PKWARE®

Spotlight on Mainframe Security: Data Protection at the Heart of the Enterprise

PKWARE WHITE PAPER

Table of Contents

Spotlight on Mainframe Security: Data Protection at the Heart of the Enterprise

In the past, several articles and white papers have focused specifically on issues of data security, risk, and appropriate controls. While information security is a pervasive need, relatively few mainframe professionals focus on data security as a discrete discipline, even though the mainframe is central to many applications and exposed to great risk. Moreover, the majority of mainframe focus has been on operational excellence, increasing the return on investment, as opposed to focusing on protection of the data assets it contains. As a result, many seasoned mainframe workers and managers could still benefit from a broader understanding of information security risks and remedies.

Data Processing on the Mainframe

Data security must start, not with the tools or techniques required to create it, but with an understanding of why it is necessary. In the earliest days of computing, data security consisted of no more than "Barney Fife" sitting at the door of the glass house, only letting those in whom he knew and trusted. Today, however, the mainframe exists in a world of pervasive "connectedness," when immediate responses are required to meet business needs. The mainframe is no longer restricted to an SNA network, but now is connected via TCP/IP, just like Windows® and UNIX® servers. Organizations must maintain a permeable perimeter while constantly exchanging data - much of it sensitive and regulated - if they expect to compete effectively in the market place. The mainframe must now defend against incursions that were unthinkable as little as a decade ago.

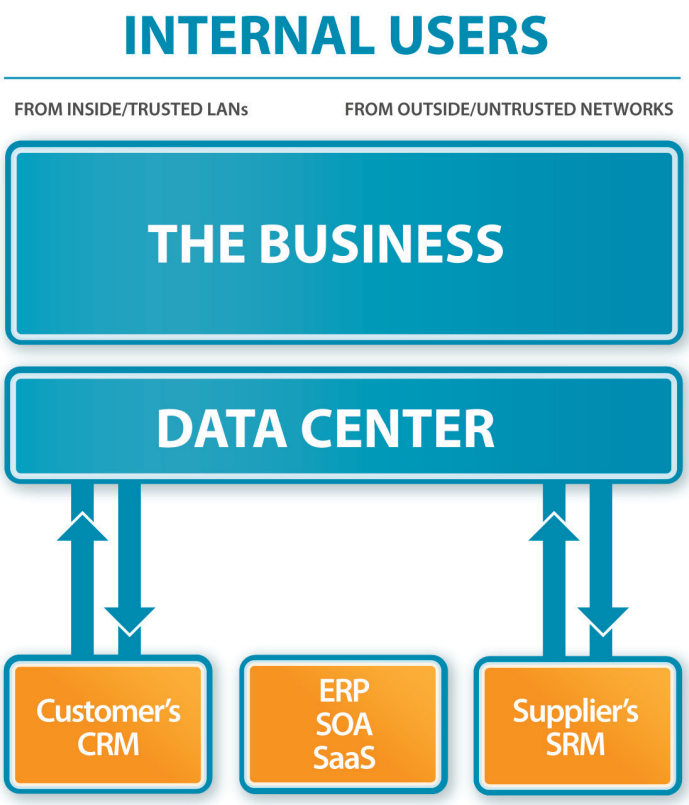

Figure 1: The Age of Pervasive Connectedness

Data processing on the mainframe is always a balancing act of usability, cost, and security. The increased need for data protection has escalated as the need to collect and deliver data via the Internet emerged at the end of the last decade. That need increased far more quickly than many organizations were able to accommodate, leaving exposures in virtually every industry. While the mainframe remains the most secure commercial data processing environment available, it no longer operates in monolithic isolation. Contemporary mainframes host web sites, allow PC client applications to access and update data, and constantly exchange bulk data files with other operating environments.

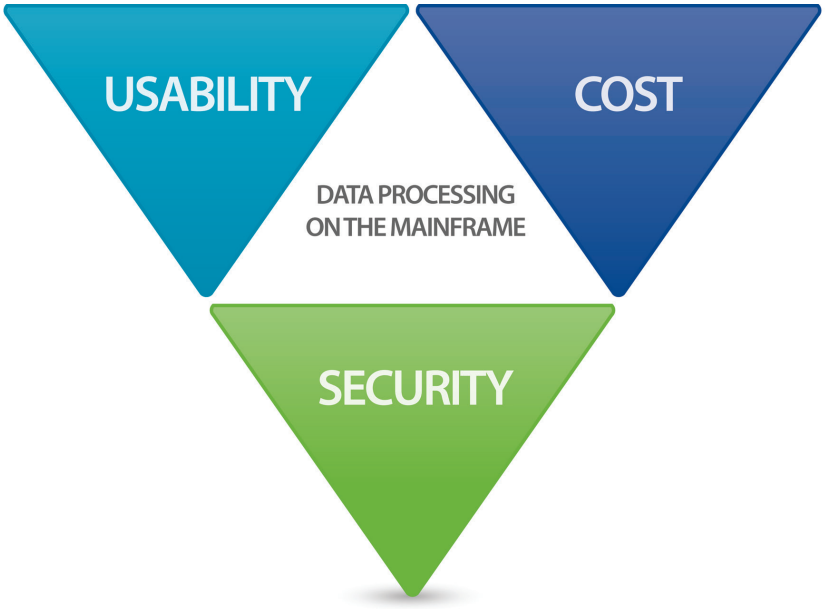

Figure 2: Data Processing on the Mainframe

Risks & Regulations

The gap between the need for security and risk remediations applied, remained so broad for such a period of time that regulators, both public and private, were compelled to take action. The EU (European Union) brought forward the Data Protection Act of 1998 (a modification of the earlier European Data Protection Directive of 1995), specifying when data may be used and, particularly, when and how it may be transferred from one country to another. The United States Federal Government passed the Gramm-Leach-Bliley Act (GLBA) of 1999 requiring financial institutions to diligently protect the privacy of consumer personal data. Finding that insufficient, a majority of states in the US, starting with California in 2003, subsequently expanded that regulation by requiring any organization to publicly disclose details when a breach of their data protections occurs. Private industry joined the call for higher data protection standards, particularly in the electronic payments arena, consolidating five separate initiatives into the Payment Card Industry Data Security Standard (PCI DSS) in 2004. The US Health Insurance Portability and Accountability Act's (HIPAA) privacy rule became effective in 2003, regulating protection of health information; it is now modified by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 to require disclosure of data breaches for any organization dealing with any aspect of health care.

Consequently, data center managers are compelled to take action both to appropriately protect customer and company data, and to avoid penalties and disruptions to the organization's business plan that regulators and auditors can represent. This means that managers must not only manage the traditional data center risks such as environmental (e.g., earthquake, tornadoes), social/political (e.g., war, riots), and operational (e.g., hardware failures), they must also consider issues of data integrity (e.g., hacking, disgruntled insiders), data availability (e.g., denial-of-service attacks), data authenticity (e.g., man-in-the-middle attacks), user access to resources (e.g., identity management), and data confidentiality (e.g., malicious and unintentional data leakage).

PRIVACY	ACCESS CONTROL	AUTHENTICITY	INTEGRITY	CONTINUITY	EX-PERIMETER	OPERATIONS
Storage	Identity	Spoofing	Internal Negligence	Physical Environment	Geographic Separation	Time Constraints
File Transmission	Social Engineering	Man-in-the-Middle	Internal Malice	Hardware Failure	Customer Communication	Limited Capacity
Email	Malware	Application	Impersonation	Software Conflicts	Vendor Management	Labor Availability
Removable Media	Facility	Device	Thrill Hacking	Social/Political Environment	Partner Coordination	Modernization

Figure 3: Results in a Range of Risks, Old and New

PRIVACY	ACCESS CONTROL	AUTHENTICITY	INTEGRITY	CONTINUITY	EX-PERIMETER	OPERATIONS
Encryption	IAM	NAC	Log Analysis	BCP	Policy Alignment	Critical Path Tuning
VPN	User Education	PKI	Event Monitoring	Redundancy	Secure Communication	Performance Tuning
Portals	Man Traps	White Listing	PKI	Integration Testing	Application Integration	Product Consolidation
DLP	Rights Management	Media Access Control	Intrusion Prevention	Geographic Diversity	Data-Centric Security	Insulation

Figure 4: Requiring an Array of Responses

Managers, then, are compelled to consider a range of responses to these risks that branch far afield of the traditional data security domain for the mainframe. Traditional disciplines of business continuity planning and testing to counter environmental, political, or operational concerns and Identity & [resource] Access Management (IAM) to restrict rights, are now only the beginning. Encryption for data privacy protection, automated log review for data integrity monitoring, realignment of batch update processes to ensure "multiple nines" availability, smart personal identity verification (PIV) technology for data and user authentication, and more – all must become part of the mainframe data center manager's repertoire for success.

The mainframe has always been considered the heart of the data center and information the lifeblood of an organization. An awareness of data security issues being faced today provides a foundation for understanding and reacting to those issues. Below are examples of several issues that managers now face:

1) Data Privacy: The Cornerstone of Contemporary Compliance

Every connection, every database extract, every write to removable media (including backup tapes), and every transaction represents a risk. After decades of focus on operational ex cellence and tuning jobs to fit tight batch windows, managers must now maintain those trends while introducing previously uncontemplated steps to protect data if it is lost or stolen. Exploring how risks to the confidentiality of data on the mainframe has changed with the advent of pervasive connectivity, increased integration with partners, customers, and vendors, and what advantages the mainframe offers for mitigating the risk of data breaches is an essential part of meeting contemporary compliance issues.

2) Resource Access Control: z/OS Resource Control & the Three Security Servers

Appropriately granting and restricting the rights of users to mainframe resources (i.e., applications, storage, and data) was once the bulk of all mainframe data security activties. However, today the need for identity and resource access management on the mainframe to mitigate inappropriate use of applications and data is essential. This includes comparing & contrasting how such an agreement is implemented by the three security servers: IBM® RACF, CA® Top Secret, and CA ACF2, as well as understanding how the three security servers are evolving to serve X.509 digital certificates for identity authentication and other uses to illustrate their role in an enterprise PKI.

3) Data Authenticity and Endpoint Security: Defending the Pervasively Connected Mainframe

Mainframe modernization, via Service Oriented Architecture, has made great impacts in terms of risks to the quality and accuracy of data. Even though the mainframe has the most durable protections in the industry, the necessary integration with user productivity interfaces has opened the door to man-in-the-middle attacks and other threats that must be addressed.

4) Data Integrity: Maintaining Consistency throughout the Data Lifecycle

Data integrity risks for the mainframe data center range from internal user negligence to potential attacks by organized criminals. Information Data Lifecycle Management from structured data sources expanding out to unstructured data sources, as well as the policies for the governance of enterprise security, plays a large role in ensuring protection from these various risks.

5) Security & Business Continuity: Staying a Step Ahead of Disaster

Business continuity extends beyond protecting against natural and man-made disasters; it also includes protecting against vulnerabilities in hardware and software components, both at the perimeter and from insider threats. This requires positioning application availability and business continuity management within the larger framework of mainframe data centers and information security.

6) Ex-perimeter Security: Data Exchange Across Operating Systems

Organizations must adopt a means for mitigating the external risks of data breach and compromise to the same degree as applied to internal risks. Certain requirements must be taken into account when exchanging data across operating systems, including the diversity of your own infrastructure and the unknown infrastructures of your customers, partners, and vendors.

7) Security Optimization: Enhancing Performance while Reducing CPU & Elapsed Time

With increasing requirements for data security and encryption, organizations must not just look to satisfy the requirements of data security and privacy; they must also look at how data security can be efficient and cost effective. Common ways of optimizing data security and encryption for best performance include reducing CPU and elapsed time.

Conclusion

Data security will always operate as something of an "arms race." As identified risks are mitigated and appropriate controls established, new threats arise from data thieves and cyber vandals. In addition to primary considerations that all organizations must address, gathering further insights into how some have addressed specific issues can be a great benefit to helping you protect your organization.

About the Authors

Joe Sturonas, Chief Technology Officer, PKWARE, Inc.
Joe Sturonas was previously CTO of Premonition Software, as well as Spirian Technologies. He was also a founding member of OneNetPlus.com, an Internet-centric Management Service Provider. Mr. Sturonas holds a MS degree in Computer Science from DePaul University.

Jeff Cherrington, Vice President of Product Management, PKWARE, Inc.
Jeff Cherrington was previously Vice President at Bank One, Director of Product Management & Consulting Services for WorkPoint, Inc., and has also worked with other top U.S. and international financial services companies. Mr. Cherrington has an Executive MBA degree from the University of Nebraska.

About PKWARE, Inc.

As the inventor and continuing innovator of the ZIP standard, PKWARE, Inc. is a global technology leader known around the world as the expert in data compression and file management. With the launch of SecureZIP in 2005, PKWARE successfully entered the data security marketplace, combining ZIP compression and strong encryption to deliver a data-centric security solution. Today, SecureZIP and PKZIP are used by over 200 government agencies and 30,000 corporate entities, including 90% of the Fortune 100. Organizations in financial services, banking, government, healthcare, and retail use PKWARE solutions daily to protect sensitive data, meet compliance requirements, avoid liability risk, and reduce their overall costs and operational overhead. PKWARE, a privately held company, was founded in 1986 and is based in Milwaukee, Wisconsin; additional offices are located in New York, Ohio and the United Kingdom.

United States
648 N. Plankinton Ave., Suite 220
Milwaukee, WI 53203
1.888.4.PKWARE
www.pkware.com

UK/EMEA
Crown House
72 Hammersmith Road
London W14 8TH
United Kingdom

PKWARE®