ExpertInsights@IBV

The modern mainframe

A banking platform from the future

IBM Institute for Business Value

Three imperative payoffs

There are three things that senior executives in the financial services industry want from their investments in computing systems. They are the same three things these institutions require for their very survival.

First is unwavering security. The integrity of customer accounts and records is paramount to maintain trust across the financial ecosystem. Cybercrime is anathema to the core function of banking and cannot be tolerated. Next is captivating, personalized experiences based on real-time data analytics leading to instantaneous customer fulfillment. And finally, there is the essential delivery of these secure experiences while providing a cost and efficiency advantage over competing solutions.

Mainframes then and now

These are the hallmarks of mainframe computing and why they're counted on for USD 7.7 trillion in annual credit card payments,[1] 29 billion annual ATM transactions[2] and 12.6 billion transactions per day.[3] And that's why 92 of the world's top 100 banks rely on mainframes to host their core systems.[4]

Of course, modern mainframe computers are very different from previous generations. In the past, they were almost always room-sized, water-cooled behemoths that were installed as much by plumbers as computer technicians. Since then, mainframes have been reinvented several times. They can be air-cooled with a much smaller footprint, come with powerful, integrated security and cryptography, and support technology including Linux, Java, Docker Enterprise Edition, MongoDB Enterprise Edition, blockchain and cloud.

In fact, the mainframe is a linchpin for the success of the cloud environment. Think about what is required for such success: security and encryption, scaling in place, real-time data analytics (without transferring data) and managing workloads. These are the emblematic of mainframes.

Mainframes provide the ability to help sustain "can't fail" core operations while providing solutions for:

- The future of banking and financial markets, which is being disrupted by next-generation transactions and technologies such as blockchain. These require new levels of speed, scale and security that only mainframe technologies can provide.
- Creating engaging experiences. Financial institutions appreciate the mainframes' ability to perform analytics "on the fly," while data is in motion.
- Highly effective system security, which is integrated within the stack, isn't something added on as an afterthought. Encrypting and protecting sensitive data is typically cheaper, easier and more effective to do on mainframes than on commodity infrastructure. This is noteworthy as highly regulated industries like financial services have some of the costliest data breaches because of fines and the higher-than-average rate of lost business and customers.

And while all this has happened, the total cost of mainframe ownership is more competitive than ever. That's why the worldwide financial services industry recognizes the modern mainframe computer as essential for conducting business and transactions that cannot afford to fail.

Let's look at some of these points in greater detail.

The perimeter against cyber-crime

When compared to alternative solutions:

Mainframes require 69% less effort to secure equivalent workloads[5]

Mainframes are more than 8X more effective at resisting security threats[6]

Mainframes provide security defense at an 84% lower cost[7]

On today's mainframe, the days of choosing what to encrypt are gone. Modern mainframes can continually encrypt everything without changing anything – including data in-flight and data at rest, with no application changes, no impact to service level agreements (SLAs), and no interruption to business operations. Consider the value of this in the complex world of digital and cloud, which has created an expanded threat landscape, making the encryption and security of sensitive data more difficult and costly than ever before.

The average cost of a breach has jumped 29 percent since 2013 and now exceeds USD 4 million.[8] A recent analysis by Solitaire Interglobal found that mainframes: require 69 percent less effort to secure equivalent workloads; are more than 8 times as effective at resisting security threats; and provide security defense at an 84 percent lower cost than alternative platforms.[9]

These capabilities extol the mainframe as the system for enabling data and the new perimeter against cyber-crime.

The encryption of data on the mainframe is supported by integrated cryptographic co-processors that reduce the cost of encryption to almost nothing. It is further hardened with a certified, tamper-responsive hardware security module for protecting keys. Policy-based management makes this system easy-to-use and low on labor cost.

Research has shown that 39 percent more of banks that outperform their peers in both revenue growth and operating efficiency have customers who report that their assets and information are safe.[10] Using mainframe pervasive encryption to protect core systems data is a solid step toward higher customer trust.

Preventing fraud "in flight"

Digitizing common banking processes and making them available online has improved customer access and experiences. But it also has increased attacks on banking data and accelerated threats to the bottom line in the form of fraudulent transactions. Although customers are typically not held liable for financial loss due to fraud, such breach of trust can have the same effect on customer loyalty and brand value as stolen data records.

Banks do take the financial hit directly, and it is significant. An IBM Institute for Business Value (IBV) study showed that direct fraud charge-offs alone can account for "more than seven basis points of revenue."[11] Still, it found that 42 percent of banking executives said their fraud operations are in need of an overhaul, and perhaps most surprising, "49 percent of these executives either wait for the customer to complain about fraud or can't detect it."[12]

It's estimated that "80 percent of consumer fraud is perpetrated by criminal organizations using multiple product channels, multiple locations, an easily recruited cadre of labor and a very short – sometimes only hours-long – campaign window for execution."[13] The only way to fight such sophisticated attacks on banks is to intervene while transactions are in flight, in real-time, before settlement.

If a transaction can be identified as fraudulent and stopped before funds are moved, the bank not only avoids losing money, it can also avoid investigative and recovery costs. The customer is not inconvenienced and trust is maintained. Yet only 16 percent of the institutions in this recent IBV survey cited the ability to detect fraud as it was attempted.[14]

It also showed that "most institutions have not undergone a fraud transformation program and 20 percent have no plans to do so."[15] The two greatest obstacles cited are perceived cost versus benefit, and the availability of necessary skills.

For banks running core operations on mainframes, neither cost nor skills are truly inhibitors to putting a real-time fraud prevention program in place. To protect customer data from unauthorized access, the modern mainframe is equipped with machine learning capabilities that easily interface with existing transactional systems, allowing its inflight transactions to be scored for fraud in real time with no SLA impact.

For example, a large Asia Pacific bank with credit card operations on the mainframe wanted to put a pre-payment, anti-fraud system in place. In 2016 alone, it managed more than 1 million incidents generating expense of approximately USD 331 million. By implementing machine learning on the mainframe and integrating directly with its transactional card system, the bank anticipates 20 percent fewer fraudulent incidents and a five-year savings of USD 336 million. The resulting alert load reduction on the fraud investigations staff could lead to further savings due to decreased support costs (USD 320 per incident) and credit card replacement costs (USD 12.75 per card).[16]

Simplifying regulatory compliance

Financial institutions need to demonstrate in an auditable way where regulated data resides, where it was last updated, who updated it and where it exists today.

Rapidly expanding financial regulations continue to dominate resources that could be better used for innovation and growth. Already experiencing USD 99 billion in annual compliance costs[17], banks expect to face upwards of 300 million pages of regulations by 2020.[18] And the penalties for non-compliance can be severe. For example, with the General Data Protection Regulation (GDPR), the European Union is seeking as much as 4 percent of overall revenues for a data privacy violation. One data security company has predicted fines of about EUR 4.662 billion in the first three years of GDPR.[19]

The strains of security and compliance are exceeding human capabilities in even the best-run organizations. Compliance must become more automated, and every layer of the organization must be inoculated against security and compliance risks by remediating vulnerabilities.

One simple way to ease the burden on core systems is by using the mainframe's pervasive encryption capability. Financial institutions are going to have to demonstrate in an auditable way where regulated data resides, where it was last updated, who updated it, and where it exists today, in terms of storage devices and disk drives. However, if such information is verifiably encrypted, the burden of proof is greatly diminished because the practice of pervasive encryption effectively decouples encryption from classification and reduces the risk associated with undiscovered or misclassified sensitive data.

Know what your customers want before they do

Sixty-two percent of banking leaders said their institutions are not effectively delivering a personalized experience.[20] Why is there such a large gap between requirement and execution? Much of the answer has to do with banks' slow mainline adoption of advanced analytics.

The sort of personalized service demanded by customers today requires increasingly deeper analytics, producing a continuous stream of insights into their needs, preferences and intentions. On the positive side, 48 percent of bankers know this, saying that investment in predictive analytics is a key priority.[21] But even as most banks are still working out how to leverage predictive analytics, the state of the art has shifted to what is called "machine learning."

Machine learning is a form of artificial intelligence (AI) on top of predictive analytics. It optimizes decisions by quickly training, deploying and monitoring a high volume of high-quality, predictive behavioral models. It continuously improves model quality by "learning" from new data.

Machine learning can enable banks to shift from a product-centric to a customer-centric business model using segmentation through demographics, daily transactions, online interactions and value of assets. It can infuse continuous intelligence into banking operations, helping to personalize and elevate customer experiences.

An overwhelming amount of the data feeding machine learning models is expected to come from core banking systems.

Insights are highly perishable. The latency resulting from extracting, transforming and loading data is simply unacceptable to banks striving to become more agile in meeting the individualized needs of customers.

The problem is that banks routinely push this sensitive data off-premises to data warehouses or cloud platforms for analysis. The time and risk involved in transferring data is a process bottleneck to effective use of machine learning. Of course, insights are highly perishable; the latency resulting from extracting, transforming and loading data is simply unacceptable to banks striving to become more agile in meeting the individualized needs of customers.

The mainframes managing banks' most valuable data are perhaps the only systems capable of running both transactions and analytics simultaneously without adversely affecting the performance of either. And modern mainframes have been optimized for machine learning to deliver in-place analysis of this valuable data without driving up cost. Some even run Apache Spark, an open-source computing framework that speeds analytic applications with in-memory processing.

As mainframe-based banking systems are touchpoints for most customer interactions, machine learning on the mainframe builds in insight and intelligence, while helping to avoid the latency and security risks of moving sensitive data.

Not only does the latency of data movement limit the effectiveness of insights, it is a costly operation. The cost of copying 1 terabyte of data per day over a four-year period has been estimated at approximately USD 10 million.[22] Analyzing data directly on the mainframe allows for acting on insights in real time and making higher quality decisions at lower cost.

Make core platforms more attractive to developers

Mainframes as a platform are the product of 50 years of innovation. Banks have been along for the ride virtually that entire time. Among the recent innovations is that current mainframes have moved beyond the traditional programming language COBOL; today, many are open source and support the latest programming languages.

With decades of constant upgrades and enhancements, the mainframe is a modern development machine – fully able to participate in the emerging dynamic hybrid banking architecture. Financial institutions can put strategies in place to exploit these technologies, creating agility and flexibility in their systems. This can take cost and complexity out of the code while maintaining a unique level of functionality and helping to deliver exceptional levels of service.

Modern mainframes work in an open and connected environment, enabling developers to seamlessly build today's business applications. They can use both legacy and open source skills and platforms, and leverage APIs for more rapid development. As a result, the time required to build new services can likely be significantly cut without the need for additional specialized skills.

> "While there have been some success stories of banks using a 'rip and replace' approach to core system modernization (particularly among smaller institutions that provision their core systems from managed services providers), the streets are littered with as many, if not more, examples of core banking replacement projects that failed, stalled, or never delivered on the promise of simplification and agility."

IDC[23]

Pricing flexibility

In addition to the various potential cost advantages described throughout this report, modern mainframes offer innovative new pricing options. This simplified pricing is extremely competitive with public clouds and on-premises commodity infrastructure, with the inherent security and transaction capability of mainframes.

New pricing models support new workloads without affecting existing workloads. For example, a payment system pricing solution can be based on the volume of payments a bank processes rather than available capacity. This gives organizations greater flexibility to innovate affordably in a competitive environment, particularly in the fast-growing area of instant payments. New pricing options can give clients added predictability and line-of-sight on pricing.

Financial institution executives around the world rely on mainframes for stellar security and encryption, powerful customer experiences and competitive, predictable pricing. The mainframe has become a modern computing platform for the modern world of banking and finance.

Notes and sources

[1] IBM Institute for Business Value analysis based on internal data.

[2] IBM internal analysis based on a correlation of ATM machine statistic data from ATMIA, National ATM Council with IBM data on known mainframe clients.

[3] IBM internal measurements.

[4] IBM Institute for Business Value analysis based on internal data.

[5] "Cyber Crime: Keeping Data Safe from Security Incursions." Solitaire Interglobal. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=ZSW03297USEN&attachment=ZSW03297USEN.PDF

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Brill, Jim, Nicholas Drury, Anthony Lipp, Anthony Marshall and Likhit Wagle. "Banking redefined: Disruption, transformation and the next-generation bank." IBM Institute for Business Value. October 2015. https://www-935.ibm.com/services/us/gbs/thoughtleadership/bankingredefined/

[11] Davis, Wilson and David Dixon. "Winning the face-off against fraud: How the most effective financial institutions are outthinking the bad guys." IBM Institute for Business Value. January 2016. https://www-935.ibm.com/services/us/gbs/thoughtleadership/fightingfraud/

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] bid.

[16] IBM internal data.

[17] "Finance in Focus Podcast: The Future of #Regtech is Cognitive." IBM. November 22, 2016. http://www.ibmbigdatahub.com/podcast/finance-focus-podcast-future-regtech-cognitive

[18] "With Watson Financial Services, IBM Launches Cognitive Era of RegTech." IBM News Release. June 14, 2017. https://www-03.ibm.com/press/us/en/pressrelease/52573.wss

[19] Press release. "GDPR: Banks, Breaches and Billion Euro Fines" AllClearID. June 14, 2017. https://www.allclearid.com/business/newsreleases/consult-hyperion-forecasts-banks-face-fines-totalling-e4-7bn-first-three-years-gdpr/

20 Drury, Nicholas, Allan Harper, Anthony Marshall and Sandipan Sarkar. “Breakthrough banking: Your cognitive future in banking and financial markets.” IBM Institute for Business Value. October 2015. https://www-03.ibm.com/systems/data/flash/ae/cognitive-bank/res/assets/Breakthrough_banking_Exec_Report.pdf

21 Brill, Jim, Nicholas Drury, Anthony Lipp, Anthony Marshall and Likhit Wagle. “Banking redefined: Disruption, transformation and the next-generation bank.” IBM Institute for Business Value. October 2015. https://www-935.ibm.com/services/us/gbs/thought-leadership/bankingredefined/

22 “The ETL Problem Solved: The Compelling Financial Case for Running Analytics on the Mainframe.” Clabby Analytics. April 2016. http://nebula.wsimg.com/be9fe8f31972a9fc8c535c0661d49412?AccessKeyId=CCAA67622F6695DC4DB7&disposition=0&allow-origin=1

23 Silva, Jerry, Karen Massey, Lawrence Freeborn. “Perspective: Core Abstraction – Rethinking Core System Modernization.” IDC. December 2016.

About ExpertInsights@IBV reports

ExpertInsights@IBV represents the opinions of thought leaders on newsworthy business and related technology topics. They are based upon conversations with leading subject matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

Experts on this topic

Likhit Wagle

General Manager
Financial Services Sector
IBM Asia Pacific
https://www.linkedin.com/in/likhit-wagle-8a3a2416/?ppe=1
Likhit.Wagle@uk.ibm.com

Chae H. An

Vice President and Chief Technical Officer
IBM Financial Services Sector
https://www.linkedin.com/in/chaean/
chaean@us.ibm.com

New Orchard Road
Armonk, NY 10504
Produced in the United States of America
September 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an “as is” basis and IBM makes no representations or warranties, express or implied.