

Security Advantages of IBM System z9 and Virtualization on z/VM (Business White Paper)

Prepared for:
Gerald Araneo
IBM

By:
Sine Nomine Associates
43596 Blacksmith Square
Ashburn, VA 20147

February 28, 2007
SNA Proprietary - Confidential

Copyright © 2006-2007 Sine Nomine Associates

All rights reserved.

Table of Contents

1	EXECUTIVE SUMMARY	4
2	INTRODUCTION	5
2.1	System z9 Overview.....	6
2.2	Virtualization and z/VM	6
2.3	Security Considerations	7
3	MANAGEMENT & ENVIRONMENT - DEPLOYMENT SCENARIOS	9
3.1	Nexxar Group, Inc.	9
3.2	University of Toronto.....	11
3.3	Business Resilience and Agility	13
4	THE FINANCIAL RISKS OF A SECURITY BREACH	15
5	CONCLUSION	17
	APPENDIX A – REFERENCES	1

1 Executive Summary

As part of a larger series of papers on the position of mainframe technology in the current IT market, this paper considers the importance of security in the decision process for organizations that may not be traditional mainframe environments, but are now considering System z as part of larger strategies within an increasingly compliance-oriented marketplace.

This white paper is focused on the security benefits of virtualization on the IBM System z9 Business Class (BC) processors combined with the z/VM Operating System. This combination is an excellent platform for hosting hundreds of Linux images in virtual machines on a single System z, either as a stand-alone Linux consolidation server, or with Linux images on the same servers with the z/OS mainframe operating systems. (Note: this paper is not intended to address the z/OS aspects of security, which are well-documented in a wide variety of other IBM publications.)

The paper is intended for prospective and current customers who are concerned with strengthening data security without impeding efficient access and speedy information flow to users. Mid-sized businesses are expected to benefit most from the IBM System z9 BC which is targeted specifically to the needs of this fast growing mainframe market segment. The paper discusses security benefits in the context of actual customer environments.

The following sections:

- Describe the security capabilities of IBM System z
- Discuss business resilience and agility features
- Set forth a sample template to calculate the financial risk of a security breach

Customers interviewed for this paper include Nexxar Group, Inc. and the University of Toronto. Nexxar, a financial services company in Europe, is an “early stage consolidator,” meaning its business model involves acquiring and integrating smaller firms. Nexxar has consolidated more than eighty x86 servers onto an IBM System z9 BC mainframe and, as a result, expects to save 30% per year in related operating costs. The University of Toronto, numbering six Nobel Prize winners among its graduates, is a significant research university with 75 PhD programs and 17 professional faculties. The University upgraded to the System z9 BC from its previous IBM System z/800 to address rapid growth while improving both the quality and security of core student applications such as course registration, grade retrieval and student elections.

This white paper concludes that many IT decision makers who are not traditional mainframe users can now take advantage of the high security inherent in mainframe environments while significantly reducing their total cost of ownership (TCO). The customer experiences detailed in this paper show the IBM System z9 with z/VM virtualization to be a cost-effective choice when seeking security for critical data together with an efficient and fast path for growth.

2 Introduction

Today's business and social trends have resulted in widespread pressure to protect all manner of strategic and personal information. Sarbanes Oxley requirements in the United States have placed new demands to control, monitor and produce information uniformly and quickly. Consequently, IT decision makers responsible for small and mid-sized (SMB) environments that are not traditional mainframe operators are considering mainframes as a solution to rapidly growing, complex environments that represent compliance and security risks. Constructing a strategy has meant finding, mixing and matching distributed hardware and software that is often difficult to manage and even harder to cost justify. As a result of these factors, emerging, growing companies are increasingly looking to mainframe technology such as the IBM System z9 for efficient and effective answers to their twin needs of scalable growth and managed security.

For suppliers these demands have converged to drive new innovations and designs onto proven mainframe technologies and to move formerly non-traditional approaches such as virtualization into the mainstream. IBM's System z9 technology employing virtualization with the z/VM (virtual machine) operating system is a leading example of these innovations. Together they solve the SMB dilemma by delivering:

- Integrated security features designed into the System z9 platform
- Advanced controls inherent in z/VM virtualization enabling better management of batch interactive and z/Linux workloads
- Economical and near-instantaneous order of magnitude growth in the same small footprint, thereby avoiding the need for costly environmental upgrades or expanded space

As a result, mainframe technology is no longer an expensive option available only to large, well-funded enterprises. In fact, Robert Frances Group (RFG), Business Advisors to IT Executives asserts,

“The multipurpose role of mainframes, with its inherent superiority in partitioning and virtualization, provides the same options now being considered on non-mainframe platforms, but with stronger and more proven technology... IT executives ...should consider the mainframe as a ‘first tier’ option for hosting new applications and acting as a central hub for security...”

- *The Mainframe: It's Baaack! June 27, 2006*

Regarding security and unauthorized or accidental disclosures of information, the benefits of tightly integrated hardware and software design are clear when employing virtualization. For example, the System z9 has achieved EAL5 certification. The EAL5 ranking gives companies confidence that they can run many applications containing confidential data – such as payroll, human resources, e-commerce, ERP and CRM systems – on one System z platform divided into partitions and virtual machines that keep each application's data secure and distinct from the others. The System z9 architecture is designed to prevent the flow of information between logical partitions on a system, thus helping to ensure that confidential or sensitive data remains within the boundaries of a single partition.

2.1 System z9 Overview

On April 27, 2006 IBM introduced the IBM System z9 Business Class (BC) and Enterprise Class (EC) extensions to the System z9 family. The z9 BC is designed to be cost effective for mid-sized enterprises with a low-cost point of entry and easy upgradeability. It comes in two models with 73 capacity settings: the Model R07 aimed at smaller enterprises and the Model S07 aimed at mid-sized organizations requiring more I/O or overall capacity. The Model S07 is upgradeable to the System z9 EC. The z9 EC, targeting mid-sized and larger enterprises, brings new benefits with added capacity settings permitting decision makers to pay only for the precise capacity needed without steep price escalations at certain growth increments. It is available in five hardware configuration models; 2094-S08, S18, S28, S38 and the S54.

2.2 Virtualization and z/VM

Virtualization is the simulation of processor and I/O resources for multiple instances on a single physical machine to maximize utilization of physical computing resources. It provides a logical rather than a physical view of data, computing power and storage capacity, thereby reducing or eliminating implementations restricted by location or packaging. Virtualization enables a shared infrastructure with better access to information through increased asset utilization that not only speeds ROI, but also helps eliminate infrastructure sprawl and its associated security risks. The full value of virtualization lies in its ability to:

- Improve total cost of ownership (TCO) by decreasing management costs and increasing asset utilization
- Increase flexibility through the pooling of resources that can be centrally managed via an enterprise hub
- Enable access through shared infrastructure

z/VM is a robust computing platform spanning the family of IBM mainframe servers. It offers a base for customers to exploit IBM virtualization technology on the IBM System z9 family. One IBM System z9 server running z/VM Version 5 can do the job of many distributed servers by hosting a variety of operating systems (including, for example, Linux). IT Managers can easily create many virtual machines consisting of virtualized processor, communications, storage, networking and I/O resources. z/VM supports many uses including:

- Guest environments
- Web server images
- Consolidation of select UNIX and Linux workloads onto a single physical hardware server
- Data and application serving for Internet/intranet users
- Application development

2.3 Security Considerations

The System z9 platform comes with built-in security advantages. A list of IBM System z9 BC security features includes:

- CP Assist for Cryptographic Function – This feature enables encryption acceleration of common cryptographic functions directly in the System z9 server. This coprocessor enables:
 - Advanced Encryption Standard (AES) – Adopted by the US government, it became effective as a standard for highly secure information encryption in 2002. By 2006 it has become one of the most popular algorithms in use.
 - Pseudo Random Number Generator (PRNG) – Generation of difficult-to-predict number sequences is integral to effective deployment of cryptographic technology. The System z9 platform manages this important function natively.
 - Secure Hash Algorithm 1 and 256 (SHA-256) – SHA algorithms are designed by the National Security Agency and published as a US government standard for protection of sensitive data. They are therefore widely deployed in financial transactions and other secure applications. The System z9 platform provides both a SHA-1 and a SHA-256 implementation in hardware to accelerate these computations.
 - SSL Acceleration for Linux and z/OS – Improves efficiency by offloading some parts of processor intensive asymmetric encryption algorithms to a hardware accelerator

The customer can also enhance the security of their System z9 with the purchase a CryptoExpress2 co-processor:

- Configurable Crypto Express2 – This co-processor enables applications requiring encrypted keys or a SSL-specific PKI acceleration module. Secure Sockets Layer is a cryptographic protocol for securing Internet communications such as e-mail, secure web transactions, Internet fax and others.
 - Tamper-resistant cryptographic processor support – This feature provides assurance of cryptographic key data integrity even in a physically insecure environment. The chip is designed in such a manner as to insure that the data will be destroyed before it is physically compromised.

In addition to the specific security features listed above, System z9 includes the following advantages:

- Certified for LPAR Isolation – Logical Partitions permit the combining of development, test, quality assurance and production on the same system with a high degree of security thereby lowering cost, speeding deployment and contributing to overall convenience.
- EAL5 certification - The EAL5 (see description box below) ranking gives companies confidence that they can run many z/VM, z/OS and Linux based applications containing confidential data – such as payroll, human resources, e-commerce, ERP and CRM

systems – on one System z9 platform divided into partitions that keep each application’s data secure and distinct from the others. The z/VM and Linux components of the environment have been subject to similar certifications, resulting in EAL3+ (z/VM with RACF) and EAL4+ (limited Linux configuration).

- CryptoExpress2 is designed for FIPS 140-2 Level 4 - A US Federal Information Processing Standard for accrediting cryptographic modules. FIPS Level 4 is the highest level of security, providing tamper-evident packaging which erases any stored Critical Security Parameters in the event of a breach.

‘The z/VM operating system takes the principles of partitioning and enriches them through virtualization. The z/VM Control Program is able to virtualize hardware resources, either by sharing or partitioning real hardware resources, or by emulating their behavior. If z/VM is thought of as a virtual computer room full of virtual servers, then think of a virtual machine user ID as a “virtual cage” around the server. No one can enter the cage unless they possess the key: the virtual machine password. This is very different from the discrete environment, where access to a machine room automatically gives access to all servers in that room.’

-Alan Altmark and Cliff Laking, z/VM Security and Integrity, April 2005

The **Evaluation Assurance Level** of a computer product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard in effect since 1999. The increasing assurance levels reflect added assurance requirements that must be met to achieve Common Criteria certification. The intent of the higher levels is to provide higher confidence that the system’s principal security features are reliably implemented.

To achieve a particular EAL, the computer system must meet specific *assurance requirements*. Most of these requirements involve design documentation, design analysis, functional testing, or penetration testing. The higher EALs involve more detailed documentation, analysis, and testing than the lower ones. Achieving a higher EAL certification generally costs more money and takes more time than achieving a lower one. The EAL number assigned to a certified system indicates that the system completed all requirements for that level

3 Management & Environment - Deployment Scenarios

To illustrate the security advantages of IBM System z9 with z/VM virtualization, interviews were conducted with IT executives responsible for varying applications and deployment scenarios. The following sections describe the key attributes of the installations they manage, identify the systems they replaced and reflect the resulting benefits identified by the executives in their own words. Their interview comments are in italics. Wim de Ridder is Managing Director and CIO of Nexxar Group, Inc. Eugene Siciunas is Director, Computing & Networking Services at the University of Toronto.

3.1 Nexxar Group, Inc.

- **Server Consolidation and Security Management Centralization**

– *“Security is always part of the discussion for the financial industry.” – Wim de Ridder*

With two acquisitions in late 2003 Nexxar Group, Inc. a financial services company, embarked upon a strategy to accelerate growth through continued acquisitions. Nexxar is currently present in over 105 countries. Critical to sustaining the momentum of this growth without losing core management control is the ability to integrate the information processing requirements of each acquisition into a consistent and smooth running IT infrastructure. Nexxar has consolidated more than eighty x86 servers onto an IBM System z9 BC with virtualization via z/VM. This has enabled Nexxar’s IT organization to quickly create a secure, custom tailored computing environment for each “private label” relationship that utilizes its money transfer, money order, bill payment and check cashing services.

Nexxar’s backend architecture is IBM WebSphere as the application server under z/Linux for delivery of its financial services products and DB2 for database management under z/OS for backend data storage. In addition to achieving a more security rich environment with better centralized control, Nexxar has been able to cut six data centers to one and reduce the headcount required to operate its former x86 environment by 75%. The expected annual cost savings is 30%. Before deciding to make the initial transition to its mainframe environment, Nexxar evaluates the IT capabilities of each acquisition as it comes on-line.

“The first step, of course, is to determine if any of the acquired computing environments are sustainable for where we want to go. The answer, unfortunately, has been no, not only from a scale, capacity and functionality perspective, but also security.” – Wim de Ridder

Nexxar found that its acquisitions operate different systems or flavors of systems frequently under different business models. Evaluations concluded that an integrated IT infrastructure had to be addressed that could support its products across many international environments. Nexxar took two approaches; one to determine if current infrastructures could be modified and re-used and, the other to evaluate new systems and vendors. Nexxar’s rapid growth and the diverse operating and regulatory environments in which it operates made it difficult to explain requirements to vendors in a straightforward year-by-year scenario. New acquisitions, products and applications together with the security demands of the locales in which they did business could not be precisely predicted.

“It is hard to get the attention of vendors when you start to explain your project by saying you are not set in the direction you are going. We noticed right at the first IBM stood out by giving us access to its different channels enabling us to compare its xSeries (PC Servers), pSeries (Power Servers) and System z9 (Mainframes) based upon our current environments and a set of variables for the future. This actually became our starting point. The comparisons were done in a two-step process. In the first step we looked at the kind of environment we would like to have. In the second step we did high level configuration pricing.” – Wim de Ridder

As a financial services company the protection of transactional data and its underlying information is paramount. Nexxar anticipated that its applications would make extensive use of SSL and other encryption rich products via the System z crypto facilities on the mainframe.

“Security is always part of the discussion for the financial industry. Because the encryption capabilities are embedded in the (System z9) mainframe we only (need to) convert one element...it makes a big difference having cryptographic processes on the mainframe versus our distributed environment. Otherwise (in the distributed server environment) we would have to install certificates individually.” – Wim de Ridder

This concept of not needing to address a multitude of distributed servers whenever an upgrade, audit or other change was required emerged as a pivotal TCO factor during Nexxar’s decision process. With more than eighty x86 servers distributed among six data centers and annual growth running at 20% to 30%, buying licenses for, and implementing certificates on each one was considered costly, complicated and unwieldy to execute. By contrast, only one IBM WebSphere license per physical processor is needed on a mainframe such as System z9 and (depending on workload) a single physical processor can support a number of system images and users analogous to multiple Intel systems. In addition, Public Key Infrastructure (PKI) certificates (an industry standard method of certifying the authenticity of parties to an electronic transaction by issuing and authenticating secure certificates to the systems involved), is implemented centrally on System z9 and then dispersed to the appropriate recipient systems. Another reason supporting Nexxar’s decision was its desire to centralize computing resources to maximize asset utilization. Virtualization under z/VM enables the simulation of large numbers of “virtual” machines on the single System z9 mainframe. This virtualization supports Nexxar’s need to quickly and securely implement private label services for its customers.

“It became clear that the System z9 was the preferable solution. We knew it [the hardware] was more expensive in the form of acquisition, but when you add in software and the required licenses in comparison to the number of processors, and that price was becoming very relevant, it was getting comparable to the solution we were looking for keeping the future in mind. Our goal is to share our infrastructures where we have a centralized form of control...that means virtualization where you don’t have to move memory, CPUs and physical servers. We found that virtualization on z/VM has been out there for many years with a proven track record. It allows us to set up a virtual environment with very secure production. It serves our need to rapidly provision private label functions such as purchasing transactions for other companies with dedicated segmentation of data, which is very easy to do in a virtual environment. For us, the data integrity and separation (security) guarantees we can give to our customers is a benefit of System z9.” – Wim de Ridder

The tipping point in Nexxar’s evaluation process was centralized control particularly in the context of security applications. Resource Access Control Facility (RACF) was cited by Nexxar as a major security benefit of System z9. RACF encompasses all three areas of security management: authorization (meaning and the enrollment of security objects into the system

identity space), access control (rules that control the availability of a particular resource to a particular identity) and, accounting (meaning the actual logging of or record keeping of every activity). Managing all of that information under a central control point gives Nexxar a better method of securing and auditing its environments. As new acquisitions are assimilated the dozens of password domains and databases they bring can be folded into its common System z9 infrastructure and managed under RACF. Thousands of user IDs that would otherwise take days or weeks to establish under Windows can be completed in minutes. This delivers dramatic cost optimization benefits in Nexxar's accelerated growth model. Describing this to regulators has proven to be an added benefit as well.

"In conversations with the regulatory people as soon as we go into explaining the differences between our former distributed environment and System z9, the ease of operation, how everything is centralized and controlled through RACF, the conversations are easier and everyone is aligned that it is a secure environment. In the distributed environment there are many elements to manage while with the mainframe we control everything through RACF." – Wim de Ridder

3.2 University of Toronto

- **Upgrading to the System z9 BC from a System z/800**

"You don't have the threat or the opportunity for hackers to play with it or figure ways to break it." – Eugene Siciunas

The University of Toronto selected the System z9 BC to upgrade from its former z/800 System supporting most student applications. The system runs student registration or, more broadly, course management. It retains student records and handles student interaction through which courses are selected or dropped, fees are paid and grades are posted and retrieved. Encountering spikes in demand at the start and end of each semester, the University wanted to improve service to students and faculty without changing its long standing applications and security techniques. Many of these applications had been developed by the University years earlier and have withstood the test of time under operating systems as historical as MVS (Multiple Virtual Storage) which IBM has improved and modified through several generations, culminating in the current "best in class" z/OS. Applications designed for these earlier operating systems are able to run seamlessly on the System z9 mated with the latest OS generations such as z/VM and z/OS. This, together with Capacity on Demand to address the demand spikes, was an important decision factor for the University's Director of Computing and Network Services.

"We (had been) a MVS shop for years...the application was (originally) designed for MVS (and we were not going to change it on a whim. We only made our previous (application) change because of Y2K pressures and prior to that it had been around for twenty or thirty years. So we don't take these changes lightly... the z/VM and IFL components of the z9 hardware made it possible to begin experimentation with some core security extensions to the faculty SecureID infrastructure by enabling a Linux environment where those technologies are more easily understood.... (also) the features of the System z9 made it very affordable in that we could secure the student's confidential data, improve the student experience and not have to sell half of the University's buildings to do it. That's why we are in the z9 family." – Eugene Siciunas

The upgrade to the System z9 was made at the end of the Spring semester. The resulting increase in processing power from approximately 110 MIPS (millions of instructions per second) to 216 MIPS was noticeable immediately. In addition, the University enjoyed the benefit of

compatibility engineering so that no changes needed to be made to its security practices which included requirements for dual access using RSA SecurID® on selected applications and web access parameters for the more common user interactions.

“Rolling the System z9 into the University’s existing framework was a snap. Just one weekend, unplug one and plug in the other. There was no problem at all. – Eugene Siciunas

IT experts have described operating system evolutions as an inherited security benefit. That is, as later OS generations are implemented to replace prior versions, the security tends to ascend automatically to a higher plateau. This higher starting point results not only from new and improved functionality to manage, measure, monitor, record and log, but also from evolving computer science that determines how a secure system is defined based upon more creative defenses. Today that often means coupling the system’s innate functionality with carefully designed external processes that, together, create a more sophisticated security environment.

It’s both the inherent security (in System z9 and its OS) and single use passwords (via RSA SecurID®)... so people who need to do serious things require two factors to get on the system. Certainly that’s why I sleep nights. – Eugene Siciunas

The University also favored System z9 technology for its indirect security. The feature depth and quantity of choices available to administrators makes it difficult for any but the most skilled outsider to intrude or otherwise disrupt system operation. Detail oriented choices permit administrators to activate levels of complexity that not only ensure that a user is authorized, but also can confound any unauthorized activity to oblivion. Individual command parameters can be controlled by the time of day, specific terminal, communications method, IP address and any combination all of these and more.

“It (runs) a fairly esoteric operating system. We use it for student elections and I had to appear before the governing council to make some statements about the security of the operating system. I said, ‘Well it’s not Windows... you don’t have the threat or the opportunity for hackers to play with it and figure out ways to break it. The skills to work with it are certainly not as common as the kinds of (skills possessed by) people hacking other systems.’ I’ve always favored it just because you don’t have hackers sitting with a system on their kitchen table where they can probe and poke and figure out how to break it.” – Eugene Siciunas

Finally, the University cites a heightened public attitude toward information security as a factor influencing its System z9 installation. Canada’s Freedom of Information and Protection of Privacy Act, while focused more on processes that determine what information can be sought, why, and controls over how it may be used nevertheless signals this attitude. Institutional and personal data can find its way onto servers and personal computers that are subject to theft and there have been plenty of published reports to this effect. The end result is potential harm to the individuals whose personal data has been compromised and negative publicity impacting the stature of the organization that lost the data. Encryption methods are one way to protect information before it is physically at risk.

“The z9 could play a role in (solving) this as we figure out some of the applications for the cryptographic engine. We have it now so let’s see what we can do with it. The risk is not just financial, it is also loss of reputation which is another reason why we are taking it seriously.” – Eugene Siciunas

3.3 Business Resilience and Agility

- **System z9 and z/VM Active and Passive Security Capabilities** - A “Defense in Depth” strategy.

Business **resilience** is the ability of an organization to **resist** external attacks. Business **agility** is the ability to **react** effectively to a threat. From an IT security perspective the distinguishing factors are:

1. How effective is the infrastructure in resisting attacks
2. How rapidly can the infrastructure detect and correct a breach

System z9 technology addresses these questions from a “defense in depth” strategy at three levels; hardware, operating system and application with the three constituting a coherent platform. A resilient platform allows customers to implement resistance tactics that are both passive and active. System z9 hardware supports passive resistance through built-in technologies, recognized by industry certifications like LPAR Isolation and EAL5 and FIPS Level 140-2 Level 4. These standards that are used across industries, have weathered the test of time and achieved their endorsements from government agencies and standards organizations precisely because they have proven their effectiveness in diverse applications worldwide.

Active resistance draws upon the system’s encryption strengths with cryptographic processors and asymmetric and symmetric acceleration capabilities. These are employed on applications to both resist and react to attack. RACF also aids both resistance and reaction by virtue of the speed with which access and authorization IDs can be added and changed.

While this white paper is focused upon z/VM as the operating system, it is important to digress somewhat with a review of a z/OS capability that should help to aid the understanding of agility. Integrated Cryptographic Support Facility (ICSF) is a z/OS program that manages crypto keys. With ICSF, if rapid reaction to a threat is needed, and it always is, the entire keying structure of a computing environment can be changed at once in one place. A single point program signals if it is threatened or actually under attack enabling administrators to use this same program to change the hardware, operating system and cryptographic application dynamically. z/OS also contains an auditing system so that when ICSF is active, security events are recognized and threat patterns are captured. Subsequently, with a database of threat signatures the system is able to take some limited defensive actions to new threats while signaling administrators for a more aggressive response using other features. This is another example of IBM’s defense in depth security strategy with post threat agility as the strength.

A significant number of the SMB installations using the System z9 BC with z/VM virtualization do not run z/OS as a primary OS, or, at best do so as a companion. Therefore, the ability to take advantage of ICSF is limited. In these instances the crypto engine can be relied upon for acceleration along with the previously mentioned RACF capabilities. Also, since z/OS is a logical upgrade path for customers growing from the z9 BC platforms, it is useful to know that integrated security is a fundamental aspect of such an upgrade.

Conversely (as security is both capability and process oriented), one area that needs additional thought is the definition and management of security policy. While IBM has devoted substantial expertise to management tools for z/OS, a similar effort could be made for z/VM and z/Linux. One approach may be to integrate or, in effect, “plug-in” the security components of ICSF

through IBM Director which appears to be IBM's interface of choice going forward. Because Director already works on z/VM, z/Linux and AIX it can then serve as a universal console with the effect of "pushing" ICSF into z9 environments using z/VM and z/Linux.

4 The Financial Risks of a Security Breach

- **Justifying a Move to the Security Advantages of Mainframe Technology Before It Can Happen**

The issues confronted by IT decision makers have expanded from merely considering the cost of establishing a secure environment to comparing that investment to the potential costs if they do not. The California Security Breach Notification Law passed in 2003, like other bell weather initiatives from that state, set the stage across the country for a rapidly proliferating set of laws and regulations intended to protect information as well as punish the enterprises that mis-handle it.

A widely quoted study by Ponemon Institute LLC looked at organizations that had lost confidential customer data and found that the post breach cost to the organization was \$140 per lost customer record. This cost was primarily driven by the customer notification requirements embedded in the new laws. However, other functions such as legal and CRM incurred incremental costs as well. An interesting point is these post breach costs are across disparate industry segments including financial services, healthcare, higher education and telecommunications. The Ponemon study found that lost or stolen devices such as PCs, desktops, and PDAs were the main factor in 49% of cases. This lends credence to Eugene Siciunas' observation that institutional and personal data can find its way onto personal computers and other devices that are subject to loss or theft. The central control benefits of mainframe platforms like the z9 and its encryption capabilities are critical protective measures that can be used to minimize this risk without hampering the customary practices of the enterprise.

In addition to notification expenditures and incremental cost impacts upon other functions like legal and CRM, costs were incurred for enterprise wide remedial actions including implementation of better manual procedures, training, and deployment of more secure platform upgrades.

Thus, with incidents of information losses appearing to occur more often and the publicity surrounding each one receiving greater attention, IT decision makers leading distributed environments are looking for ways to cost justify the implementation of more sophisticated security. NIST has even prepared Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, for use by federal agencies subject to the Federal Information Security Management Act of 2002. In the past some IT executives may have reluctantly resisted the adoption of more secure mainframe technologies due to perceived higher cost. Now innovations such as System z9 that have driven mainframe computing costs down, when compared to well publicized security breaches that have upped the ante for information protection, the business case for mainframes becomes considerably stronger.

Using some of the findings of the Ponemon study as inputs, a security breach cost model can be constructed with which to compare any expenditures needed to make certain such a breach has little chance of occurring. All dollar amounts and percentages are illustrative only. In practice IT decision makers can populate each cell with actual data from their respective computing environments:

Post Breach Corrective Measures @ 50,000 Customers		
Actions @ \$140 per Compromised Customer Record		\$
Damage Controls 65%	Notification 15%	1.05M
	Legal Counsel 10%	0.70M
	CRM Incremental 10%	0.70M
	Customer Retention 10%	0.70M
	Customer Losses 10%	0.70M
Process Improvements 15%	Security Audit	0.35M
	New Manual Procedures	0.35M
	Employee Training	0.35M
System Improvements 20%	Prevention/Detection Systems	0.35M
	Encryption Algorithms	0.70M
	Other Improvements	0.35M
Total		\$7.0M*

*Does not include an estimated cost for damage to the enterprise's public stature or reputation.

Once the above model has been modified and populated with enterprise specific inputs it is easy to do a cost comparison with an investment in IBM's System z9 with z/VM virtualization. The results, when realistically evaluated, will likely surprise and please decision makers who lead distributed environments. They will find that they can not only secure their organization from the cost and reputation risks of an information breach, but also significantly improve the overall computing power delivered to their users.

5 Conclusion

Past assertions that the mainframe has lost its place in the age of distributed environments have been supplanted by more recent analyst and user accolades. Their statements describe IBM's mainframe innovations that deliver security and control that is superior to discrete environments with better performance and the flexibility to grow economically on-demand.

The IBM System z9 arrives with an array of powerful security features "out of the box." These include Certification for LPAR Isolation to segregate and protect data, use of an encryption acceleration processor hardware for secure web transactions, and tamper-resistant cryptographic data and key management support. These features are part of a larger mainframe security solution that merges the active central control benefits of RACF with the passive protections of an access controlled mainframe environment. Taken in total and executed under virtualization, the security cornerstones of authorization, access control, accounting and auditing as well as data separation are better and more easily managed than in a distributed environment.

As demonstrated by Nexxar Group, Inc. and the University of Toronto, it is more cost effective to enable an integrated security management strategy on the IBM System z9 than on discrete systems. Nexxar's ability to cut six data centers to one, reduce the headcount required to operate the former distributed environment by 75% and dramatically lower license and certificate costs cannot be overlooked. These savings together with the flexibility of Capacity on Demand efficiently supporting 20% -30% per year growth contributes to a TCO that is strikingly attractive to small and medium sized (SMB) organizations. At the University of Toronto the ability to improve the student experience without changing longstanding applications and security techniques and to replace one system with another overnight represent significant advantages when change is necessary.

Finally, recent studies of lost or stolen information have isolated metrics that can be used to accurately compare the cost of a security breach to the investment in mainframe technology that is best able to prevent it. The balance of advantage between distributed environments and mainframe technologies for small and mid-sized enterprises is tipping to the mainframe.

Appendix A – References

The following additional resources provide more details about the security features and capabilities of the System z9 BC, z/VM virtualization, and the value to the SMB community.

The official IBM website <http://www.ibm.com>

About Virtualization <http://www-euro3.ibm.com/systems/virtualization/about>

z/VM Overview <http://www.vm.ibm.com/overview>

IBM System z9 Business Class <http://www-03.ibm.com/systems/z/z9bc>

What IT Analysts Are Saying About The New IBM System z9 BC
<http://www-03.ibm.com/systems/z/about/quotes>

The New IBM System z9 <http://www-03.ibm.com/systems/z/feature042706>

System z9 http://en.wikipedia.org/wiki/System_z9

Altmark, Alan and Cliff Laking, z/VM Security and Integrity, April 2005

z/VM Reference Guide <http://www.vm.ibm.com/library/zvmref08.pdf>

The Mainframe: It's Baaack! Robert Frances Group IT Agenda June 27, 2006

FIPS 140-2 http://en.wikipedia.org/wiki/FIPS_140-2

About University of Toronto <http://www.utoronto.ca/aboutuoft/quickfacts.htm>

Integrating IT Security into the Capital Planning and Investment Control Process, NIST Special Publication 800-65 Version 1.0 January 2005, Joan Hash, Nadya Bartol, Holly Rollins, Will Robinson, John Abeles, Steve Batdorff

Average data breach costs companies \$5 million, John Fontana, Network World, 11/02/06
<http://www.networkworld.com/news/2006/110206-data-breach-cost.html>

Data breach costs rise, drive security spending, Shamus McGillicuddy, News Writer, 15 Nov. 2006, SearchSMB.com

