say a shortage of IT skills is preventing innovation.

Building and maintaining a security program is also difficult. Qualified cybersecurity personnel are difficult to recruit and retain. Maintaining and staffing a 24x7 security operations center can also prove cost-prohibitive for many organizations. Many financial services organizations lack the advanced tools needed to filter security alerts, provide context-based analysis, and automate many threat response functions.

Cloud adoption and migration pose another challenge. One recent study found that up to 80 percent of organizations lack the internal skillsets for cloud migrations. While cloud services can be adopted with a few keystrokes, effective use of the cloud requires a thorough analysis of existing applications and workloads to identify the best candidates for cloud migration. Organizations must also implement processes for managing the cloud effectively, ensuring proper configuration and security, and keeping costs in check.

HOW MANAGED SERVICES CAN HELP

In a managed services arrangement, institutions transfer much of the burden and risk of managing and monitoring complex IT systems to a third-party provider. At the same time, they gain access to the expertise necessary to implement new and specialized solutions that drive IT modernization efforts.

MSPs typically have one or more Network Operations Centers (NOCs) for the centralized supervision of their customers' networks. The MSP's engineers and technicians use state-of-the-art tools to monitor and manage the network 24x7. When network service interruptions or performance problems are detected, the MSP can work to remediate these issues remotely, often before the customer even realizes there is a problem. The MSP also serves as a single point of contact for help desk support.

Some managed services go beyond monitoring and maintenance to include network design, managed security services, and more. A qualified MSP is particularly helpful in shifting applications and services to the cloud — a complicated process that requires a good deal of specialization.

For operations requiring around-the-clock attention, a U.S.-based NOC and Security Operations Center (SOC) can provide ongoing services for continuous security event monitoring, investigation, and remediation. A quality managed security information and event management (SIEM) and SOC service will provide customers with contextual alerts and escalations of security events, valuable reports, ongoing tuning of the SIEM, and an overall customized security services experience.

BUSINESS AND IT BENEFITS OF MANAGED SERVICES

Managed services can help keep a lid on IT operational costs by eliminating the need to hire additional staff and buy more operational tools. Freed from the burden of day-to-day network maintenance and support, in-house IT teams can more quickly implement new technologies to increase competitiveness and meet changing demands.

All services are bundled into a subscription-based contract, with a predictable monthly fee based upon the number of locations, the service level agreement (SLA) and/or other metrics. Customers may also have the option of outsourcing some tasks while retaining others in-house.

While organizations typically focus on operational savings when evaluating managed services, it has the potential to impact many cost metrics. IT capital expenditures can be optimized through sound recommendations from professionals who are familiar with the network and business needs. The productivity gains that come with a highly available, high-performance network are another benefit of managed services.

Bundling security within the managed IT services platform can provide an effective and affordable best-practices cybersecurity framework. Best-in-class MSPs offer a broad range of cybersecurity solutions and services delivered by a team of highly trained, certified, and experienced cybersecurity professionals.

And last, but not least, Managed Services Providers familiar with financial services organizations can help these organizations adopt, deploy, and scale new technologies in a seamless fashion across multiple locations – providing logistical and on-site support as needed. Experienced project managers, implementation specialists, and dedicated warehousing and shipping facilities can take the logistics burden off the backs of the financial services organization, allowing them to focus on their own core business objectives. These core MSP services, combined with value-add solutions such as digital signage and wi-fi deployments to enhance the customer experience, can help financial services organizations stay ahead of their growing digital savvy competition.

CHOOSING THE RIGHT PROVIDER

Although the business case for managed services is strong, not all providers are created equal, and not all solutions are created equal. Rather than pushing a one-size-fits-all solution, the MSP should take the time to understand each customer's unique needs and growth trajectory. Only then can the MSP develop a plan that will meet the customer's business requirements and budget.

When choosing a managed services provider and solution, organizations should also look for:

- **Industry-specific expertise.** An MSP who provides services for similar organizations will have a better understanding of the customer's business needs and challenges.
- **Monitoring.** All services should be monitored around the clock with automated fault notification to ensure high levels of performance and support.
- **Support.** The MSP should provide a dedicated single point of contact and explain automated processes for 24x7 support and problem resolution.
- **Visibility.** Customers should be able to see the status of their network and support tickets through an Internet-based portal.
- **Scalability.** The MSP should have the staffing levels and operational processes needed to support growing numbers of locations and users.

Best-in-class MSPs also offer a suite of extended services, including network design, security, compliance, and more. By partnering with an MSP that serves as a "one-stop shop," organizations can further streamline operations and increase the ROI of managed IT services.

CONCLUSION

Experienced MSPs provide on-demand access to the skills, tools, and expertise that are difficult to find in the open market. Working with a managed services provider to support legacy technologies, enhance security, and drive IT modernization efforts, financial institutions can increase operational flexibility, reduce risk, and improve their ability to retain customers during a time of profound change in the industry.

However, choosing the right MSP is an important business decision. While cost containment is one of the major reasons for working with a provider, it's a mistake to simply choose a technology partner on price alone. Instead, organizations should look for an experienced provider with a strategic approach, technical expertise, and proven track record of success in the financial services industry.

About SageNet

SageNet is a leading managed services provider specializing in connectivity, cybersecurity and digital signage. The company connects, manages and protects technologies and devices across widely distributed enterprises. SageNet's people, processes and technologies, coupled with its collaborative approach, empowers customers to achieve their core business objectives.

The company offers world-class service and support via its US-based 24/7/365 Network Operations Centers (NOCs) and Security Operations Centers (SOCs), geographically-diverse teleports, a central National Logistics Center, multiple data centers, and a nationwide field service organization.

What makes SageNet unique is its Why: SageNet is passionate about Trusted Connections. This is a two-fold calling. First, the company creates trusted, reliable and secure technological connections for its customers. Second, and perhaps even more importantly, SageNet works tirelessly to build trusted human connections with its customers, partners and communities. The company believes that by creating, discovering and nurturing these trusted connections, SageNet enhances the world that connects us all.

With a three-decade track record in managed services, SageNet boasts a long-term customer base that includes the nation's largest retail, financial, healthcare, utilities and energy organizations. SageNet manages communications for more than 220,000 endpoints. Headquartered in Tulsa, SageNet has regional offices in Atlanta, Philadelphia, Toronto, Chicago and Washington D.C.