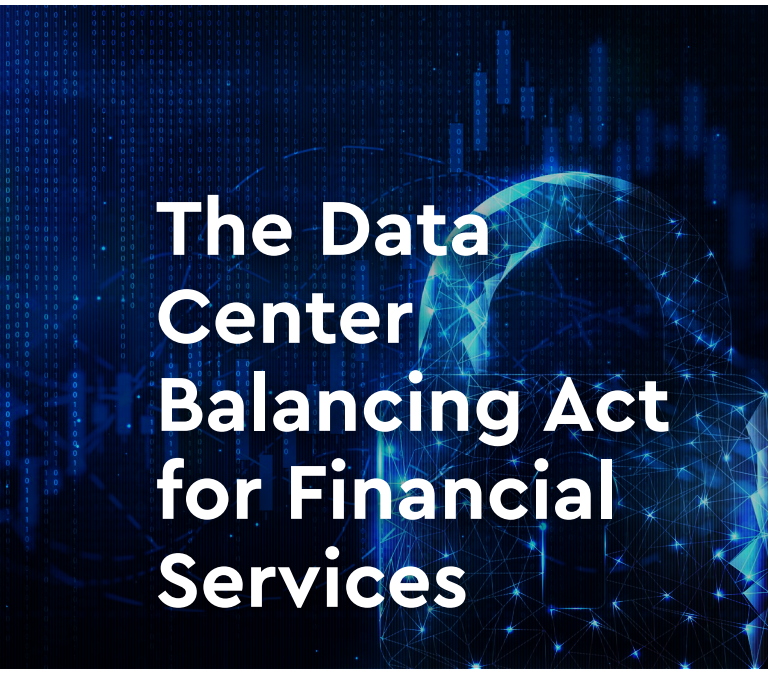

The Data Center Balancing Act for Financial Services

Balancing compliance, connectivity and disaster mitigation in the highly regulated financial services space with colocation

Executive Summary

Financial services organizations are under intense pressure to protect sensitive data and critical systems from cyber threats and physical disasters—all while creating robust connections to a rapidly evolving and fast-paced ecosystem of customers and partners. No easy task for sure. A third-party data center provider with a robust compliance program that meets rigorous security needs and provides a comprehensive suite of connectivity solutions can offload some of this challenge. However, colocation can also introduce risk into the equation if not vetted properly and proactively. A third-party risk management plan can help financial services businesses evaluate their providers as the connected world continues to modulate.

Introduction

Financial services organizations walk a tight line between maintaining a strong security posture to protect the business, its customers, and the privacy of its data and achieving a high availability, connectivity-rich data center environment. To meet the demands of an increasingly connected, data-infused world, businesses need a resilient environment that integrates a robust security and compliance program, redundant power and cooling, and a diverse selection of connectivity options.

> According to IDC, the amount of data created and stored will reach 175 zettabytes by 2025.

For the financial services industry, this ability to address the challenges of digitization is a critical success factor. The industry has embraced digital transformation, allowing customers to access financial information and conduct transactions online—and customers have followed suit, tallying 161.6 million digital banking users in 2019. **Today's financial services customers demand instant, around-the-clock access and a speed of delivery that would have once been thought impossible.** Without a doubt, this digital shift has thrust security, compliance and connectivity into the shared spotlight to ensure these organizations meet regulatory standards while staying connected with customers, vendors and partners—down the street, across the country and around the world. Balancing compliance obligations with connectivity needs is more critical than ever as noncompliance can levy serious consequences and hefty fines.

To help bridge this gap, organizations are increasingly relying on third-party colocation services to rapidly access secure, well-connected data center space. However, not all data centers are created equal. In a time of digital transformation, a forward-looking

provider equally focused on robust security and future-proof connectivity can be a critical differentiator. Those with a commitment to sustainability and real-time visibility into core data center functionality including access, connectivity and power draw can further boost security, data center management capabilities and cost efficiencies for an improved environment.

A third-party data center can help bridge the gap between stringent compliance demands and dynamic connectivity.

However, this partnership is not without risk. Organizations need to move beyond simply vetting colocation providers to develop a third-party risk management (TPRM) strategy that persistently assesses a provider's security program and assures the compliance of its environment.

Remaining compliant while connecting to the world

Security and compliance conversations tend to naturally focus on information security technical controls such as firewalls and encryption. However, when assessing a third-party data center, the discussion takes on a different slant: one that addresses the physical security of the facility and its ability to keep out unauthorized visitors, ensure continued operations and maintain a strong, internal compliance program.

Under stress to meet their own compliance obligations, data center providers need to ensure the resilience of their services and the security of their infrastructures to provide customers with the confidence that their systems are protected and optimized to ensure continuity.

To achieve the rigorous standards of the financial services market, a colocation provider must continually monitor and maintain the data center environment. Data center transparency can help meet strict regulatory standards to meet businesses' own compliance standards by offering real-time visibility into and control of data center access, power usage, temperature and humidity readings, asset management and more.

EXPERTISE TO MANAGE SECURITY AND COMPLIANCE

Data centers are also responsible for offering expertise in managing this infrastructure and ensuring it meets regulatory obligations. This requires specific knowledge sets which makes hiring and retaining this workforce even more difficult. This only becomes more complicated when you consider the frequency at which this information changes.

Business executives understand this challenge. According to a Ponemon report, 70% of CISOs report a lack of competent in-house staffing as a top area of concern. Even more troubling, the same study notes that 65% of CISOs expect inadequate in-house expertise to be the reason they experience a breach or cyberattack. A third-party data center can provide the level of expertise to alleviate these concerns and expertly support your needs.

COMPLIANCE STANDARDS WITHIN THE DATA CENTER

The financial services industry must comply with a series of rigorous regulatory requirements including PCI DSS and ISO 27001. To support these needs and ensure its own security and compliance, a colocation provider must create and maintain a comprehensive compliance program that, at a minimum, has the following compliance certifications in place:

SOC 1. This certification addresses the internal controls related to a business' financial reporting.

SOC 2. Specifically designed for data centers and other IT providers, SOC 2 provides a comprehensive set of five criteria, known as the Trust Services Principles (TSP), for managing customer data.

PCI DSS. The Payment Card Industry Security Standards Council establishes controls to maintain network security and a risk management plan to ensure credit card information is securely transmitted, processed and stored.

ISO 27001. The International Organization for Standardization addresses risk management by assessing the people, processes and technologies involved in physical and network security. Colocation providers must plan and implement controls to manage these risks.

HITRUST. Best known for its healthcare applications, the Health Information Trust Alliance establishes a Common Security Framework (CSF) that all organizations can use to create, access, store and exchange sensitive or regulated information.

FISMA. The Federal Information Security Management Act provides guidelines and security standards for federal government agencies and their contractors. FISMA requires an inventory of information systems, risk prioritization, system security planning, security controls, risk assessments, and yearly certification and accreditation.

Don't let the data explosion compromise speed

We live in an impatient world and the financial services industry certainly feels this pressure. Businesses, customers and partners want information available instantly. The ability to quickly and securely connect to partners, customers and vendors is critical—as is the speed at which these connections are made.

Large banks with ATMs spread across the world need to ensure customers' money is dispensed quickly. A customer who waits minutes for an ATM to process a request is an unhappy customer. Having the right low-latency connections can make all the difference. The same is true for online banking. Lags in connection speed—or even worse, interruptions or downtime—can be a black mark against an organization. Ensuring a positive customer experience is vital.

Traders have an even more intense need for breakneck connectivity speed. Fractions of a second can impact customer retention and profitability, making latency this group's kryptonite.

The truth is, financial services customers have many options, and an organization that cannot meet their needs will be left behind for a faster, better-connected option. Speed to market, network agility and time to install are other major concerns. In a highly connected world, traffic spikes are an inherent part of business, and organizations need a plethora of connectivity options to ensure they can quickly turn up capacity to address new or expanded connectivity demands. As more services are delivered online and customer bases expand, additional bandwidth and new connections will be needed. A colocation provider needs to be able to meet these connectivity needs now and down the road.

FINTECH: A NEW WRINKLE IN THE LANDSCAPE

With the rapid growth of the financial technology (fintech) industry, compliance and connectivity are even more critical. Fintech takes aim at traditional financial services delivery models by digitizing more financial transactions. Fintech offerings like Venmo, Cash App, Xoom, Zelle, Circle Pay and GoFundMe have become more mainstream, and even content technology companies like Facebook, Google and Apple are entering the market with their own versions of the electronic wallet. The result is—and will continue to be—more internet traffic and more opportunities for cyber criminals.

The increase in traffic also stresses bandwidth even more—and with no end to its growth in sight, implementing the right interconnections becomes more crucial. This makes a robust interconnection

strategy essential to deliver the speed and resilience your organization needs to thrive. A third-party data center can offer the security and connections needed to meet these escalating demands.

Optimize disaster resiliency with a diversified footprint

Maintaining uptime is a quintessential business need, and an effective disaster recovery strategy is key to ensuring this reliability. This begins with the redundancies built into the data center's infrastructure and extends to a diversified footprint within high-traffic regions. Best practices dictate that organizations utilize a primary and a disaster recovery (DR) site. Partnering with a provider who can offer both is ideal.

Location is another important factor in an effective DR program. Strategically located facilities provide the necessary geographic disparity to ensure both data centers are not impacted by the same local outage. To minimize risk, sites are assessed based on the probability of intense weather conditions such as hurricanes or flooding.

Colocation can also improve the resiliency and reliability of power and cooling. By establishing multiple power feeds and regularly maintained, redundant equipment, colocation can provide an added layer of assurance around operational integrity to deal with unexpected circumstances such as a cut fiber, natural disaster or DDoS attack.

THE EMERGENCE OF THE MULTI-HUB MINDSET

Resiliency plays a major role in the operational integrity of a business. Historically, customers have wanted to reside in the data center that was a carrier hotel or the most connected hub in the city. While there is benefit to being in a highly connected facility, that does not mean it can—or should—be the only solution. For the sake of resiliency across business communities, the single hub is an outdated and liability-laden solution. Additional options have emerged in major markets offering opportunities to diversify footprints and improve resiliency.

Data centers that provide a routing infrastructure with access to multiple IP networks can offer the diversification needed to enrich resiliency. An architecture that supports dual connections to the facility, as well as redundant paths to multiple upstream IP networks, enriches resiliency. This multi-homed architecture can also optimize traffic to increase reliability and performance. In many cases, these data centers also offer more modern infrastructure with improved power, capacity and connectivity for a more dynamic environment.

Diversifying your IT footprint can also reap significant rewards. Many companies think operating out of a single location offers an ease of operations. However, there are risks involved—the most critical of which is resiliency. If the single site goes down, how do you continue to operate? For financial services companies that means your customers cannot access ATMs or online banking and investors cannot make trades.

Businesses are starting to get this message and rethinking their plans, shifting from building a large footprint within a single facility to diversifying their footprints to other facilities. This offers both physical redundancy and access to additional carriers and a new group of customers with whom you can directly connect. With multiple interconnection options in a metro area, the connectivity landscape is expanded and strengthened to ensure communication can continue if a natural disaster or planned attack impacts on site.

Connecting to the world from a third-party data center

In addition to a resilient environment, you need robust connectivity options. Financial services organizations need a variety of connections to achieve resiliency and meet the needs of various stakeholders in growing and disparate geographic markets. Because proximity has a direct impact on connectivity speed, financial services organizations need to be in key markets where a bulk of their customers reside. Utilizing a data center with a presence in that metro area can minimize hops for lower latency delivery.

The kinds and quantity of connections within a colocation facility is also a major consideration. Data centers that provide a comprehensive suite of connectivity options offer improved opportunities for low-cost, low-latency connections. Access to multiple carriers allows you to readily connect with the carrier of your choice and also heightens resiliency by offering multiple paths to divert traffic if one carrier is down. Diverse connectivity offerings allow you to choose the solution that best suits your current needs or create a variety of connections for a hybrid implementation, all within a single data center location.

In a global marketplace, financial services firms should also consider the data center providers' options for international connections. Access to subsea infrastructure is critical to any global business or business with global aspirations as these cables improve access to international locations with the lowest latency available.

A well-connected data center should provide a variety of connections as each delivers unique advantages to meet diverse connectivity needs. A mix of subsea cables, dark fiber, LIT networks, internet exchanges, cross-connects and peering are just a few of the most common and desired options. A data center should also provide access to internet service providers (ISPs) and public clouds such as AWS, Google and Microsoft. Direct connections to other businesses within the same data center can also improve deliver speed and minimize costs and connection complexity.

Adopting a third-party risk management plan

To meet the escalating demands of digital transformation and evolving compliance obligations, financial services businesses are increasingly relying on third-party data center providers to deliver the secure, connected environment they need to thrive. While third-party colocation can offer a number of benefits, it can also introduce risk. Cyberthreats introduced by third parties are a danger to every organization.

However, given the sensitive data it regularly handles and the rigidity of the regulations by which it is bound, this is more pressing for the financial services industry.

In the first half of 2019, there were more than 3,800 reported breaches totaling 4.1 billion exposed records. Third-party partners can increase this already-present risk. In fact, the Ponemon Institute found that third-party breaches were responsible for 59% of U.S. data breaches. Ascension, a data and analytics company that services the financial services market, knows this well.

Ascension was breached through a misconfigured server in its third-party OCR vendor's environment. The breach exposed millions of bank loan and mortgage documents with sensitive data from major financial players including CitiFinancial, HSBC Life Insurance, Wells Fargo and CapitalOne.

The risk is all too real and hitting too close to home—and CISOs are worried with 60% reporting an increased concern about a data breach caused by a business partner, vendor or third-party contractor.

To mitigate third-party data center risk, financial services firms need to assess the reliability and resiliency of their colocation facilities and their commitment to mitigating evolving threats. This is an ongoing effort that extends for the life of the relationship. Due diligence at the beginning of the relationship is far from enough as Gartner reports that more than 80% of legal and compliance leaders said that third-party risks were identified after initial onboarding and due diligence—a testament to the danger of evolving threats.

> **Third-party breaches cost more than $370,000 more than in-house breaches.**
>
> Ponemon's 2019 Cost of a Data Breach

BUILDING A TPRM PLAN

The frightening reality is that only 41% of organizations have a fully mature Third-Party Risk Management (TPRM) plan in place and a third have no plan at all. A continued effort to ensure your data center provider remains vigilant in addressing emerging risks and delivering a robust security program is critical.

According to Gartner, "Traditionally, 73% of effort devoted to risk identification is allocated to due diligence and recertification efforts, with only 27% of effort allocated to identifying risks over the course of the relationship." When it comes to evaluating risk, compliance is a minimum security foothold. A TPRM plan will help your organization assess if your third-party colocation provider has done the required amount of work to manage the risk. To best manage the evolving threat landscape, your TPRM plan needs to be an ongoing, proactive and multifaceted endeavor that measures and controls this outside risk to limit any operational exposure.

A strong TPRM program is essential because you are only as secure as your third-party providers.

Third-party security can be assessed based on quantifiable metrics such as security ratings, which evaluate and grade a data center's security performance. These security ratings provide ongoing, up-to-date and objective insight into the security health of the organization. Ultimately, your organization needs to be willing and able to walk away from a provider that harbors too much risk. Your reputation, operational integrity, financial stability, success and business continuity are on the line. Risk management cannot be a static endeavor. A TPRM plan needs to be more expansive to truly assess a data center's evolving risk surface and its response program.

QTS expertly balances compliance and connectivity

QTS, a leading provider of hybrid colocation and mega scale data center solutions, is dedicated to being a strategic partner. QTS delivers world-class infrastructure and security that meets the financial services industry's rigorous expectations, while offering powerful interconnections with the speed, reliability and service options financial services organizations need.

QTS data centers are the home to more than 200 financial services firms, including three of the world's largest.

QTS VALUES THIRD-PARTY RISK MANAGEMENT

QTS takes security and compliance to heart. Its infrastructure services have been designed to meet or exceed every compliance obligation including SOC 1, SOC 2, PCI DSS, ISO 27001 and HITRUST. Additionally, seven of its data centers have gone through the FISMA High Compliance program. QTS has adopted, implemented and maintained these programs, routinely validating its compliance with each program through an independent third party.

To provide customers with insight into its security and compliance programs, QTS has joined Shared Assessments, a membership-driven organization focused on third-party risk management. This organization manages a 900-question report designed

to help businesses assess third-party provider risk. To protect its environment—and its customers—QTS is committed to identifying potentially threatening internal and external events, putting controls in place to mitigate risk.

"QTS has implemented a risk-based information security and physical security program to identify, assess and manage the risks we face as a data center and third-party provider," said Andrew Wild, Chief Information Security Officer for QTS. "This risk-based program positions us to better address the needs of our customers in the financial market."

QTS is also dedicated to complete data center transparency. By digitizing the data center, QTS provides customers with critical insights and valuable real-time details. This level of detail is delivered via QTS' Service Delivery Platform (SDP), a real-time data center management and optimization platform. Through SDP, you can monitor and control physical access to your environment, view power consumption, order cross-connects, manage assets, log tickets and more in live-time. To address the strict security and compliance standards of the financial services sector and support auditing requests, SDP also provides a self-service library of QTS compliance documentation as well as a detailed log of data center access. This transparency helps customers better manage their TPRM program.

FLEXIBLE, ROBUST CONNECTIVITY TAKES ON THE CHALLENGES OF DIVERSE NEEDS

QTS' established ecosystem has been built and enhanced over the years to create robust connectivity hubs in major metro regions. Its suite of connectivity options allows you to devise the connected environment that best meets your existing needs, while offering the flexibility to address future demands. This diverse and dynamic ecosystem includes dark and lit fibers, direct connections, cross connections, internet exchanges, peering and more.

This network of interconnections poises QTS to challenge the single-hub mindset and offer a new level of geographic resiliency. "We've invested in our data center ecosystem to provide the dynamic connectivity options the financial services market needs to thrive," said John Ferrel, senior director, cloud and network engineering services development for QTS. "Our data centers are connectivity hubs that offer improved security, interconnections, and space and power capacity. Our innovative approach to data center connectivity provides modern options in major markets for more low-latency connections."

QTS is also data-center neutral to allow you to connect with non-QTS customers in a QTS data center without a fee. This level of flexibility is not available at other data centers.

THE QTS DIFFERENTIATORS

QTS offers a host of value-added capabilities not found at other data centers. Its commitment to partnership and full transparency and visibility into its environment are changing the way customers interact with their data centers.

Compliance. Supported by a dedicated compliance team, QTS provides a flexible compliance framework of physical and logical security. Its compliance certifications and accreditations include SOC 1, SOC 2, HITRUST, PCI DSS, FISMA, ISO 27001 and more. Its multi-layered physical security controls includes perimeter fencing, patrolling guards, ID checks, visitor screening, active video monitoring, and proximity card with biometric access controls.

SDP. QTS' Service Delivery Platform (SDP) takes its data center transparency mission to new levels. The API-driven platform provides on-demand, real-time access to a wealth of digitized data center information, including environmental data, physical access logs, compliance reports and much more.

Connectivity. Every data center in the QTS portfolio features robust connectivity with a diverse mix of options including dark and lit fiber providers, SDN based providers, Cloud Access, IP Services and Internet Exchanges

QTS Network Access Points (NAP). The QTS NAP locations provide access to existing fiber networks, internet exchanges, SDN networks, subsea cables and large-scale data centers located in the connectivity-rich hubs of Richmond, New Jersey and Hillsboro, OR.

Operational Maturity. QTS' in-house staff provides a level of expertise not easily duplicated internally. Its engineers have been integral in developing its products and services. This helps facilitate troubleshooting conversations and ensures experts can be quickly tapped for more immediate responses. This is demonstrated most visibly in their industry-best NPS score of 88, nearly twice that of the closest data center company. NPS is an ongoing, independent customer survey that rates companies based on customer service and the likelihood a customer will purchase again or recommend the organization to another business.

Sustainability. To support their company Core Values, QTS have set measurable, relevant and timely targets that will reduce their carbon footprint, support the clean energy industry and improve the lives of their stakeholders – including a commitment to procure 100% of power from renewable energy sources by 2025.

QTS is actively working to boost interconnections to provide businesses with more secure, low-latency connectivity options by making continued investments in building an increasingly diverse connectivity ecosystem.