Driving Resiliency and Security in the Financial Services Industry

bmc

Increased Resiliency Is Crucial to the Long-Term Success of the Financial Services Industry

The financial services industry is one of the biggest drivers of sustained economic health in America, helping to facilitate and finance the export of US manufactured goods, services, and agricultural products. According to the US Department of Commerce, the industry **exported $114.5 billion and had a $40.8 billion surplus** in the finance and insurance trade in 2017.[1]

The continued success of the financial services industry into the next decade and beyond requires more powerful IT solutions than ever before, with challenges posed by a rapidly-evolving global financial outlook, complex new security threats, and a changing regulatory landscape set to test even the industry's biggest players.

The nature of cyber threats facing financial services firms is changing fast as malicious actors develop increasingly-sophisticated methods. As part of their day-to-day operations, financial firms collect and manage massive amounts of sensitive personal data, which includes credit applications, banking details, private investment information, and more.

It is little surprise then that an industry so rich in high-value data, and one worth over $1.5 trillion, should be such a prime target. And regulatory standards around the industry are shifting rapidly to keep up with the growing data security dangers of doing business online. Increasing divergence in those global regulatory standards poses further challenges and puts the burden on firms to meet the highest possible compliance standards and security benchmarks.

As of the date of first publication of this document, the novel coronavirus COVID-19 has caused major declines in global markets, with full consequences not yet known.

[1] U.S Department Of Commerce, SelectUSA, Financial Services Spotlight, www.selectusa.gov/financial-services-industry-united-states

From the 'Reducing Regulation and Controlling Regulatory Costs' Executive Order which has significantly changed the way US-based financial businesses operate to ongoing Brexit-related regulatory challenges, firms face mounting difficulties in navigating differing regulatory landscapes.

Changes in legislation like the General Data Protection Regulation (GDPR) and Payment Services Directive 2 (PSD2) have also impacted the collection, storage, and use of sensitive private data.

Within the industry, arguably the biggest concern facing many C-suite-level decision makers is, "How can we make our company more resilient against both the threats we face and the pressures of increasingly complex regulatory requirements?"

In today's fast-paced, digital-first world, there is no allowable downtime to analyze data or remediate issues; companies must perform at peak levels while still effectively mitigating risk and meeting current and future capacity requirements.

Effective Resiliency Relies on Capacity and Security

Planning and managing IT infrastructure resource usage and costs—the foundation of capacity—is critical as the industry faces growing pressure to deliver digital services faster and more reliably.

Firms must have adequate capacity to drive availability of complex applications at all times. Disruption to everyday business activities, and even the smallest interruptions in customer experience, can cost a financial services company millions.

From a performance perspective, the root causes of any issues negatively impacting the company's ability to deliver services—and especially any issues centered on data security or vulnerability management—should be identified immediately, with fast resolution prioritized.

In fact, a recent joint report from The Ponemon Institute and IBM estimates that the average cost of a security breach is nearly $4 million.[2]

Data breaches in highly-regulated industries like financial services are even more costly than in other industries because of the potential size of the fines involved and the higher-than-average rates of lost business and customers.

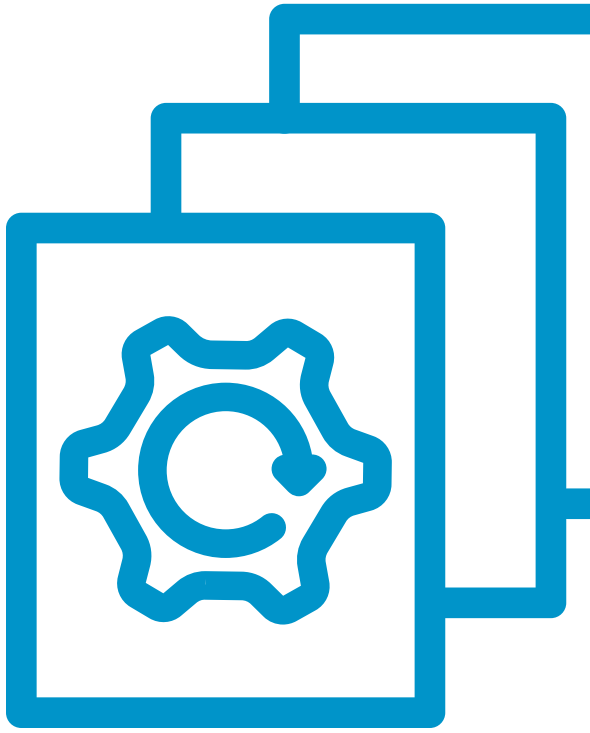
The challenge for firms as the scale and complexity of threats increase is how to maintain focus on proactively fixing security and compliance issues as early as possible while driving continuity and minimizing business disruption. With so much at stake, more financial services companies are employing a two-pronged strategic approach that combines intelligent capacity management and proactive vulnerability management.

[2] IBM, Cost Of Data Breach Report, www.ibm.com/security/data-breach

A Dual-track Plan Is Required to Support Resiliency

Both capacity planning and vulnerability management processes are needed for a variety of reasons:

- Planning solutions can help provide "right-size" capacity requirements to improve business efficiency and reduce costs
- Effective planning can inform procurement decisions by providing high-value historical data
- Automated reports can help inform key stakeholders and relieve management burdens
- Strategic performance issues impacting business development can be identified and fixed faster
- Security or compliance issues discovered later in a development cycle are costlier to fix, and incidents and compliance lapses can cost millions in fines and lost revenue.
- Managing threats will become more difficult in the future due to the growing complexity of cloud environments as well as a lack of skilled cybersecurity professionals.



Intelligent Capacity Management for the Future of Financial Services

Capacity requirements for the financial services industry are changing to meet new demands. While previously many organizations focused on capacity management infrastructure alone, we are now moving to an era of more service-aware capacity planning and forecasting.

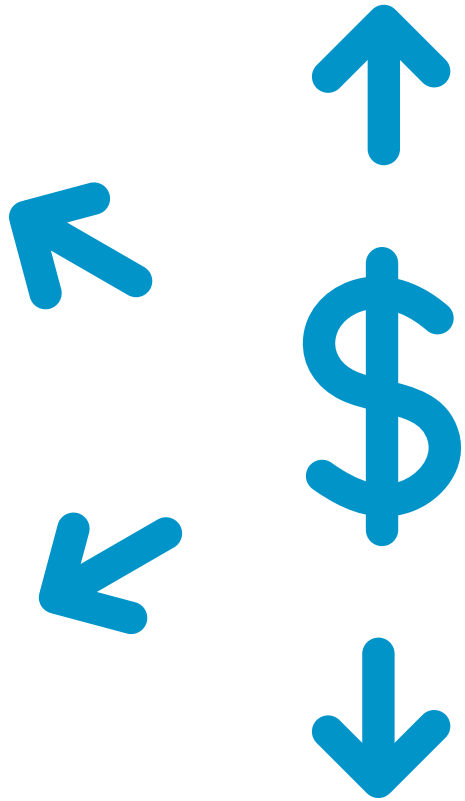
Many financial services organizations still run on the mainframe and may lack the more accurate performance reporting, business-aligned capacity forecasts, and guided workflow advantages provided by advanced automation solutions.

With the right tools, they would instead have more availability and resiliency to meet their evolving challenges and correlate infrastructure performance with business KPIs and specific metrics in mind.

BMC AMI Capacity Management uses intelligent automation to help financial services companies optimize mainframe capacity while diagnosing potential future capacity issues before they become critical.

This allows better, more accurate capacity planning and performance, greater organization-wide availability, enhanced mainframe security, and lower costs, as well as allowing firms to:

- Evaluate multiple scenarios with interactive "what if" modeling before making final recommendations
- Make informed capacity procurement decisions based on business application performance
- Track and manage performance via extensive reporting from a historical performance database
- Reduce costs by "right-sizing" the capacity requirements based on the organization's needs
- Improve productivity through intelligent, automated web-based reporting
- Drill down into root causes of performance issues quickly and accurately

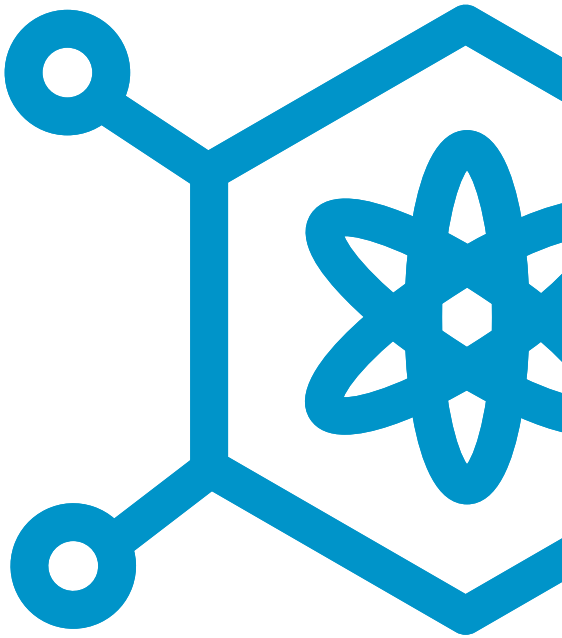


Whether managing traditional infrastructure or newer technologies, IT continues to grapple with escalating complexity in their budget. IT resources are now both capital and operational expenses, and IT must plan use of existing resources and new purchases carefully. Cloud services and containers require IT organizations to have better insight into the usage and performance of infrastructure as they may not own the physical assets on which they are run.

A future-ready capacity management solution provides visibility into the entire IT infrastructure—physical, virtual, containers, and cloud—so IT can easily adjust compute, storage, network, and other IT infrastructure resources to meet changing application and service demands.

Capacity management tools also allow firms to forecast future capacity requirements based on current and historical behavior to avoid over- or under-provisioning. Automated performance reports eliminate programming effort and can be shared quickly within ITOps as well as with relevant business leaders for greater visibility.

With **BMC Helix Capacity Optimization**, a cloud-based solution for organizations adopting new technologies, businesses can predict IT resource needs based on changes in business service demand and reserve and schedule IT infrastructure resources for releasing new applications. A single, holistic view of the state of business services across an entire enterprise is available on demand, classified by level of importance to empower relevant decision makers.



Smarter Vulnerability Management to Combat Changing Threats

The intricate regulatory landscape for financial services firms is now more difficult to navigate than at any time in the last decade. While global standards have diverged since the financial crisis, the focus in the US has remained firmly on refining or replacing existing regulations rather than introducing new ones.

To ensure good governance practices, it's crucial to understand how changes in financial compliance standards impact operations within such a regulated space. The majority of regulatory changes have occurred around the management, security, and storage of customer data.

Regulations like GDPR, PSD2, and KYC mean that businesses must proactively ensure they are improving processes and streamlining operations to stay ahead of changes.

Another driver toward achieving resiliency is the levying of heavy fines for data breaches, which can run into the tens of millions of dollars and lead to a long-term reduction in both business and consumer confidence.

Security lapses like the Capital One breach in 2019 serve as cautionary tales, with the firm reportedly set to pay up to $400 million in total costs.[3]

So how do financial services businesses ensure compliance with changing regulations while guaranteeing that the systems they have in place are agile, responsive, and dependable?

At BMC, we've worked closely with major banks, insurance companies, and other finance-focused firms throughout the U.S to help ensure the safety of their critical customer and operational data. Our cloud-based security solutions are designed to meet their unique challenges by identifying potential weaknesses, mitigating risks, and providing deeper insights into the entire business infrastructure.

[3] Forbes, 'How Could The Recent Data Breach Affect Capital One's Stock', www.forbes.com/sites/greatspeculations/2019/09/11/how-could-the-recent-data-breach-affect-capital-ones-stock

Compliance and vulnerability management are embedded in our security solutions, leveraging the power of automated remediation in service delivery and cloud operations with end-to-end visibility, continuous compliance, and powerful analytics. Regulatory requirements are also managed comprehensively, allowing systems to meet compliance criteria instantly as regulatory standards change.

BMC solutions leverage intelligent automation to proactively identify weaknesses throughout the entire IT ecosystem. With tools like **BMC Helix Remediate**, financial services companies can:

- Streamline workflows with scan verification and automated remediation
- Import and analyze data from vulnerability scanners to significantly improve response times
- Quickly prioritize remediation activities via a powerful universal dashboard
- Highlight performance trends, SLA compliance, and vulnerability lifecycle information
- Create custom reports that help meet audit requirements and fuel process improvement efforts
- Scale security with automation to manage growth of cloud applications

While today's technological advancements offer incredible business opportunity, they also bring the threat of increasingly sophisticated cyberattacks, and the use of third-party providers can lead to inconvenient and reputation-damaging service interruptions. As financial organizations look ahead to the continuing, operational, security, and regulatory challenges of the next digital revolution, it is crucial to have IT solutions that can scale to their business while meeting auditory requirements and rigorous security standards.

Embracing the possibilities of new technology and the capabilities of IT solutions that can optimize capacity, security, and compliance requirements will help today's businesses achieve the resiliency to remain successful.

To find out how BMC solutions can help your firm navigate today's digital demands, visit our solution pages at **www.bmc.com**