Solitaire Interglobal

Cyber Crime: Keeping Data Safe from Security Incursions

May the Cyber Security Force Be with You

Introduction

> *"Information is a significant component of most organizations' competitive strategy either by the direct collection, management, and interpretation of business information or the retention of information for day-to-day business processing. Some of the more obvious results of IS failures include reputational damage, placing the organization at a competitive disadvantage, and contractual noncompliance. These impacts should not be underestimated."*
>
> Institute of Internal Auditors

All of cyberspace and its underlying infrastructure is vulnerable to a wide range of risk and exposure from both physical and cyber threats and perils. Sophisticated cyber individuals and groups exploit standalone and congregated vulnerabilities to steal money and information, or disrupt, endanger and damage operations.

The combination of wide opportunity for crime in cyberspace and the ability to execute from geographically-dispersed locations has produced a transformation of traditional criminal activities. Many of these crimes are now being committed via cyberspace. This includes banking and financial fraud, intellectual property violations, blackmail, extortion, and other crimes, all of which have extensive economic, human and sociological consequences.

Cyberspace is extremely difficult to secure. The sheer worldwide expanse for criminal location is the least of the challenges. The increasing integration between cyberspace and the physical world has exponentially expanded the opportunities for theft, damage and corruption. Emerging targets for crime are multiplying as the connection between the cyber world and the physical one develops new associations. Reducing vulnerabilities and minimizing consequences in complex cyber networks are the goals, but ones that are increasingly difficult to achieve.

Every organization leverages technology, even a service station that swipes credit cards. The need to incorporate secured data and processes is no longer a requirement for just large corporations, but has changed to an essential technology component for all sizes of organizations. This security in the virtualized, internet-connected, cloud-oriented world of today is a growing and complex challenge to *business*, not just information technology.

Solitaire Interglobal Ltd. (SIL) views security in a holistic way. This includes a broad-reaching perspective of security, focused on four main areas. They can be generally classified as:

- Data – access (read, copy) or manipulation[1]
- Process security – ability to execute, hinder, hijack
- Architectural – intellectual property, such as business model, structure of process, metadata
- Physical – access to the physical plant or facilities[2]

While physical security and access control is important, the large majority of SIL security analyses focus on the other three areas.

As a result of various analyses performed by SIL, research data was compiled that shows significant changes in threat types, scope and rate over the last several years, all of which are accelerating. Information from organizations concerned with the effectiveness of their security form the base study data, supplemented by detailed threat and security information from the Global Security Watch (GSW). This member service has tracked the detailed evolution of security threats and the associated effect on business on a worldwide basis for 20 years and currently collects reported information from more than 3.9 million organizations. The data from the GSW provides a deep source of threat Intel from a business perspective that provides input to the study and is built on a foundation of real-world production information. Although threat footprints and other detailed mechanisms are collected in the GSW, the main focus relates to the impact on business operation, organizational assets, and prevention and remediation costs.

One significant finding from the GSW data, and supplemented by more than 23K targeted security analyses run by SIL in the last two years, is that although some organizations are aware of security incursions, many are either not aware, or are only partially aware, of these events. Additionally, over 89.6% of the organizations within the scope of examination were unaware of the full ramifications of the cybercrime perpetuated on them. All requested audit and analysis of vulnerabilities by these organizations showed that the scope of vulnerabilities was either ignored or only partially acknowledged by the business portion of the organization. The most surprising discovery was that the large majority of those organizations were *not aware of the total number of actual incursions*[3] into their systems. To add to the challenge, many of these incursions were not a single occurrence, but instead opened the window of damage for a significant span of time. An example can be seen by looking at a published summary of the HIPAA violations thru December 2015.

---

[1] Data security includes some form of access to an organization's information. This may be to read or take a copy of specific content. Manipulation of an organization's data means that the information is modified or deleted to change the content or change the relationship of attributes and entities.

[2] Physical security is not covered in this paper.

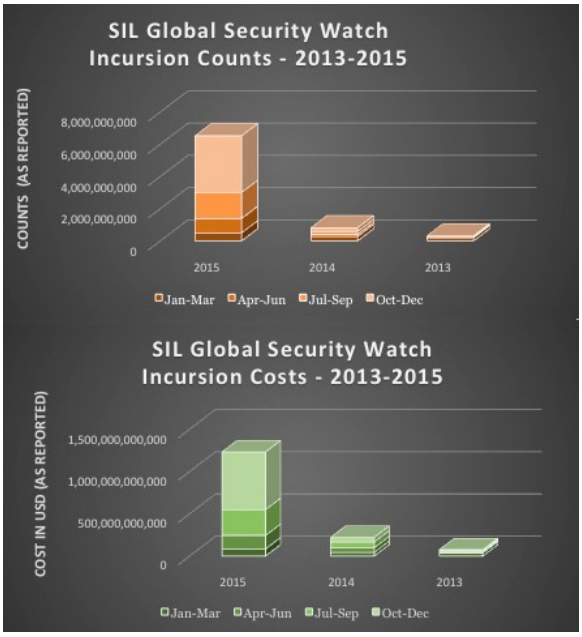
[3] Incursions are successful forays into the organizational IT landscape and include the initial intrusion or breach and each successive theft, destruction or blockage (i.e. data, research or process capture, denial of service, etc.).

"More than 10% Of 1,135 major HITECH breaches, as of Oct. 17, 2014, were ongoing and not attributed to one-time events, ranging from more than one day to 2,891 days. Looking into this further, it was found that:
-- 4 Breaches lasted more than 2,000 days
-- 7 breaches lasted between 1,000 And 1,500 days
-- 10 breaches lasted between 500 And 1,000 days
-- 35 breaches lasted between 100 And 500 days"

Source: Melamedia, LLC analysis of Office of Civil Rights Data, 2015

Extended periods of active incursion presence can have a substantial negative effect on organizational viability. Tracking general gross revenue effects for organizations with discovered active incursion fissures over the last two years shows that the average net valuation effect ranges from *-12.2% to -63.7%*, when the incursion fissure has existed for longer than three months.

Overall, the increase in outward facing applications exposes the organizational infrastructure to a larger and less-controlled user base. Additional stress on security is created by the increased use of virtualization software. Each of those virtual machines creates new points of vulnerability and adds to the complexity of the security challenge. As more organizations embrace and build out hybrid cloud solutions, the increased demand of responsive and resilient security practices must likewise grow and evolve.



The mandate of the changing security role is illustrated every day by the growing number of incursions and the associated damage costs. A look at the reported incursion details for the last three years shows an exponential rise in both of these dimensions.

It is not only the number of attacks that has changed. The evolution of the face of incursions has significantly changed in the last 20 years. Where two decades ago, security dealt mostly with access control, the topology of threat is far more complex today. One of the fastest growing threat vectors is the recombinant forms of virus and malware programs. In this type of attack, the incursion mechanism is packaged into two or more pieces. The fragmented nature of these components is not being caught by many security schemas. This is primarily due to the fact that by themselves the components are not executable and do not contain the easily-identified threat footprint that the fully-assembled version possesses.

While the recombinant incursion has been around for quite a length of time, the earlier versions of this threat vector had static components, where today's versions have variable and flexible assembly. This variability increases the difficulty in capturing and blocking this type of incursion. Additionally, correlation between the original

components and its damage is clouded by the multi-pattern behavior of the end result. This specific challenge has become a topic of discussion for security personnel everywhere, as more organizations deploy heavily virtualized platforms, move to cloud environments and increase the interconnectivity of their operations.

> *"We didn't even know that we had been hit! Somehow the attack not only came in three pieces, but managed to produce two very different footprints. One of them sat quietly and grabbed customer information, while the other destroyed order history. It has been a disaster to try to fix, since the damage persisted over six months."*
>
> CIO - Large Retailer

Security measurement is reflective, as it is evaluated by the absence of pain and problems. Security failure is highly visible, while its success is invisible. To build an understanding of the reflective metrics associated with security, IBM engaged SIL to conduct surveys, gather data and perform analysis to provide a clear understanding of the benefits and relative costs that can be seen when organizations implement IBM's z Systems platform as part of their IT architecture as compared to other platform architectures. This analysis has been primarily directed at the value of security from a business perspective, so that those whose role it is to provide business leadership can understand the benefit of the IBM z Systems security offerings when evaluating security solutions.

During this study, the main behavioral characteristics of software and hardware were examined closely, within a large number of actual customer sites (2,322,900+). All of these customers have deployed security as part of their production environments. This group has organizations that maintain both a single security standard and those that allow a heterogeneous mixture of security methods and mechanisms. They include organizations that are required to support regulated and industry standards for security of information, such as HIPAA, PCI, SOX, etc. The information from the customer reports and the accompanying mass of real-world details is invaluable, since it provides a realistic, rather than theoretical, understanding of how the use of different types of security can affect the customer.

The real world threat and attack activity from the GSW has been included in the analysis. Over 37 million data points of detailed incursion activity and impact provide a foundation of expectable costs and exposure, which is essential in understanding security and asset protection in today's marketplace.

In the collection and analysis of the study data, a number of characteristics were derived. These characteristics affect the overt capacity, efficiency and reliability of the secured environment. Also examined was the synergy of security and business operations. The behavior represented has been projected and modeled into possible options for deployment. In order to build this understanding more than sheer server performance is required, since ultimately security needs to protect, not hinder, the business process and operations. Although the capacity demand and throughput effects of the security systems are important, their translation into business terms is more germane to today's market. The business perspective encompasses a myriad of factors, including reliability, degrees of security, staffing levels, total security cost (including

recovery) and other effects. This ties directly into the decisions that IT managers, CTOs and business leadership have to make daily.

Perspectives and Views

There are two sets of perspectives or views that rose from the analysis itself. The first of these is the categories of relative activity and performance that a comparison of security behavior formed from the preponderance of reported experience. These four areas are:

- Operational efficiency
- Security effectiveness
- IT risk
- Resilience and agility

Each of these areas has contributed to another layer of perspective. Within this layer the importance and focus differs based on the part of the organization that is considering the challenges and ramifications of security. There are two main camps in this responsibility and awareness structure, business and technical. While the technical side is the typical view of the establishment and management of security, the increased scope of the challenge and the changing vectors of cybercrime have moved the primary responsibility for security to business.

Ultimately, IT and technology are designed to support business functions. One of the primary sources of the study data is the view of the security by an organization's business management, both executive and line-of-business. The patterns of operations from the study organizations are grouped and threaded throughout the four areas of comparison to identify their influence on business metrics. Each of these business metrics has measurable and significant differentiation when the IBM z Systems security solution is viewed and should be considered within the critical thinking of the organization.

The technical security aspects are also represented in the study. The fact that these are the more traditional responsibilities for IT does not lessen their importance in the evolving cyber security world.

Many of the categories have findings that address both the business and technical viewpoints. The complexity of viewpoint, authority, business need and responsibility are typical of the very complex challenge that faces organizations today. This study provides a data-driven articulation of some of those challenge components.

The granular metrics summarized in the study show how a specific success criterion is different in the general population of the implementers, broken down by platform type. These metrics are broad in coverage and touch on areas of financial consideration, as well as organizational quality. They are presented with short definitions and the focused net effect of each platform's deployment. In order to be meaningful across a variety of

industries, all of them have been normalized on a work-unit basis[4], and categorized by levels of organization size (small, medium, large and very large). The base measure has been set by the medium company average, so that all other metrics are based on a variance from that standard set point. The implementations included in this study have been restricted to those in production.

OPERATIONAL EFFICIENCY

Operational efficiency is the capability of an enterprise to deliver products or services to its customers in the most cost-effective manner while still ensuring high quality of its products or services. Operational efficiency can be viewed as the ratio between the input to run a business operation and the output gained from the business. When improving operational efficiency, the output to input ratio becomes more favorable. Inputs are typically based on money (cost), people (headcount or Full Time Equivalent - FTE) or time and effort.

When security is viewed from an operational efficiency perspective, the contributions are sourced from those specific areas. The difficulty in measuring operational efficiency in the security layer stems from the embedded form of security. The SIL analysis examined several distinct areas that lend themselves to extract of analysis. These are:

- Staffing load
- Targeted expenses through TCO aggregation
- Workload

Within these areas, both business and technical information needs are addressed. However, the metrics derived from the data form different patterns for business versus technical evaluation. The measurements allow the different groups to strategize and control aspects of security that align with the objectives appropriate to their organizational responsibility.

STAFFING

An underlying factor that shows itself in many other areas is the efficiency of the interface between the security administrator and the infrastructure. It includes software, hardware and operating system components, and the subsequent effect on staffing. As staffing efficiency increases, the level of productivity improves. The effort necessary to accomplish the same task in the security arena is lessened so that each member of the security staff is more productive.

[4] *Work-unit basis has been defined using the published International Function Point User Group standards and is based on function point (FP) analysis.*

The efficiency of any of the specific components that provide that influence on the user experience are difficult to break down into metrics other than in overly-detailed comparisons that lose their effectiveness by virtue of the degree of detail. A general view of the staff effort groups into FTE was reviewed to provide a general metric for the platform comparison. The overall average for security staff effort has been included in the graph as another comparison measurement. This average aggregates all reports, irrespective of size.

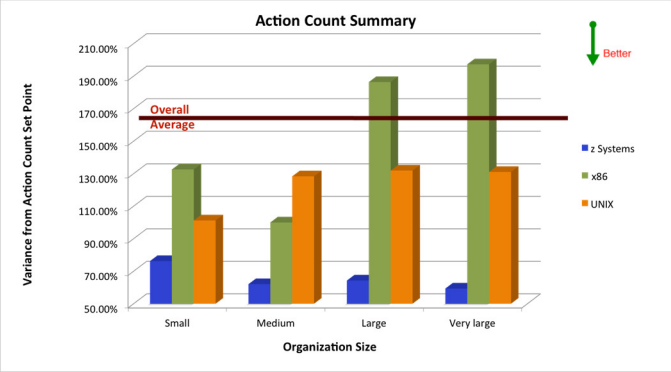
The comparative effort levels are those required to maintain a "gold standard" environment for each operating system group. The workload on the systems was normalized to identical levels to maintain the same level comparison field as defined in earlier comparisons. The set point for comparison is the median of the overall responding field, since so many options are available for security components.

> *"Our workload and application count on our mainframe have increased over the last two years by 300%. The same security staff that we had two years ago is still handling all of the work necessary with that expanded application base. This contrasts with our x86 workload that has increased its application count by approximately 200%, and an activity level of about 300%. We had to quadruple our security staff for that platform and double our budget for platforms and software. In that timeframe, we have had 112 security breaches that required active remediation on the x86 platforms, while the mainframe has had no security issues during the same period."*
>
> CSO - Very Large Financial Services

Since different security architectures have varying sets of implementation standards, it is important to keep the rigor of those standards in mind when reviewing the staffing. The noticeably lower security staffing level for the IBM z Systems deployment and use is directly attributable to the integrated nature of the z Systems operational stack. This is of special note as an organization increases in size or if an organization is on the path to a cloud service delivery model. The normalized staffing levels for IBM z Systems deployments are smaller than those for the alternate offerings by as much as *71.3%*.

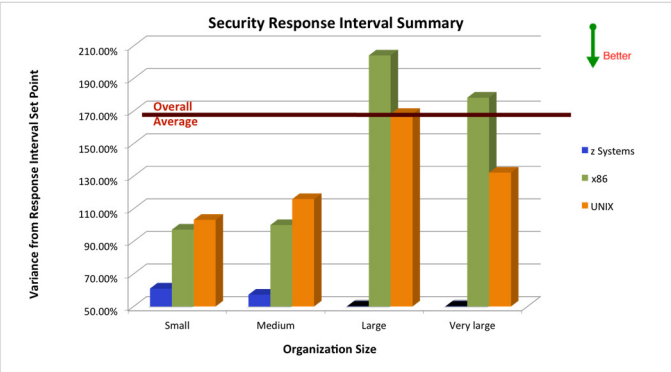
A key portion of this operational efficiency is the number of manual tasks and the length of time that it takes to perform those tasks. The tasks that are counted and timed are those that need to be implemented by security personnel in order to achieve the same level of due diligence, proactive activity and responsive modification. In an effort to thoroughly understand the platform differences, SIL was provided detailed video and action capture information by over 300 clients. This data was assembled into a time motion and activity framework, analyzed for causal chains and efficiencies, and used to build an effort comparison of the different platforms. The comparison data is normalized to provide a level playing field, as discussed elsewhere in this document. The

resulting activity comparison and timeframe comparison can be seen in the following charts.



Security action tasks vary significantly by the underlying platform and the organization size. In general, the larger the organization, the more complex and varied the security practice must be. The platform type adds another dimension of work profile onto this escalating effort. Comparing the base count of actions that need to be performed to maintain the security standards, the number of tasks that have to be manually performed by the z Systems security staff is substantially lower than that of the other platform groups. Time and motion studies show that z Systems security solutions require *69.91%* fewer tasks to implement standard protection levels. The incorporation of fewer tasks into staff responsibilities significantly raises staff productivity. It may also lower the FTE level that needs to be maintained in the security arena by requiring a significantly lower number of context switches, which in turn lowers risk.

> *"The security technical officers that are responsible for our Z platforms consistently have time to complete all of their tasks including their proactive ones. That is not true of those that support our UNIX and Wintel environments. It is not because of a difference in dedication or time. It is simply easier and more efficient to protect Z than it is to do the same protection on the other platforms."*
>
> Director of Security - Medium Manufacturer



There is a corresponding influence on time intervals necessary to carry out security objectives. The chart shows the impact on security modification response times. This metric shows the intrinsic security agility associated with the platform groups. The lower response timeframes documented here indicate faster response, which in the security world means minimizing incursion damage. The time intervals included in this summation are those that are part of normal design, maintenance, and proactive behavior. The activities and intervals that are part of incursion investigation are not included in this visualization.

Activity interval for normal, gold standard activities for security personnel show that there are substantial advantages in this aspect of staffing for z Systems deployments.

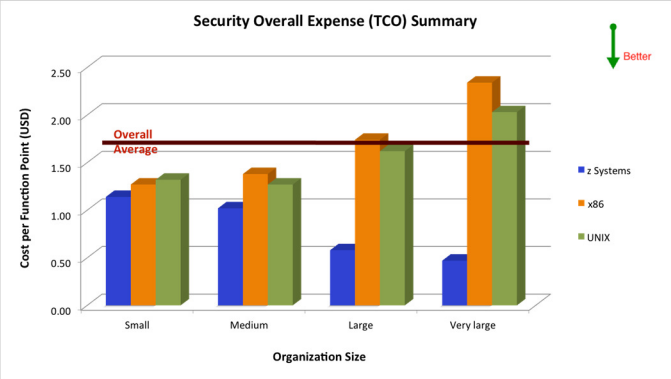
The same standard activities on z Systems consume up to *79.64%* less clock time than those executed on other platforms.

> *"You asked me what I thought about security on our mainframe. I can sum that up in a very few words - faster, efficient, effective. That is one spot in my responsibility that causes me the least heartburn."*
>
> CSO - Medium Retailer

TOTAL COST OF OWNERSHIP

Total cost of ownership (TCO) provides one of the main business side metrics for operational efficiency. This high-level metric aggregates all of the expenses within the organization that contribute to any aspect of the security deployment. In this portion of the study analysis, all expenditures that contributed to the protection of assets are summarized. This excludes physical security, but includes all other aspects. Once again, the projects and their expenditures have been normalized based on the standard basis. This enables large and small organizations, and their expenditures to be more accurately compared.

Isolating the TCO for the security practice is challenging in that security is increasingly embedded into all aspects of an organization's operations. By normalizing the TCO based on a standard work unit definition, like function points, an accurate comparison can be made and trending highlighted. The patterns of expenditures show increasing trends for some of the platform types as the complexity of the deployment grows. There is a contradictory trend for z Systems. A declining pattern of unit expenditure translates into efficiency of scale, where the leveraging of framework and foundation allows a cost-efficient pattern of financial investment. As seen in the accompanying chart, the expenditures for z Systems security implementations are significantly lower than for those of other platforms. This stems partially from the combination of architected security base and highly scalable platform. The efficiency of this synergy is demonstrated as the architecture is more heavily loaded, a significant drop in cost for work unit is realized. This footprint is present in all situations where architecture is designed for highly scalable environments, but is more normally seen only in hardware. In this case, the commonality of design for scalability is present both in the physical hardware and the operating system. The result for security TCO is that z Systems expenditures are lower by as much as *79.91%* from those for alternative platforms.



> *"The IBM mainframe platform shows a much lower cost level than are other platform types, both for total and per platform. The costs have been pretty flat for the last three years even though we have doubled the applications on the mainframe."*

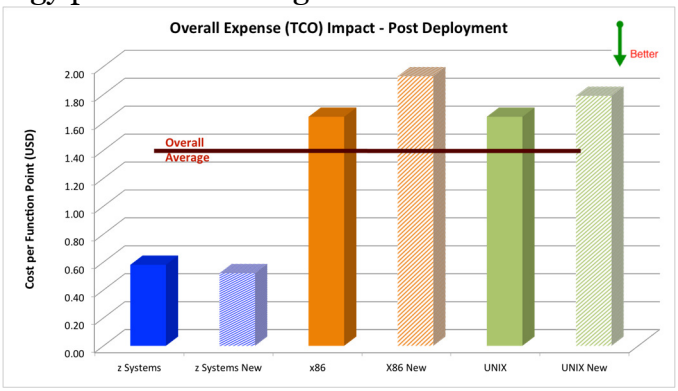
CFO - Very Large Insurance Provider

Architected scalability is especially important when systems become more complex, such as when users are scaled up, bring your own devices (BYOD) are proliferated, or extensive cloud applications and multiple access is deployed. The escalation in cloud adoption and increasing deployment of applications in the cloud have exacerbated the pain of maintaining responsive security. The form of cloud deployment also affects the challenges of security. Whether there is a private, public, community or hybrid cloud deployed, security practices are undergoing a constant evolution.

The advantages of balancing control and accessibility to the use of hybrid clouds has become better understood, and the adoption of this form of cloud deployment has resulted in the hybrid cloud becoming the most popular new implementation option. It presents one of the most complex scenarios for security, since multiple platform architectures all have to be secured.

In situations where security is handled with a series of additive protection components or where main security governance is solely resident in the deployed application, the overall expense comparison takes a significant jump when new services are added. The following chart shows this type of effect. The projects included in this portion of the analysis show the short-term impact of security acquisition. In all cases, these 2,463 organizations added a single cloud application to existing cloud deployments. The deployments targeted private, public and hybrid clouds. There were only a small number of community cloud applications included in this portion of the analysis. All deployments in this group were designed for more than 1K users.

The TCO based on function points shows the short-term expense difference that is present at the time of acquisition. The impact on overall work unit expense illustrates the influence on business that the technology presents. Adding additional workload on the z Systems deployments did not add any significant expense, enabling the security costs to be spread over even a higher number of function points and greater amounts of workload. Other platform groups required additional expense in terms of licenses, etc. The average impact before the single additional cloud deployment lowered the cost of a unit of work on z Systems implementations by an average of *10.34%,* while the alternate platform solutions were increased by as much as *17.68%*. The summary chart illustrates the average for each of the architectural groups. The underlying data for the individual projects is notable in that none of the z Systems implementations showed a rise in TCO per function point, although two of them showed



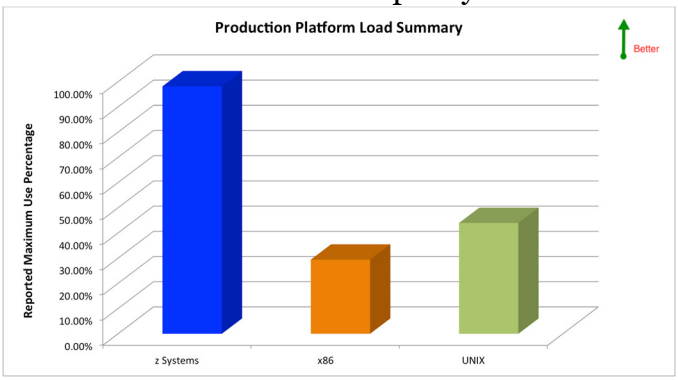
a null impact. The other architectures demonstrated individual results that ranged from an increase of *2.7% to 31.6%*. The pattern of impact is significant when considered within the framework of an expanding business targeting the cloud, expanding distributed user devices and facing substantial new services offerings.

Communicating the actual cost and impact of security is another challenge. The articulation of a business case for security improvements and expansion is a frequent topic of discussion, and an object of complaint by security professionals all over the world. The cost impact of security as an aspect of operational efficiency is not clearly understood by the majority of business executives. In a pool of data collected in 2015 that included over 3.6 million organizational executives, less than 14% had ever seen a business case for security expenditures. Less than 1.2% of these people claimed to understand how security costs, economies of scale and projected expenses were derived. Sadly, less than 5% of the people responsible for making organizational strategic decisions believed that their security personnel understood how to project or calculate costs. All of these contribute to a situation where the reduction, or increase, of overall security workload cost allocations are unexpected and unappreciated. With this particular blind spot, executive management fails to understand the sizable efficiency of z Systems security deployments.

WORKLOAD

The measurement of TCO is primarily a business metric. It incorporates key characteristics of the scalability of the architecture to expand, and better leverage the expense. However, the metric relates to scalability and resiliency in its raw form. Managing security resources efficiently rests on controlling personnel time as well as the embedded cost of the infrastructure and software needed to maintain the security practice. Scalable and resilient platform architecture forms the foundation for efficient expenditures of the time and money resources. A more scalable platform means that fewer implementation projects need to be performed and the ability of the IT resources to support the business is greatly increased. Therefore, a highly scalable platform that requires few activities to deploy additional workload increases the operational efficiency of the IT services group.

One dimension of the deployment scalability and resiliency is the level at which a foundation architecture can be loaded prior to undependable and erratic performance. The ability to use a higher percentage of the theoretical maximum capacity of a machine translates to lower expenditures and lower risk. The maximum production load reported from the study group was used to articulate the confidence of the professionals responsible for running smooth operations in the ability of the platform to maintain a workload. Workloads that spiked to a higher level, but had a duration of less than 10 minutes, have been omitted from this analysis.



"When you asked us how high our systems normally run, we not only sent you the data but actually looked at it. I didn't realize that our average load on our Wintel platforms was less than 14% while our mainframe consistently runs at 98%+. I guess I never realized how much more efficient that platform was. Somehow mentally I assumed all of the boxes could be pushed to the same level. This will definitely make us look more closely at which application we host where."

COO - Large Healthcare Organization

SECURITY EFFECTIVENESS

Security is reflective metric. Its success is only measured by the absence of problems, which is difficult to quantify. In order to examine the area of security effectiveness, SIL found measurable comparisons in a combination of objective and subjective metrics. The objective metrics included the ability of the security measures to capture and prevent successful incursion, both in the reported incursions and those discovered by detail audits. The information contained in this measurement has applicability to both the technical side and business side of an organization, since the quantity of incursions can be largely translated into the effect on the organization's bottom line.

A second objective measure is provided by an evaluation of the total cost of information[5] (TCI) of the IT services covered by the security deployment. This metric is part of the normal view of business executives and communicates both effectiveness and quality to those decision-makers.

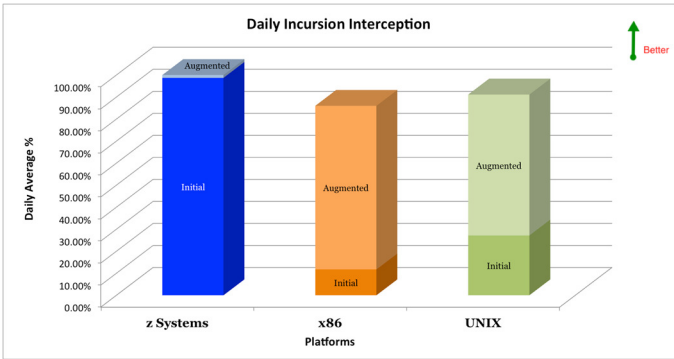
Each area provides some key differentiation for the IBM z Systems cyber security solution.

INCURSION RESISTANCE

The primary metric of security success is the number of incursions that are trapped and prevented from causing any form of damage. The incursions aggregated into this metric do not include those incursions that have been blocked by firewalls and security devices. Instead, only those blocked by the security solution present on the platform have been counted. These numbers have been normalized by the actual virtual machine count resident on a platform, since each VM represents a separable logical entity. This is an indicative metric, since no adjustment has been made for the number of users within each VM.

The level of incursion blocking provided by the initial installation for each of the platforms forms the foundation for any add-on security required or installed. This graph shows the security provided by the initial installation and the supplemental layer, expressed as a percentage of incursions that have been blocked. Based on initial

[5] *Total Cost of Information metric includes organizational expenses for the sustenance and protection of organizational IT and intellectual property assets.*



installations, the foundation z Systems security solution provides as much as *8.41 times* the interception level of alternative platform solutions.

Supplemental security layers are add-on applications, tactics and techniques, etc. These differ from organization to organization, but are variable based on individual security oversight, posture and governance. Higher levels of supplemental security requirements indicate increased levels of effort on the part of security software and personnel.

The combination of intellectual capital and automated services, coupled with the architectural design of the z Systems cyber security solutions results in the interception of a significantly higher percentage of incursions. The z Systems platforms deliver base incursion interception that is as much as *12.69%* better than the combined security of foundation augmented with extensive, competent and rigorous efforts for supplemental security tactics, techniques and procedures provided by the alternate platform solutions.

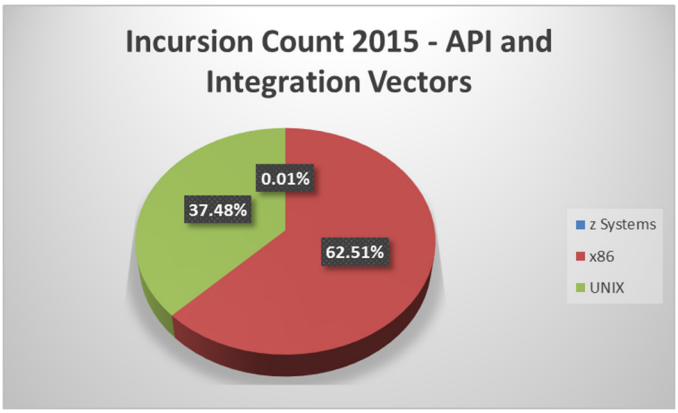
> *Note: SIL collects data on real-world, production deployments. This provides an actual, rather than theoretical, viewpoint operational practices, behaviors and metrics that are untainted by vendor claims or artificial benchmarks.*

Further insight into the effectiveness of the security solution requires a deeper look. Security services start with the foundation of the architecture, including any hardware, software and middleware components. Layered on top of that are the organizational policies, procedures, posture and governance. While these can be measured against current best practices and considered as key differentiation, this study is focused on an examination of vendor solutions that combine platform hardware, software and middleware, including operating systems.

> *"I have no idea exactly why there are fewer security problems with the z platforms, I simply know that we don't have any. The security people are constantly telling me things about this and that, it really boils down to it just works. The last time we had a problem with security on that platform it turned out that somebody stole somebody else's password. The last time I had a problem on a different platform was about an hour ago. Asked me which when I would prefer!"*
>
> CIO - Large Distributor

The nature of the z Systems embedded security is significantly different than that which is created with an additive topology. With a broader group of interfaces to secure, the protection of the organization's data and process is most vulnerable defined at the device level. A more effective strategy pulls the policy control and definition to a more centralized point. The highly integrated and embedded z Systems security stack

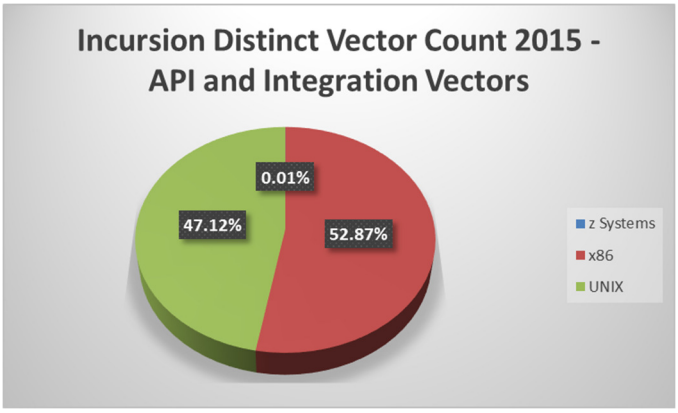
provides a significant advantage in this area. Measurement in this area can be articulated by an examination of the incursion patterns that exploit API and application integration. The chart shows the entire reported domain of this type of incursion, looking down by the platform of occurrence.



The variance in API and integration incursion vectors is not reflective of "protection by obscurity". All integration points and APIs that were aggregated into this portion of the analysis are publicly and extensively used. Instead, the variance is dependent on the baseline vulnerabilities and architectural protections for each of the platform groups.

While the sheer count of incursions that exploit weaknesses in integration and API access is informative, an examination of the count of the distinct vulnerabilities is also important.

The distribution of distinct vulnerabilities is somewhat different between the overall incursion count and the distinct vector count for the 2015 period. However, the low risk of this type of incursion vector for the z Systems deployments is significant.



The maturing cloud deployment landscape provides both opportunities and dangers to the implementing organization. The exact form of the cloud deployment also affects the challenges, whether that deployment be for public, private, community or hybrid cloud. With organizations avoiding both the expense of the private cloud and the exposure of a public cloud deployment, an increasing number of hybrid and community clouds are being implemented. The hybrid deployments carry a variety of vulnerabilities by the merger of various levels of security, while the community clouds have increased exposure due to the common usage by a wide variety of different organizations.

There have been a significant number of recent incursion reports where the transfer of information among the more secure platforms, such as the z Systems, and the less secure platforms have occurred. This type of incursion has been recorded for on-premise clouds, hybrid clouds and systems that are effectively supported by a managed service provider (MSP). The access information necessary to integrate the two platform applications was not protected on the more accessible platforms in this incursion form. This is the primary source of the small number of incursions identified for the z Systems platforms in the previous charts. These more vulnerable access points were used to

capture key access information to the more highly controlled platform and then used to perpetuate theft on the more secured platform. There is very little that can be done to secure any platform if the sanctity of the security is violated by its partners, but this increasingly exploited avenue has the potential for substantial damage.

An example of this type of contagious theft is where hackers attack law firms handling an organization's patents. When the patent application is stolen (often undetectably), the hackers then get the patent filed before the organization that has invested time and substantial money into the research and testing. This theft is only apparent after a time delay, and has exceeded $220 billion in loss in the last 18 months.

> *"Over the last three years we have had three major threats that have stolen some of our IP. All three have resulted in the loss of patent position and a significant investment in research. Unfortunately, we did not discover until long after the theft happened what had been stolen. It turns out that the theft occurred from our attorneys' machines, which were not as secured as the remainder of our platforms. With over $2 billion in projected loss, we are certainly trying to address this."*
>
> CSO - Large Life Science Organization

The role of the MSP in the IT world is evolving as the use of cloud becomes more prevalent. MSPs are ideally suited for implementing cloud for their customers, since their platforms are remote from the client organization by design. The structure of the hosted clouds is a cross between a private and public cloud, and can be viewed as a community cloud, where all applications and resources are managed by the MSP. This provides a unique view on cloud computing, and is one that carries with it an extremely compelling argument for customers when considering an MSP relationship.

The security for MSP operations can be very challenging. By nature, the mixture of application modules, user profiles, plug-in components and so on, provide many avenues for security breaches. Virtualization is also a factor, since it creates additional vulnerabilities. If the database and application security contributions are assumed to be the same across all the platforms, the underlying security in the platform architecture can be seen. This forms another layer of protection for customer process, data and intellectual property.

The average successful security incursions reported in the study organizations for their MSP cloud production environments were as much as *1300 times* higher for non-z Systems deployments. With safety cited by customers as the number one decision driver for selection of an organization's infrastructure, this is a notable comparison for selection of an MSP.

Public clouds are not being embraced as quickly as expected especially by larger enterprises, due to security concerns. As a partial bridge, many of the community clouds are being used by controlled membership organizations such as Visa or realtor groups. In these cases, shared data or application functionality is provided, but is well secured. There have been community clouds such as Visa, Master Card and American Express who have a limited audience covering multiple entities such as banks and card holders and continue to maintain a reliably secured environment.

At this point in the technology curve, many organizations have chosen to go with public clouds, partially because of a lack of knowledge about the costs and risks of private clouds. As the knowledge base increases, the consideration of the increased protection of the private cloud also grows, with more companies selecting private or hybrids clouds. Cloud security exposure is rising as the use of cloud increases. Despite this trend, no successful security incursions have been reported to the SIL GSW for clouds deployed on IBM z Systems platforms, other than those that stem from misuse of passwords.

Another challenge to the security of organization process and information is the growing trend to allow BYOD into the workplace as integrated infrastructure components. This issue is exacerbated by unsponsored devices making appearances in the workplace. Over the last twelve months, the use of these devices in the analysis group has increased by 1,403%. This trend will continue to rise, since the cost and expense advantages to the organization is considerable. With the introduction of a wide range of device types, securing organizational assets has become far more complex and volatile.

The use of private devices exacerbates the danger in security vulnerabilities, with the less secure deployments highly targeted by hackers. This is seen in the rise in x86 deployments that have experienced BYOD incursions over the last three months, with an increase of 6,043% over the same period last year. This can be contrasted with a similar metric for z Systems deployments of 0.012%.

The continuously growing capabilities of these devices, as they are used to retrieve and manipulate organizational information, creates another layer of complexity in security policy definition. The policies that define acceptable information access are more prone to drifting in this environment, where blind spots are created by distributed and siloed security controls.

Another complexity factor that is pertinent to an examination of comparative security effectiveness is the rise in mobile computing. With public network connections and hotspots increasing exponentially, a growing contribution to security risk stems from the policies, governance and effectiveness of these unknown access points. If the main effectiveness of the security solution is designed to be distributed, rather than centrally administered, the risk profile for the application and its data rise significantly. In this type of increasingly common application and accessed topology, the z Systems solution has architectural advantages. For those flexible deployments, SIL risk profiling sets the z Systems platform risk rating at less than 1/20 of any of the alternative solutions.

COSTS AND EXPENSE

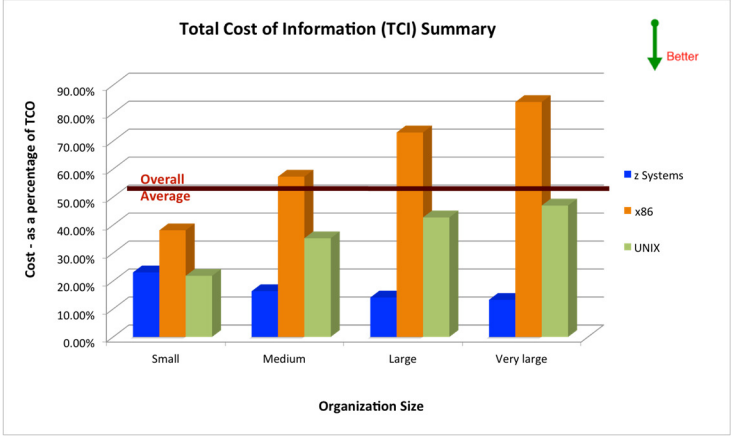
The costs associated with security touch on both traditional metrics, such as TCO and those that are coming into more common usage that relate to an expanded view of cost contributions within an organization, such as total cost of information (TCI).

TCO is comprised of the expenses necessary to run a continuing operation. The categories of cost in this metric include IT operational staff; break and fix application support; outside services to supplement operational staff or to problem solve; power

and cooling expenditures; hardware and software maintenance and licensing; and floor space.

TCI is a metric that takes a perspective that frames organizational expenses with respect to the sustenance and protection of organizational IT and intellectual property (IP) assets. These include data, business process, research, application structure and other intellectual properties. The expenses incorporated into this metric include the infrastructure that holds and deploys assets, staffing, power, cooling, security measures, etc. that keep the asset safe and running. This metric takes into account the negative impacts of IP loss and damage; and lost opportunity, e.g., denial of service and downtime. The metric that best reflects the impact and influence of IT security within an organization is TCI, since it builds an understanding of the reflective metric of security.

When looking at the TCI for different architectures, there are several ways of summarizing the relative issues. Since there is a wide variance in the size of infrastructure deployments, summarizing based on total IT and IP asset value is statistically vague. A normalized comparison base expresses TCI as a percentage of TCO. The results of this analysis can be seen in the chart.



The IBM z Systems implementations show as much as *84.21%* lower TCI over a wide range of organization size. Since this metric is a key driver to new implementation costs, the lower factor reinforces the efficient scaling present with the z Systems deployments. TCI comparison incorporates the cost of availability, incursion effect and downtime metrics, so that no additional view has to be taken into account. The differential among the solutions is based largely on three contributions, in the areas of:

- Staffing costs
- Costs due to incursion effects
- Infrastructure architecture add-ons

The costs for both staffing and the infrastructure are auditable, while the cost for incursion effects is a combination of both objective and projected subjective amounts. In all cases, the costs are directly from customer reports and have not been altered, but instead have been simply aggregated and averaged across the study base.

The lower costs associated with the IBM z Systems security configurations compare favorably to the x86 and UNIX security options on both the traditional expense basis and on the reflective costs due to incursions. This is primarily the difference between a highly integrated out-of-the-box security stack versus bolt-on architectures, with their increased susceptibility and vulnerability.

IT RISK

IT risk can be defined as the potential that a given threat will successfully exploit vulnerabilities of a process or an asset or group of assets, causing harm to the organization. It is measured in terms of a combination of the probability of occurrence of such an event and its associated consequences. SIL builds risk profiles that are actuarial constructs used to provide a consolidated view of the overall risk of an organization. This incorporates individual risk contribution from applications, interfaces, management structures, social engineering aspects, etc. For the purposes of profiling risk in a security deployment, the main dimensions of the risk profile are:

- Experiential pool of incursion activity
- Incursion costs
- Exposure

The changing landscape in the IT world has mandated a change in perspective to clarify the options from a management perspective. Some of the incursion effects reported by the customers are:

- Loss of service
- Customer falloff due to lack of trust
- Non-strategic architecture changes
- Recovery of missing or damaged data
- Loss of exclusive intellectual capital

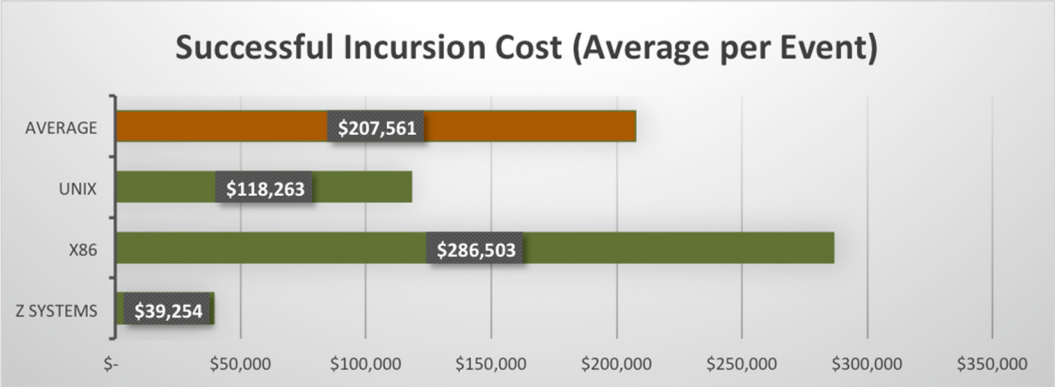
Those effects have aspects of probability and cost and relate directly to the organizational security practice.

> *"We have been plagued by denial of service attacks that have resulted in a significant loss of confidence with our customers. The attacks have forced us to move applications from our UNIX and Wintel boxes to the mainframe. Luckily, the same attacks have been unsuccessful in shutting us down since the move."*
>
> CMO - Medium Financial Firm

INCURSION COSTS

In some cases of security incursions, the costs to an organization may take a long time to assess. An example of this delayed impact realization is when proprietary research is stolen. The loss of the exclusive IP may have a significant market impact.

The average of all of the costs associated with an incursion, artificial as that may be, produces a metric for financial impact that is an indication of relative exposure for the different technologies. Unfortunately, a climate of "acceptable loss" has been building in the marketplace, due to the averaged costs of the multitude of smaller incursions. This has set a precedence for laxity in security definition and control that ignores the very real exposure to the larger, and more severe, incursion impacts. When an organization is conditioned to tolerate repeated "manageable" losses, it leaves its information and operations in a vulnerable state and ripe for major damage.



The average cost of an incursion is increasing and the rate of that increase is accelerating. Part of this stems from the broadening scope of cloud applications, where more people and data can be affected by incursions during each time period. The other factor to consider is that those responsible for the incursions are getting better and more aggressive in their attacks. This indicates an increasing level of threat that should be considered when selecting IT components.

The average cost of an incursion is affected by a multitude of characteristics. The speed and effectiveness of detection, the ability to isolate the incursion from causing further damage, the thoroughness of remediation, etc., all influence the general financial impact. The substantially lower cost per incursion for the z Systems platform demonstrates the synergy of all of these factors. Overall, remediation on z Systems security deployments average *86.30%* less than the alternative platforms. Stated from a slightly different perspective, organizations will spend an average of *7.3 times* more money in solving incursion damage if their deployment platform is not z Systems.

Incursion can be defined as a successful foray into the organizational landscape. This foray can take the form of theft, destruction or blockage. The current protections have to cover a wider variety of access points than are necessary for security at a whole platform level. In this situation, control over all aspects of processing needs to be in place. Many government and secure installations require protection for the allocation and handling of the main IT spheres: I/O, network access, memory management and overall normal execution access.

If the security perspective is split into the different classes of security, and a cost analysis is performed on what has to be added to the base platform to implement those security levels, an interesting picture is formed. The cost to achieve different levels of security is substantial – sometimes a significant percentage of the overall implementation. To understand these factors, the different security forms can be divided into levels of control:

- Normal corporate
- Credit card processing involved
- Banking
- Healthcare
- Research
- Defense

Based on critical functionality and control, weighted evenly, the different platforms provide the security coverage summarized in the following table. This configuration examines only the security features that are supplied with the originally deployed installation, since add-on options can be applied to any security setup.

Security Natively Covered by Platform

Security Level Description	IBM z Systems	x86	UNIX
Normal corporate	100.00%	18.16%	30.26%
Credit card processing involved	99.00%	11.04%	18.28%
Banking	94.00%	5.26%	10.22%
Healthcare	100.00%	3.24%	8.51%
Research	92.50%	2.86%	4.16%
Defense	85.54%	0.26%	1.86%

During separate study activities, SIL has conducted a series of vulnerability analyses for a random group of customers. Some of those customers were aware of security incursions of one sort or another, but all were concerned with a view into the effectiveness of their security. A total of 8,305 customers were analyzed in detail during the SIL vulnerability studies out of the total customers present in this main study. The most surprising finding from this targeted analysis is that the large majority of those customers were not aware of the actual incursions into their systems. In general, some of the organizations were aware of security breaches. However, the most startling finding was the sheer number of organizations that had experienced security breaches of which they were unaware. During this random set of vulnerability checks, 3,541 organizations had alien extraction processes that were still in active piracy mode, stealing information and affecting processes in real time.

The number of discovered incursions is significantly higher than the initially known level. Many of the incursion results may not be known for a considerable amount of time, especially when the effects of IP theft become evident.

The longevity of incursions has increased as attackers have grown more sophisticated. In the analysis of the unsuspected resident incursions mentioned previously, the longevity of the embedded criminal activity was studied. More than 14.52% of these parasitic incursions were determined to have existed longer than two years. Approximately 41.60% of them had existed between one and two years. Another 27.73% had been active on the systems for between three and 12 months. The remainder was split between short-lived incursions and those with an un-trackable start date, preceding detailed security tracking measures. The z Systems implementations were noticeable by their absence from this list.

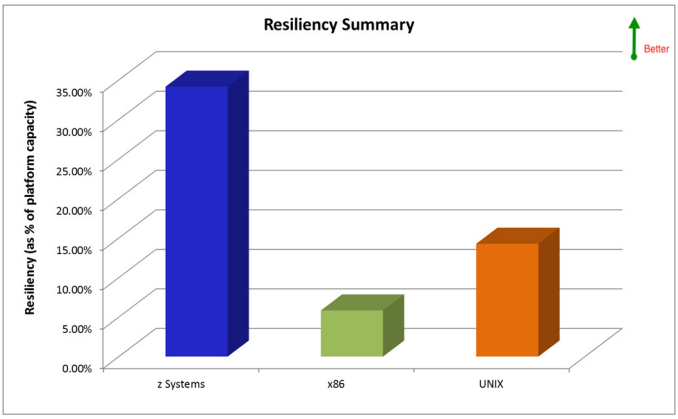
> *"OMG! We found out just last week that we have had a bunch of active programs stealing our data for more than six months. The ramifications for us is very large, since the information that has been stolen and exposed is primarily that of children. The only platforms that have been affected by this are our Wintel platforms. Everything is fine with our mainframe."*

CSO - Very Large Healthcare Organization

This type of extended vulnerability and covert criminal activity carries with it the highest exposure for an organization. Understanding the effect on the organization is difficult at the point of final discovery, since the extended exposure window leaves the organization open to significant loss of customer confidence, extensive legal action and protracted remediation.

RESILIENCE AND AGILITY

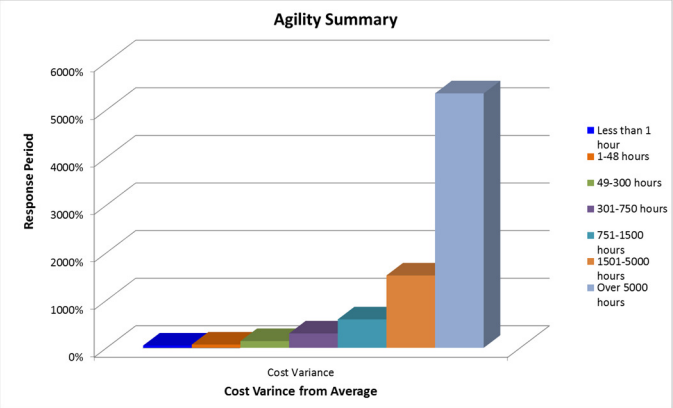
Major factors in a successful security practice are the resilience of the security deployment to handle unexpected levels and forms of incursions, as well as the speed in which responses to emerging attacks and threats are implemented. The resilience of the implementation can be viewed as the ability to handle unexpected resource demand without overall platform failure. Extreme cases can be seen in deployment crashes with concentrated denial of service attacks. The more resilient implementations rely on the capacity and elasticity of the operating system and hardware. Resilience is a typical metric when evaluating hardware for purchase and operating systems for deployment. The combined resilience rating of the platform groups is seen in the chart. The resilience rating itself is the result of recorded and reported breakpoints of scaling from the production implementations that are part of this study. The rating is expressed as a percentage of workload, and represents the amount of queue build and stress that the dispatching algorithms, buffering mechanism, and other components can tolerate without negatively impacting overall operations.



There is a substantial difference between the resilience of the z Systems deployments and the remainder of the solutions. The reported, average resilience of the IBM z Systems implementations is as much as *5.86 times* of the other options. This translates into less over engineering in the IT solution, which contributes to the lower TCO and TCI reported earlier in the paper.

The final metric area in this focus area relates to agility. Earlier metrics that touch on agility fed into communication effectiveness and other business perspectives. There is a remaining piece of agility that relates to the resilience and adaptability of the security practice itself. In this view, the agility is measured against expected exposure and incursion cost. This chart shows the effect on average incursion cost when balanced against the ability to quickly resolve incursion threats.

There is a demonstrated exponential increase in the financial impact of an incursion based on the length of time that the security deployment takes to respond to the attack. With a demonstrated speed of response reported for the z Systems, average incursion costs can be significantly controlled.



Next Wave Impact

The impending changes in evolution planned for release within the security arena will modify each of the platform groups within the next year. Short-term advances planned for UNIX and x86 environments are focusing on shoring up the individual additive products, primarily improving visualization and threat recognition. These products will individually improve their security coverage, but no general architectural changes are planned, partially due to the massive array of security product vendors. Based on the information for early release from 372 security product vendors, the relative positioning within the platform group will change, but the inter-platform relationship will remain substantially the same.

The advances with z Systems solutions address the main vulnerability of platform itself. In various places in this study, password misuse has been identified as the major recorded z Systems deployment vulnerability. The planned advances for IBM address this. These changes substantially remove the ability for most password misuse by a change in the underlying authentication structure. This change allows multifactor authentication, creating an extensibility to BYOD, including iOS devices, and covering the complexity of public network and hot spots.

When the impact of this change was modeled against the incursions of 2015, this architectural and procedural change would have reduced incursions by over 1.07 billion, with the financial impact of more than $9.6 billion. That impact would also reduce the sparse incursion count for z Systems deployments to less than 30 worldwide for 2015. With just this single advance security, 14.3% of the UNIX and 37.6% of the x86 deployments within the study could cost justify redeployment on the IBM z Systems platform. SIL will be watching the rollout of this architectural evolution carefully and will be incorporating it into the GSW reviews.

Conclusion

> *"Vulnerabilities in the internet are being exploited aggressively not just by criminals but also by states. And the extent of what is going on is astonishing – with industrial-scale processes involving many thousands of people lying behind both State sponsored cyber espionage and cyber crime. This is a threat to the integrity, confidentiality and availability of government information but also to business and to academic institutions. What is at stake is not just our government secrets but also the safety and security of our infrastructure, the intellectual property that underpins our future prosperity and the commercially sensitive information that is the life-blood of our companies and corporations. And the threat to businesses relates not only to major industrial companies but also to their foreign subsidiaries, and to suppliers of professional services who may not be so well protected."*

Sir Jonathan Evans, Director General of the Security Service, United Kingdom, June 2012
(Link: https://bit.ly/1517RBI)

As companies embrace and build out hybrid and private cloud models the critical nature of security increases. The security surrounding an organization's data and other intellectual capital is quickly becoming a major focus, as our world becomes more and more connected. With this increased integration comes larger challenges, as organizations struggle to protect their market advantage and finances. IBM z Systems has a long history of asset protection and highly secured deployments, and with that maturity comes features that are absent from other virtualizations, including that which controls the security of access and process.

The purpose of this analysis was to examine the real-world impact on business security based on platform architecture. For that purpose, major architectures such as IBM's z Systems platforms, UNIX and x86 products were compared. The metrics used to analyze the differences in platforms were both objective and subjective. A few of the highlighted findings can be seen in the quick summary below.

Quick Summary

Category	Commentary	Quick Byte
Speed of Response	The same standard activities on z Systems consume up to *79.64%* less clock time than those executed on other platforms.	Faster security response is delivered by z Systems.
Risk	SIL risk profiling sets the z Systems platform risk rating at less than *1/20* of any of the alternative solutions.	Security risk is significantly lower when deploying on z Systems platforms.
Security Effectiveness	Based on initial installations, the foundation z Systems security solution provides as much as *8.41 times* the interception level of alternative platform solutions.	IBM z Systems platforms provide the most secure application environments.

Category	Commentary	Quick Byte
Security Effectiveness	The z Systems platforms deliver base incursion interception that is as much as *12.69%* better than the alternate platform solutions with augmented security.	The base security delivered by z Systems platforms is more effective than the augmented solutions on alternate platforms.
Staff Effort	Time and motion studies show that z Systems security solutions require *69.91%* fewer tasks to implement standard protection levels.	IBM z Systems require less staff effort to secure.
Total Cost of Information	The IBM z Systems implementations show as much as *84.21%* lower TCI over a wide range of organization size.	Securing organization assets on z Systems is cheaper, irrespective of organization size.
Remediation	Remediation costs on z Systems security deployments average *86.30%* less than the alternative platforms.	Repairing security damage is less expensive on z Systems.

Whether an organization is running its own applications or utilizing a community cloud for secured financial or informational data or processing, the preponderance of data shows a clear delineation among architectures and relative levels of security. These reports from thousands of production customer deployments show that z Systems remains the most secure of all IT platforms.

SOLITAIRE INTERGLOBAL LTD.

Solitaire Interglobal Ltd. (SIL) is an expert services provider that specializes in applied predictive performance modeling. Established in 1978, SIL leverages extensive AI technology and proprietary chaos mathematics to analyze prophetic or forensic scenarios. SIL analysis provides over 4,900 customers worldwide with ongoing risk profiling, performance root cause analysis, environmental impact, capacity management, market trending, defect analysis, application Fourdham efficiency analysis, organizational dynamic leverage identification, as well as cost and expense dissection. SIL also provides RFP certification for vendor responses to government organizations around the world and many commercial firms.

A wide range of commercial and governmental hardware and software providers work with SIL to obtain certification for the performance capabilities and limitations of their offerings. SIL also works with these vendors to improve throughput and scalability for customer deployments and to provide risk profiles and other risk mitigation strategies. SIL has been involved deeply in the establishment of industrial standards and performance certification for the last several decades and has been conducting active information gathering for the Operational Characterization Master Study (OPMS) – chartered to develop better understanding of IT-centric organizational costs and behavioral characteristics. The OPMS has continued to build SIL's heuristic database, currently exceeding 250 PB of information. The increased statistical base has continued to improve SIL accuracy and analytical turnaround to unmatched levels in the industry. Overall, SIL runs over 2M models annually in support of both ongoing subscription customers and ad hoc inquiries.

METHODOLOGY NOTES

In order to understand the impact of IBM z Systems platforms as a key part of an organization's IT infrastructure and the effects on customer experience, a significant number of deployments were examined. The relative degree of difference in operating behavior for each factor, i.e., total number of outages, etc., was then compared to understand the net effect of the respective combinations. The effects were observed in general performance and capacity consumption, as well as other business metrics.

The approach taken by SIL uses a compilation and correlation of operational production behavior, using real systems and real business activities. For the purposes of this investigation, 7,241,948 environments were observed, recorded and analyzed to substantiate the findings. Customer experience was obtained to match against the deployment data. Over 4.5M customer feedback profiles on their experience were analyzed, matched against the IT environments and included in the study. Using a large mass of customer and industry experiential data, a more accurate understanding of real-world behavior can be achieved. The data from these systems was used to construct a meaningful perspective on current operational challenges and benefits. The reported behavior of the systems was analyzed to isolate characteristics of the architecture from both a raw performance and a net business effect perspective. Additional information on the methodology and study diversity can be found in additional methodology notes at the end of this document.

In a situation such as that presented by this study, SIL uses a methodology that incorporates the acquisition of operational data, including system activity information at a very detailed level. It should be noted that customers, running on their production platforms, provided all of the information. It is essential to understand that none of the data was captured from artificial benchmarks or constructed tests, since the value in this study comes from the understanding of the actual operational process within an organization, rather than the current perception of what is being done. Therefore, these sites have tuning that is representative of real-life situations, rather than an artificial benchmark configuration. Since the focus of this analysis was not to tightly define the differences among different minor variations of operating system or hardware, the various releases were combined to show overall architectural differences. This provides a more general view of architectural strategy.

In order to support the comprehensive nature of this analysis, information from diverse deployments, industries, geographies, and vendors were obtained. In any collection of this type, there is some overlap that occurs, such as when multiple vendors are present at an organization. In such cases, the total of the discrete percentages may exceed 100%. Those organizations with a multi-layered deployment, such as multiple geographical locations or industrial classifications, have been analyzed with discrete breakouts of their feedback for all metrics. Additional filtering was performed to eliminate those implementations that

substantially failed to meet best practices. Since the failure rates, poor performance and high costs that appear in a large number of those implementations have little to do with the actual hardware and software choices, these projects were removed from the analytical base of this study.

The industry representation covers manufacturing (20.06%), distribution (12.31%), healthcare (4.93%), retail (10.12%), financial (21.24%), public sector (10.83%), communications (13.38%) and a miscellaneous group (7.13%).

The geographies are also well represented with North America providing 49.36% of the reporting organizations, South and Central America 11.36%, Europe 24.42%, Pacific Rim and Asia 14.21%, Africa 0.54%, and those organizations that do not fit into those geographic divisions reporting 0.12% of the information.

Since strategies and benefits tend to vary by organization size, SIL further groups the organizations by the categories of small, medium, large and extra large. These categories combine the number of employees and the gross annual revenue of the organization. This staff count multiplied by gross revenue creates a metric for definition that is used throughout the analysis. In this definition, a small organization could be expected to have fewer than 100 employees and gross less than $20 million, or a value of 2,000, e.g., 100 (employees) X 20 (million dollars of gross revenue). An organization with 50 employees and gross revenue of $40 million would have the same size rating and would be grouped in the analysis with the first company. The classifications used by SIL use thresholds of 2,000 (small), 10,000 (medium), 100,000 (large) and 1,000,000 (extra large).

The information in this study has been gathered as part of the ongoing data collection and system support in which SIL has been involved since 1978. Customer personnel executed all tests at SIL customer sites. The results of the tests were posted to SIL via the normal, secured data collection points that have been used by those customers since their SIL support relationship was initiated. As information was received at the secure data point, the standard SIL AI processing prepared the data in a standard format, removing all detailed customer references. This scrubbed data was then input to the analysis and findings.

ATTRIBUTIONS AND DISCLAIMERS

This document was developed with IBM funding. Although the document may utilize publicly available material from various vendors, including IBM, it does not necessarily reflect the positions of such vendors on the issues addressed in this document.

ZSW03297-USEN-00