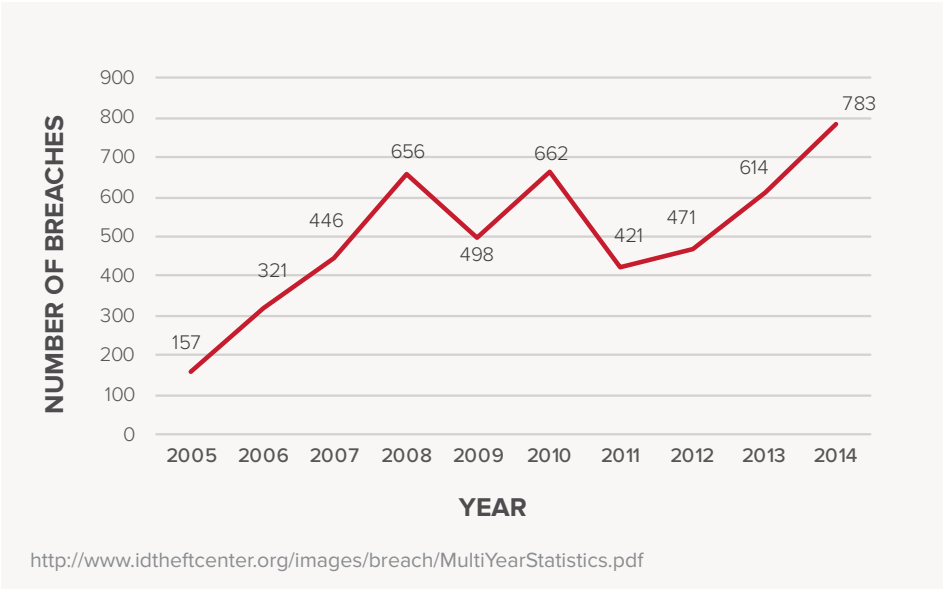
EVOLVING DATA LANDSCAPE CREATES CHALLENGES FOR ARRAY OF INDUSTRIES

OVERVIEW

As the number and frequency of data breaches increased and subsequently gained more media attention, people have become more aware and concerned about the security of their data. As businesses and agencies face increasingly complex security requirements, stringent compliance restrictions and the growing demand for immediate access to data, it makes less and less sense for these organizations to invest resources in the operation and management of their own data centers. Enterprises are leaving the data center business, opting instead to seek a partner for their data center, colocation and cloud needs.

In 2005, there were a total of 157 data breaches, according to the Identity Theft Resource Center. In 2014, that number rose almost 400% to 783 breaches – an average of 15 breaches a week. The healthcare industry experienced the most substantial jump, recording an almost 2,000% increase (16 in 2005 to 333 in 2014).

CONTENTS



http://www.idtheftcenter.org/images/breach/MultiYearStatistics.pdf

Healthcare organizations tasked with storing patients' healthcare and other personal data must comply with ever-evolving Health Insurance Portability and Accountability Act (HIPAA) compliance standards. Financial services companies must comply with Sarbanes-Oxley (SOX) regulations when handling their customers' data. And because Federal government agencies contract with outside agencies to manage their data services, those contractors must ensure they meet the requirements of the Federal Information Security Modernization Act (FISMA).

In this whitepaper, we will examine the specific challenges facing a variety of industries, including federal agencies, healthcare organizations, digital media and financial services companies.

FEDERAL AGENCIES AND THEIR PARTNER

Federal agencies and the government contractors that work with them face a number of unique challenges that go hand in hand with bureaucratic operations. From security issues to compliance requirements to working with big data, navigating the federal data services maze can be a tall order.

SECURITY

Managing data for the federal government requires the implementation of stringent security protocols. Failing to provide a high level of security can result in the compromised data of millions of Americans. In June 2015, the U.S. Office of Personnel Management (OPM) announced that the personal records of roughly 4.2 million people had been compromised in a cyber breach. A few weeks later, it was revealed that the number of people affected by the hack was actually closer to 21.5 million. Data compromised in the breach included Social Security numbers, names, dates and places of birth, as well as addresses and other information related to security clearances. Also included in the breach were 5.6 million sets of fingerprints. OPM officials later estimated the breach would cost the government $133 million, mostly for credit monitoring services for victims of the breach.

Government IT consortium MeriTalk surveyed 300 Federal IT managers about current security efforts, key threats and recommended improvements. According to their study, the number of reported breaches on U.S. Federal computer networks rose 73 percent between 2009 and 2014. Two-thirds of the managers interviewed, expressed concern about security as they work to modernize their data centers, especially when it came to migrating to public, private or hybrid clouds. While 72 percent of respondents graded themselves at an A or B level for their efforts to maintain security through the modernization process, more than half said they are missing some key security measures.

Due to the nature of the data the government stores, they are valuable target for hackers. With attacks on data systems becoming increasingly more and more sophisticated, opportunities are expanding for government contractors. As such, there is a large sum of money budgeted by the government for cybersecurity contracts with private sector businesses. Between 2015 and 2020, MeriTalk projects $65 billion will be spent by Federal agencies as they work to modernize and secure valuable data, while at the same time working to consolidate their data centers. In fact, 67 percent of federal managers say they intend to increase spending on cybersecurity in the next year.

Between 2015 and 2020, MeriTalk projects **$65 billion will be spent** by Federal agencies as they work to modernize and secure valuable data, while at the same time working to consolidate their data centers.

COMPLIANCE

Maintaining compliance with federal requirements is also a challenge. Government agencies and their contractors must comply with Federal Information Security Management Act (FISMA) guidelines. Under the law, which was enacted in 2002 as part of the E-Government Act, federal agencies are required to create and implement a plan to secure all data from unauthorized access or use. That law was updated in 2014 by the Federal Information Security Modernization Act, which streamlined security reporting and increased information sharing on data breaches.

In 2010, the federal government elected to institute a "Cloud First" policy in order to increase computing power and flexibility, as well as save money. In 2011, the Office of Management and Budget (OMB) created the Federal Risk and Authorization Management Program (FedRAMP) to provide oversight and security protocols for cloud services. While FISMA is the approval process for on-location data centers, FedRAMP is its counterpart for cloud services. Any cloud provider that wants to work with government agencies has to be FedRAMP compliant.

Compliance requirements continue to evolve as new regulations are introduced, creating even more complicated, time-consuming management to maintain.

As government officials turn to advanced analytics to aid in the decision making process across an array of federal agencies, there is growing concern about how to provide cost-effective access to the massive amount of complex data needed to drive those analytics.

In March 2012, President Obama announced the "Big Data Research and Development Initiative," committing more than $200 million to improve the government's ability to collect and analyze big data.

Big data can include anything from telephone and bank records to video surveillance to medical imaging and biological samples, like DNA. But big data requires big storage, which puts a strain on existing data center resources and subsequently, the IT budget. Once you have storage space for the data, it takes extensive computing power to analyze the data and turn it into something useful. And these increased storage and computing resources place more demand on a data center's power grid.

FEDERAL DATA SOLVED

Providing data solutions for government organizations certainly presents its own set of distinct challenges, not only for the organization itself, but also for contractors working alongside the agency. That's why teaming up with QTS to provide government agencies with a customized technology strategy can improve efficiency, agility and innovation ability.

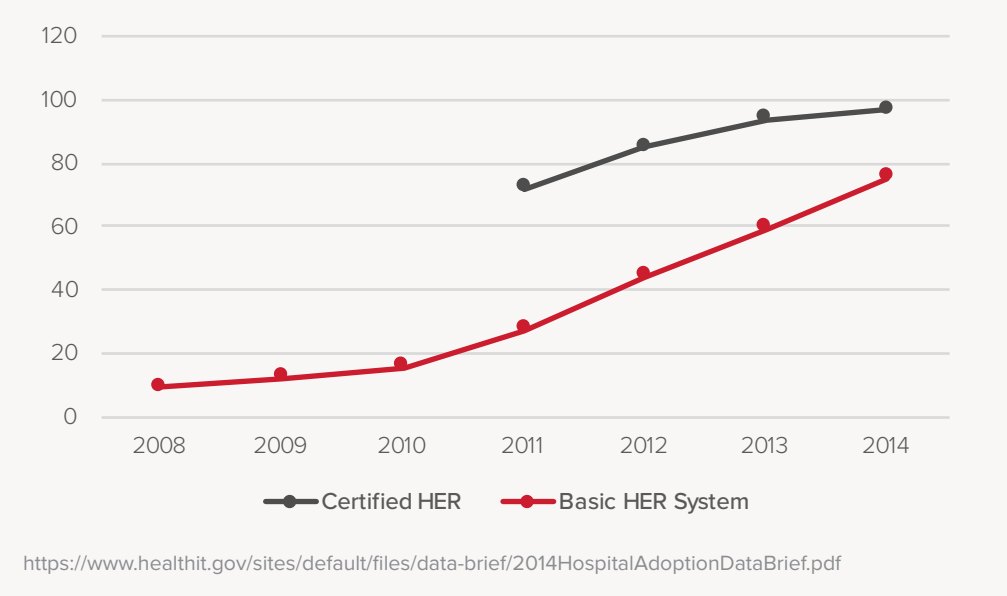
QTS operates two data centers in the Washington DC area - Richmond and Dulles - and supports customers across the Federal, Civil, DoD and Intelligence Community sectors. Whether your agency needs to build infrastructure or move applications to a virtualized platform, QTS' team of experts can design and implement a custom IT infrastructure that meets your security, compliance and big data requirements.

HEALTHCARE ORGANIZATIONS

As healthcare organizations digitize more and more of their patient records and other healthcare-related information, the data center becomes a vital part of their day-to-day operations. These data centers must be able to grow to accommodate the influx of data while at the same time keeping that data secure. Meanwhile, the data has to be easily recoverable in the event of a disaster – a time when the inability to access crucial data could be a life or death matter.

DATA STORAGE

The adoption of electronic health record systems by hospitals grew 27 percent from 2013 to 2014 and more than eight times from 2008 to 2014, according to research by the Office of the National Coordinator of Health Information Technology. The amount of data that must be stored at hospitals, clinics and other healthcare entities is increasing - from laboratory tests to x-rays and other diagnostic images, the server space required to store the records is growing exponentially. Add to that, the amount of new data coming into the EHR system to the archival storage requirements, and the results are staggering.



https://www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf

DATA SECURITY

The International Data Corporation predicted that in 2016, one in three individuals would have their healthcare records compromised by cyber attacks. Add this to the fact that since 2009, 120 million people have had their healthcare data compromised in 1,100 separate breaches, according to the Washington Post. And healthcare information is valuable to criminals. The FBI said stolen records can be sold for as much as $50 each[1] - a sizeable amount of money, when one considers the number of records stolen in the last six years. All the more reason why healthcare organizations face increasing pressure to secure their patients' records.

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), organizations can face stiff financial penalties if healthcare data is stolen. The cost of a HIPAA violation can reach $1.5 million in civil damages[2].

DISASTER RECOVERY

Whether it is of the man-made or natural variety, a disaster can result in serious problems for a healthcare organization if it doesn't have a proper plan in place. If a disaster occurs and the main data system is compromised or inaccessible, healthcare organizations must be able to quickly transition to a backup system without interrupting functionality or losing data along the way.

[1]http://www.infoworld.com/article/2983634/security/why-hackers-want-your-health-care-data-breaches-most-of-all.html

[2]http://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

Patients' lives rely on a medical staff's ability to access their medical records. Failure to maintain that access could have catastrophic consequences. In addition, HIPAA-compliant organizations are required to have a plan in place to guarantee access to electronic health records should a system go offline.

HEALTHCARE DATA SOLVED

Healthcare organizations face ever-changing compliance standards and increasingly complex security needs as they work to manage and protect their patients' data. By leveraging QTS Healthcare Solutions, you can work with a specialized team of healthcare data experts who will partner with you to reduce capital expenses while improving data security and access.

QTS has HIPAA-compliant mega data centers and HIPAA-compliant cloud services, allowing you to quickly scale your data needs without compromising the security of your data. With the experience and technology, QTS can protect your data and ensure 24x7x365 availability while you focus on caring for your patients.

HIGH-TECH BUSINESSES

In fast-moving cloud and mobile environments where development speed is everything, high-tech organizations have a difficult task on their hands. Likewise, enterprises in the digital ecosystem must deliver their websites and applications to a demanding global audience – a task that comes with its fair share of challenges. Content providers, digital retailers and other similar high-tech companies need to ensure consistent uptime and fast speeds around the clock; anything less jeopardizes revenue growth. On top of that, these organizations need to be prepared to handle the peaks of usage without wasting resources, even in the face of unpredictable traffic patterns and computing demands.

INTERNET OF THINGS (IOT)

As the Internet of Things becomes more prevalent – IDC projects the market will grow from $655.8 billion in 2014 to $1.7 trillion in 2020 – there will be an ever-growing demand on IT departments and the data centers they manage. In fact, it is projected that the number of devices connected to the Internet of Things will be double the global population in 2018 – and with that comes an increased demand for data storage and accessibility.

AVAILABILITY

Regardless of geography, today's Internet users require a high-quality online experience on a variety of devices – from computers, to tablets and mobile phones. That means downtime must be kept to a minimum. Users, especially those using IoT services, expect their devices and apps to be constantly available. A 2013 Ponemon Institute survey placed the cost of unplanned downtime at $7,900 per minute, up 41 percent from $5,600 per minute in 2010[1].

[1]http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/infographics/documents/ponemon-infographic-cost%20of%20downtime-r11-13-final.pdf

A 2013 Ponemon Institute survey placed the cost of unplanned downtime at **$7,900 per minute,** up 41 percent from $5,600 per minute in 2010.

CONNECTIVITY

A 2014 survey by Forrester Research found that connectivity issues were the top concern of 82% of the IT managers surveyed[1]. Companies must be able to consistently deliver fast speeds so as not to jeopardize revenue. Additionally, digital companies have to be able to cope with peak usage while not wasting resources, even when traffic patterns are unpredictable.

HIGH-TECH DATA SOLVED.

QTS' international network of data centers provides a redundant, robust and dependable platform – ideal for workloads that demand high performance, high transaction volumes and low latency while processing vast amounts of data reliably and cost-effectively.

FINANCIAL SERVICES

Like the healthcare industry, businesses in the financial services sector have strict federal regulations. Because of the highly sensitive nature of the data they store, these companies must also pay close attention to the security protocols used to protect their data.

COMPLIANCE

The Sarbanes-Oxley Act of 2002 (SOX) was signed into law after a rash of corporate scandals, including Enron and Worldcom. While designed to protect shareholders and the public from accounting errors and fraud, SOX also has stringent data storage requirements . SOX-compliant data centers are required to have systems to regulate data access and encrypt financial information. They must also submit to regular audits to ensure compliance.

Data centers that deal with credit cardholder data should also implement the Payment Card Industry Data Security Standard (PCI DSS). While this isn't required by federal law, compliance with PCI helps vendors avoid possible liability in the event of a data breach.

SECURITY

The number and scope of cyber attacks on financial institutions has increased dramatically in the last two years with losses totaling in the billions of dollars. As hackers become better organized and better funded, global IT security spending will continue to grow – Gartner projected their spend to grow 8% to almost $77 billion in 2015[2]. Because the trust of a client is key to financial institutions, securing clients' financial information must be a top concern for financial services providers.

FINANCIAL SERVICES DATA SOLVED

QTS delivers an integrated platform of colocation, cloud and managed hosting solutions designed to simplify strategies for our customers by delivering increased IT efficiency and reduced capital expenses. QTS' international footprint of data centers provides a redundant, robust and dependable infrastructure, ideal for workloads that demand high-performance, high transaction volumes and low-latency, while processing vast amounts of data, reliably, securely and cost-effectively.

[1]http://www.datacenterdynamics.com/app-cloud/network-connectivity-and-resilience-still-top-us-data-center-priorities/86696.article

[2]http://www.gartner.com/newsroom/id/3135617

DATA SOLVED

IT decision makers are in complex, high-pressure environments and they need a partner to help manage and protect their critical data during a time of unprecedented change. We are proud to be the only fully integrated data center, managed hosting and cloud services company that relies on people first to provide advice, technology and infrastructure to meet their evolving needs. At QTS, our job is to help you overcome critical data challenges and "Data Solved" is our promise to our customers.

At the heart of the Data Solved promise are three core attributes - People Powered, Technology Focused and Infrastructure Invested. We leverage our strong, diverse team of more than 700 employees to enable our Powered by People motto and deliver on our promise. With 24 data centers on four continents, we are poised to deliver world-class infrastructure and value-added technology services to our more than 1,000 customers in North America, Europe, Asia and Australia.

CONTRIBUTORS