Pervasive Encryption

A New Paradigm for Protection

Introduction

> *I've been a professional hacker for more than 15 years. I find cybersecurity problems in technology in order to make that technology more secure. But after doing this for many years, I'm frustrated. I see the same problems over and over again. We are not getting better. And while we depend more and more on technology, technology is becoming more and more insecure."*
>
> Cesar Cerrudo, professional hacker, and CTO of IOActive Labs,

The changing face of computing is a ripple effect of the way that organizations and people are increasingly connecting via the internet.

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.

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.

The trend is accelerating, and the challenges are becoming overwhelming. The basic approach to security is proving to be inadequate to the demands of the aggressive nature of the environment. A paradigm shift is necessary and soon.

Solitaire Interglobal Ltd. (SIL) has been monitoring aspects of business and security for over 21 years. The collection of information via the Global Security Watch (GSW) provides thousands of organizations with trend and risk information on an ongoing basis. To effectively construct a global and comprehensive picture of the risks and opportunities that are offered, SIL views security in a holistic way. This includes a broad-reaching perspective of security, focused on four main areas. They can generally be 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]

To form the basis of this most recent study, SIL has performed analyses on research data from real world organizations supplemented by detailed threat and security information from the Global Security Watch (GSW). It's no surprise that significant changes in threat types, scope, and rate over the last several years continue to accelerate at unprecedented levels.

GWS is a member service has tracked the detailed evolution of security threats and the associated effect on business on a worldwide basis for 21 years and currently collects reported information from more than 8.9 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 the business operation, organizational assets, and prevention and remediation costs.

Summary of Findings

One significant finding from the GSW data, and supplemented by more than 62K 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 91.3% 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 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.

Increasing the danger, 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.

> *"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*

---

[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.).*

-- 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."

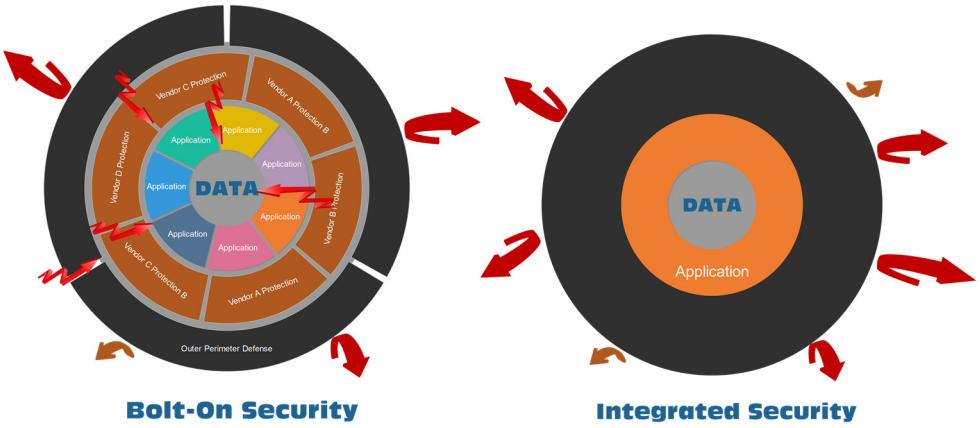
Source: Melamedia, LLC analysis of Office of Civil Rights Data, 2015

Extended periods of active incursion presence can have a substantial negative effect on organizational viability. Businesses stand to suffer between 16.2%-63.7% average reduction in gross revenues and valuation if an incursion lasts longer than three months.

With the acceleration of cloud deployment, the increase in outward facing applications exposes the organizational infrastructure to a larger and less-controlled user base. Changing market demands drive the organization to faster design and deployment cycles. Each of those new sets of users, each new application produces an increase in the possibility of a successful security incursion.

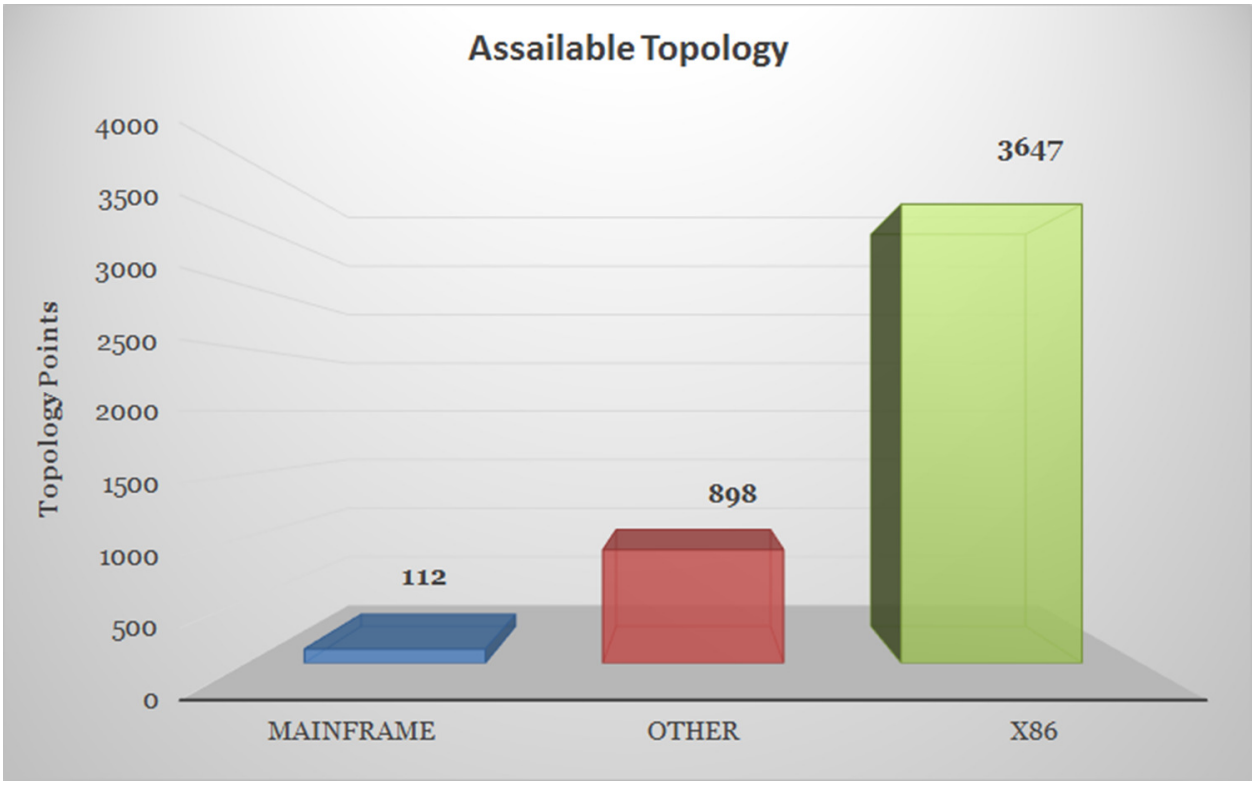
When tactical responsiveness includes the addition of layers of security and safeguarding, the resulting architecture starts to resemble an onion, something with layers on layers, intended to provide additional safety. However, in reality, the actual layers themselves can create additional points of assailable topology.

Each place that a partial solution is "bolted onto" is yet another target for a knowledgeable hacker. The more complex the layers, the higher the assailable topology. This vulnerability is part of a security risk profile that is increasingly used by insurance companies to determine the exposure of an organization to significant cyber damage.



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 for responsive and resilient security practices must likewise grow and evolve.

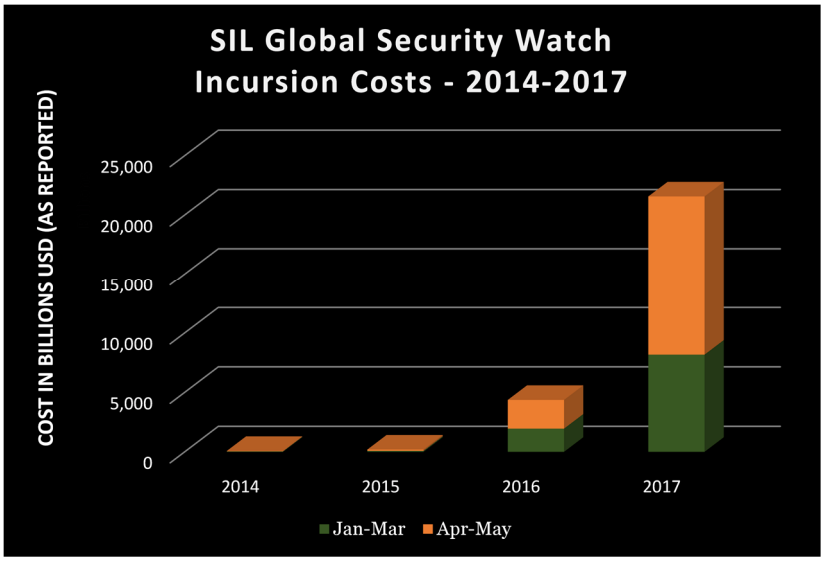
The assailable topology varies among the foundational architectures significantly. A general analysis of a group of over 115K organizations illustrated this difference, as seen here.

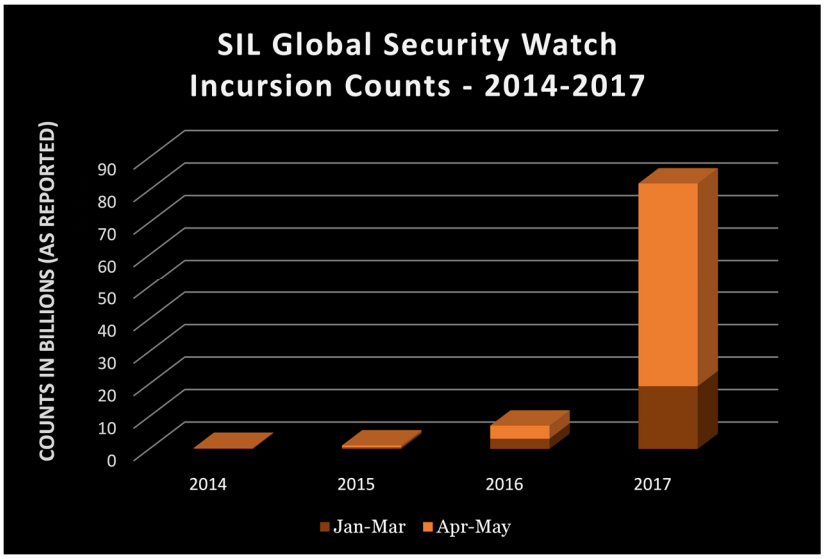


This significant difference stems from the base structure and realized strategy behind the platform architecture, chip design, operating system, and method of stack integration.

A look at the reported incursion details over the last four years shows an exponential rise in both number of incursions and the associated damage costs.

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





It is not only the number of attacks that has changed. The face of the incursions themselves 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 ransomware attack. In this type of attack, the incursion locks the files, directories, and other components of the system. The owner is asked to pay for an unlock code, which may or may not actually work.

> *"We have been hit by 5 major waves of security problems this year. Some of them have been malicious, while others are pure extortion. We ended up paying over $1M to get our main webservers back and we are still not sure how the hackers were able to get to them. It has cost us customers, tons of time and money. This is not a good feeling, not at all."*
>
> CFO – Medium-sized Manufacturer

Security Platform Comparison

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 the IBM Z mainframe 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 security offerings when evaluating security solutions.

During this study, the main behavioral characteristics of software and hardware were examined closely, across a large number of actual customer systems (9,602,000+). All of these customers have deployed security as part of their production environments but vary in a 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.

Over 81 million data points of detailed incursion activity and impact from the GSW provide a foundation of expectable costs and exposure, which is essential to 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. 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 perspective is related to the inherent categories of relative activity and performance which include:

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

Each of these areas opens the door to yet another layer of perspective. Within this layer, the importance and focus differ 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 is designed to support business functions. One of the primary sources of the study data is the view of security by an organization's business management, both executive and line-of-business. The patterns of operation 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 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 by platform type show how a specific success criterion is different in the general population of the implementers. 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. 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 or partners in the most cost-effective manner while still ensuring high-quality standards. Operational efficiency can be viewed as the ratio between the input to run a business operation and the output gained by 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 of security stems from its embedded form. The SIL analysis examined several distinct areas of importance including:

- 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

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

accomplish the same task in the security arena is lessened so that each member of the security staff is more productive.

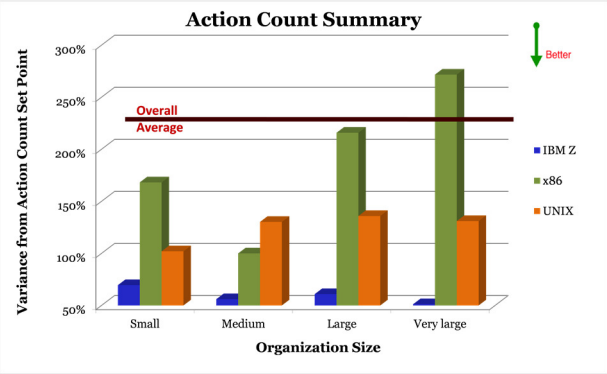
The efficiency of any of the specific components that provide that influence on the user experience is difficult to break down into metrics other than in overly-detailed comparisons that lose their effectiveness by virtue of the degree of detail. A general view of the staff effort groups into FTE was 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.

> *"We are running about four times the amount of work on the z (sic) platform compared to three years ago. We have lost two people in that time, but the remaining people are still handling all the work.*
>
> *If you contrast that with the increase in our other platform groups, we have to have almost ten times the number of people to handle one of the work for those.*
>
> CIO - 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 deployment and use is directly attributable to the integrated nature of the Z 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. IBM Z requires 88.35% less security staff time than other alternatives.

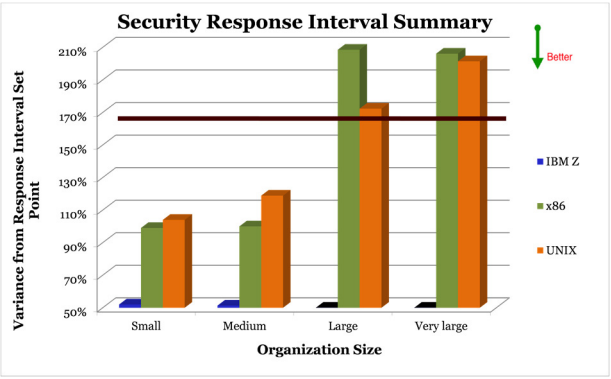
A key portion of this operational efficiency is the number of manual tasks and the length of time that it takes to perform those tasks. The tasks that are counted and timed are those that need to be implemented by security personnel in order to achieve the same level of due diligence, proactive activity, and responsive modification. To thoroughly understand the platform differences, SIL was provided detailed video and action capture information by over 620 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 IBM Z security staff is substantially lower than that of the other platform groups. Time and motion studies show that Z security solutions require *81.17%* 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 a faster response, which in the security world means minimizing incursion damage. The time intervals included in this summation are those that are part of the normal design, maintenance, and proactive behavior. The activities and intervals that are part of incursion investigation are not included in this visualization.

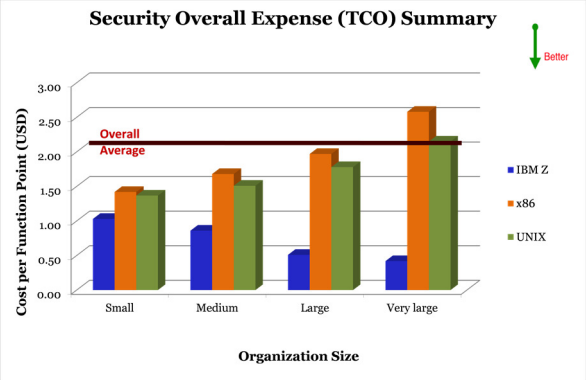
Activity interval for normal, gold standard activities for security personnel shows that there are substantial advantages in this aspect of staffing for Z deployments. The same standard activities on Z consume up to *81.66%* less clock time than those executed on other platforms.

"Our security on the mainframe is the least problem area of our organization. We frequently forget that we have a security group on the mainframe because it causes us the least problem."

CIO - Medium Financial Group

TOTAL COST OF OWNERSHIP

The 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 IBM Z. A declining pattern of unit expenditure translates into the 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 security implementations are lower by as much as 83.72% 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.

"Our IBM mainframe has a much lower cost than any of the other things we do as a company. The costs have actually gone down over the last three years, although our financial people keep telling us that the costs are too high. I keep telling them that the overall cost is lower since we have fewer problems, fewer staff, and less chance of problems."

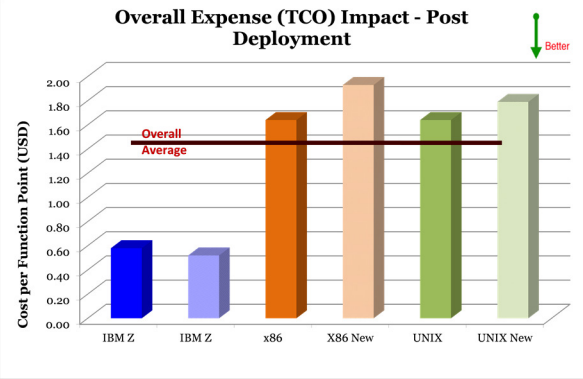
CFO - Very Large Distributer

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 must undergo constant evolution.

The advantages of balancing control and accessibility to the use of hybrid clouds have 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 16,027 organizations added a single cloud application to existing cloud deployments. The deployments targeted private, public and hybrid clouds and 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. The additional workload allowed the IBM Z deployment to spread a stable cost of security over a higher number of function points, without adding any significant expense. Other platform groups required additional expense regarding licenses, etc. The average impact before the single additional cloud deployment lowered the Z implementations by an average of *14.02%,* while the alternate platform solutions were increased by as much as *19.62%*. 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 IBM Z 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 *2.9% to 38.4%*. 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.

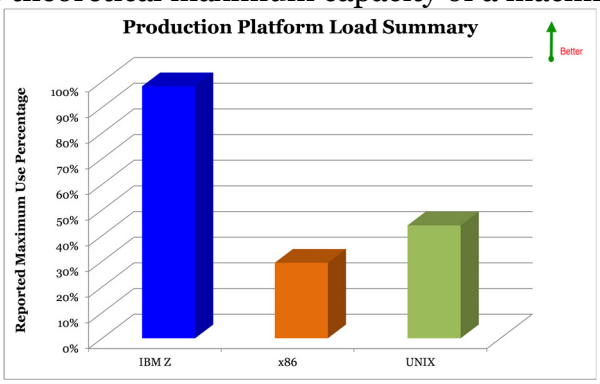
Communicating the actual cost and impact of security is another challenge. The articulation of a business case for security improvements and expansion is a frequent topic of discussion and an object of complaint by security professionals all over the world. The cost impact of security as an aspect of operational efficiency is not clearly understood by the majority of business executives. In a pool of data collected in 2015-6 that included over 9.5 million organizational executives, less than 11% had ever seen a business case for security expenditures. Less than 0.9% of these people claimed to understand how security costs, economies of scale and projected expenses were derived. Sadly, less than 35% of the people responsible for making strategic organizational 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 IBM Z 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 fewer 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

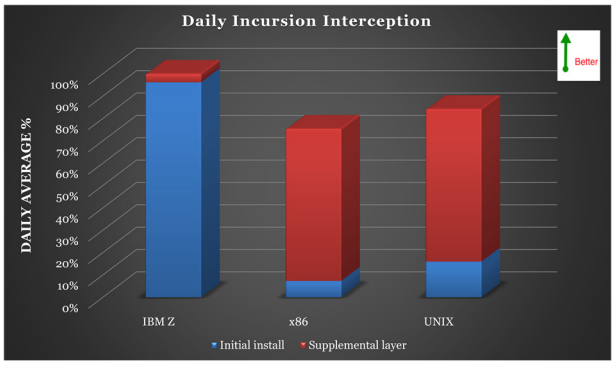
To examine the area of security effectiveness, SIL found measurable comparisons in a combination of objective and subjective metrics. The objective metrics included the ability of the security measures to capture and prevent successful incursion, both in the reported incursions and those discovered by 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.

Each of these areas provides some key differentiation for the IBM Z cyber security solution.

INCURSION RESISTANCE

The primary metric of security success is the number of incursions that are trapped, neutralized or prevented from causing any form of damage. The incursions aggregated into this metric do not include those incursions that have been blocked by add-on 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 installations, the foundation IBM Z security solutions provides as much as *13.21 times* the interception level of alternative platform solutions. Additionally, the Z solution provides a base, foundational protection that exceeds 92.1%, even without the bolt-on supplementation required for alternate architectures.

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 IBM Z cyber security solutions results in the interception of a significantly higher percentage of incursions. The Z platform delivers base incursion interception that is as much as *20.74%* better than the combined security of foundation augmented with extensive, competent and rigorous efforts for supplemental security tactics, techniques and procedures provided by other alternate platform solutions.

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 (sic) platform, 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 embedded Z security is significantly different than that which is created with additive protection solutions. With a broader group of interfaces to secure, the protection of the organization's data and process is most vulnerable when 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 security stack provides a significant advantage in this area.

Another complexity factor that is pertinent to an examination of comparative security effectiveness is the rise of 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 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 topology, the Z solution has architectural advantages. For those flexible deployments, SIL risk profiling sets the Z platform risk rating at less than 1/20 of any of the alternative solutions.

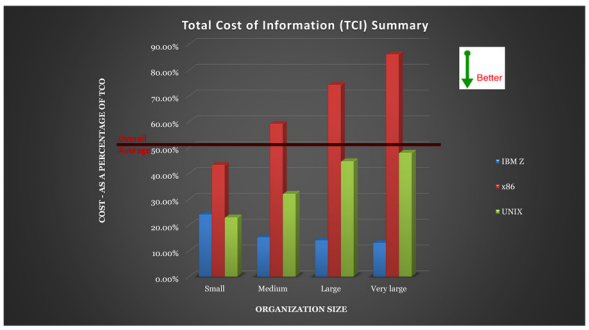
COSTS AND EXPENSE

The costs associated with security include both the traditional metric of TCO and the newer metric of total cost of information (TCI) that provides an expanded view of cost contributions within an organization

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 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 implementations show as much as *84.83%* 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 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 costs associated with the IBM Z security configurations are lower than the x86 and UNIX security options on both the traditional expense basis and on the reflective costs due to incursions. This represents the difference between a highly integrated security stack versus bolt-on with other architectures, creating increased susceptibility and vulnerability.

SECURITY RISK FACTORS

Security 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 or the clients it serves. 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 fall off 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.

> *"A variety of attacks have left us reeling from customer fade, remediation costs, and other horrific influences. The whole experience has resulted in a big loss of customer confidence. We are moving quickly to an MSP that runs some of the workload on a big mainframe, since that seems to the only safe place to run these days."*

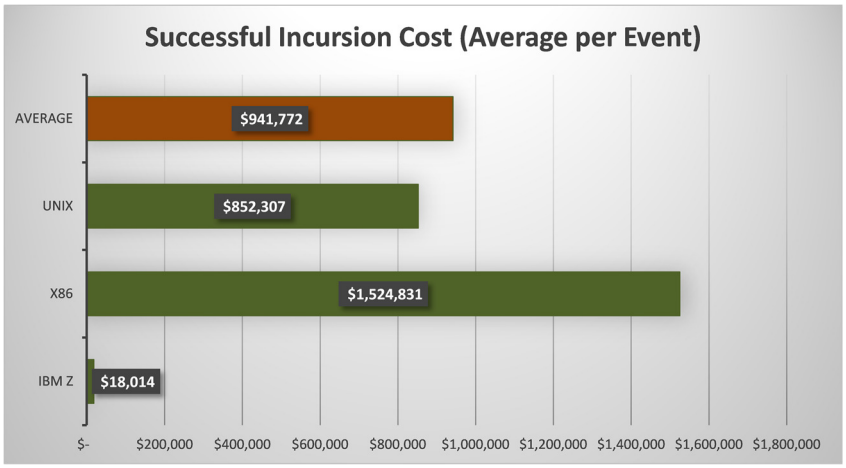
Director - Medium Distribution Company

INCURSION COSTS

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.

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 the costs associated with an incursion indicates relative exposure for the different technologies. Unfortunately, a climate of "acceptable loss" has been building in the marketplace, due to the averaged costs of across the multitude of smaller incursions. This has set a precedent 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 platform demonstrates the synergy of all of these factors. Overall, remediation on Z security deployments averages *98.82%* less than the alternative platforms. Stated from a slightly different perspective, organizations will spend an average of *84.65 times* more money in solving incursion damage if their deployment platform is not IBM Z.

The cost to achieve different levels of security is substantial. 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	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. A total of 14,625 customers were analyzed in detail during the SIL vulnerability studies out of the total customers present in this main study. 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, 8,2061 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.

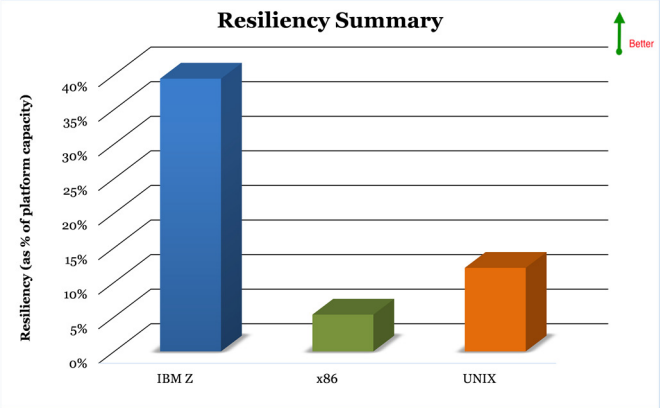
The longevity of incursions has increased as attackers have grown more sophisticated. In the analysis of the unsuspected resident incursions mentioned previously, the longevity of the embedded criminal activity was studied. More than 31.19% of these parasitic incursions were determined to have existed longer than two years. Approximately 43.28% of them had existed between one and two years. Another 23.16% 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 implementations were noticeable by their absence from this list.

> *"We acquired a company as part of our M&A efforts about 4 months ago. One of the main reasons we went through the merger was to leverage some of their IP. Well, we found out soon after starting the rationalization of the systems that they had a whole bunch of spy programs on their systems. Now our legal people are fighting over whether this can get us out of the arrangement, since the value of the IP is seriously endangered. What a mess!"*
>
> CIO - Very Large Biologic 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.

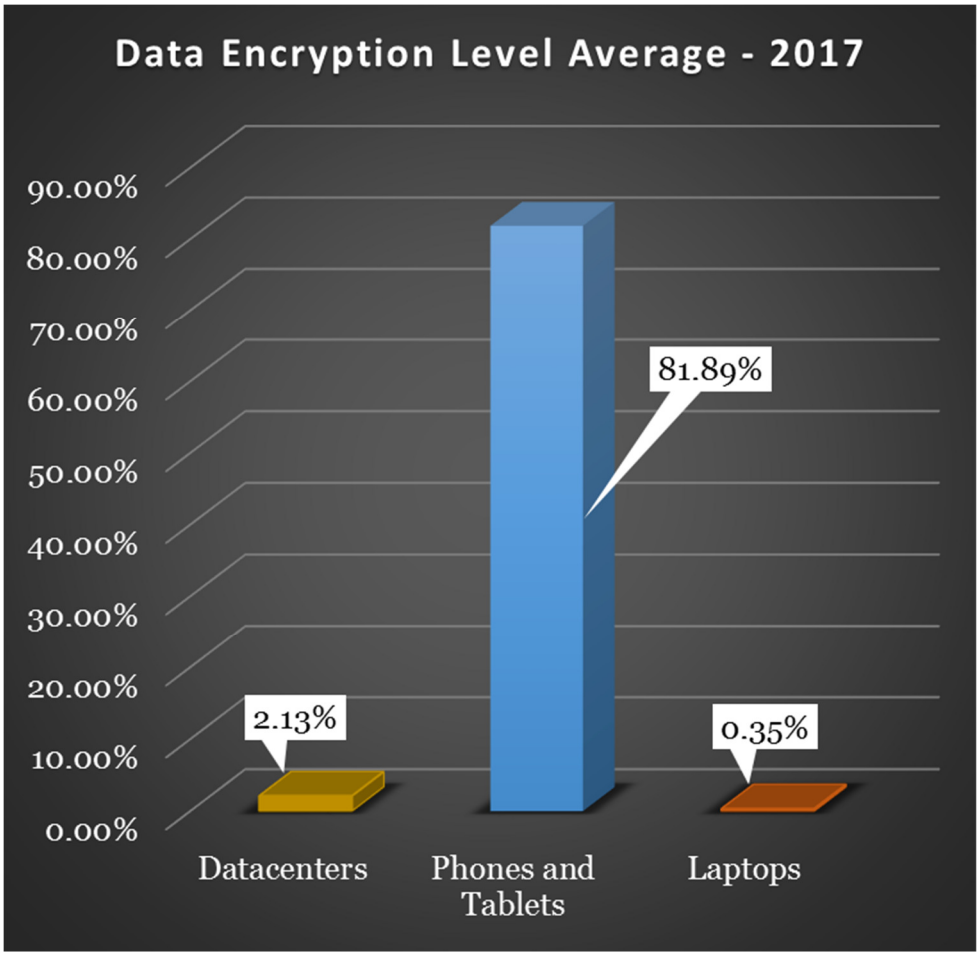


There is a substantial difference between the resilience of the Z deployments and the remainder of the solutions. The reported, average resilience of the IBM Z implementations is as much as *7.41 times* of the other options. This translates into less over engineering in the IT solution, which contributes to the lower TCO and TCI reported earlier in the paper.

PERVASIVE ENCRYPTION

An organization's client and corporate data is a key resource. It is literally priceless since it forms the core market advantage and intellectual capital of any business. Encryption has been one way of protecting this asset since once encrypted, its availability and vulnerability to hackers is eliminated. Many of those assets are currently unprotected.

The perspective is different in other areas of data communications. The use of mobile devices has been built on a view of privacy that included encryption from the initial design onward. A comparison of the different encryption levels is enlightening.



This summary highlights the base difference in the mainstream IT and mobile communications approach. Since the communication industry realized early on the importance of encryption when it came to mobile devices, approximately 82% of data on those platforms is encrypted, whereas only 2.13% of enterprise data within datacenters is encrypted. The discordance of the lack of encryption on the extremely valuable organizational resources located in datacenters and on laptops is severe.

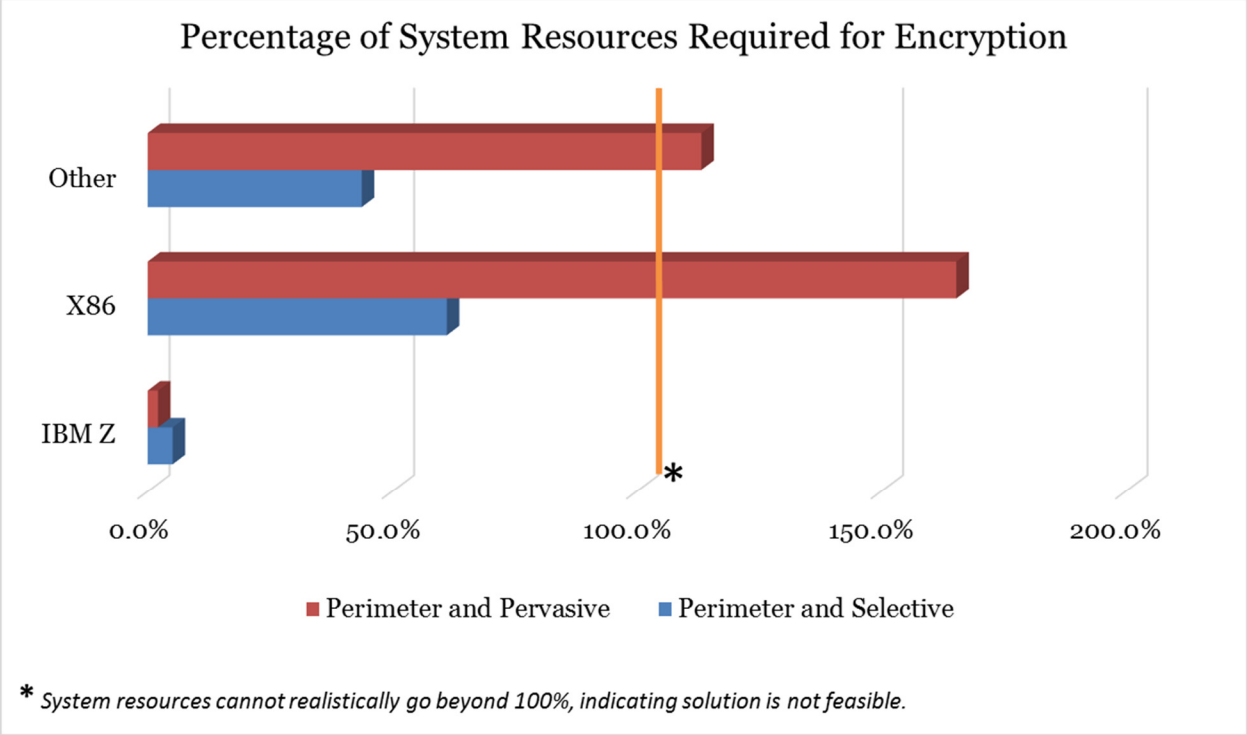
According to SIL GSW information, less than 3.5% of the 11.2B records breached in last 3 years were encrypted. Effectively, this means that as soon as a breach is made, the information is totally vulnerable to attackers. The loss of customer and partner trust is understandable since this lack of foresight is a serious breach of expected confidentiality.

There are several core reasons for the low levels of encryption. The cost in terms of time and system capacity has encouraged organizations to concentrate on perimeter defense techniques and selective encryption. With perimeter security defenses currently consuming up to 61.2% of overall platform capacity and increasing, a paradigm shift is needed.

A recent advance in one of the foundational aspects of our current computing environment is poised to make a significant difference in the market. The change is the expansion of the current IBM Z encryption from a selective model to one that is pervasive. Such a significant modification in the basic structure of computing and its effect on security will cause a major disruptive effect.

The overall concept is to not introduce a decision layer that says what will or will not be encrypted. Instead, it will be possible to have encryption be part of normal processing. The removal of the decision for selective encryption is a further savings in the overall cost and a reduction in the difficulty in using encryption in the current market.

The largest barrier to doing full-scale encryption has been the cost of the encryption and the performance load that such activity puts on the computing platform. However, for the reporting organizations in this study, the bolted-on solutions that are being deployed have caused system capacity to grow such that there are loads of up to 61% of the system load that is being consumed by security processes. That translates into a significant amount of infrastructure costs, performance drags, etc.



The current encryption resource requirements can be clearly seen in the chart above. The change to pervasive encryption highlights some of the fundamental differences in architecture. While Z leverages its ability to bulk encrypt for reduced cost, other architectures show the significant rise in overhead. To enable the non-Z architectures to handle pervasive encryption, a massive distributed topology would have to be implemented. Taking the average load for each platform within the study group, that deployment would result in the addition of up to ***12.2 times*** the number of current servers.

Such an increase in platform count would substantially raise the cost of operations. The impact on the organization adopting this solution would be considerable, with sharply rising hardware, software, and personnel expenses. This solution would address the shortfall in pervasive encryption but would still fail to mitigate the weaknesses of bolt-on architecture.

Even without the newest advances, the Z architecture delivers encryption with more effective and less costly resource expenditure. It delivers over ***8.5 times*** the security

protection, at ***93% less cost*** in overall expenditure, and with ***81% less effort***. This is, however, selective encryption which lessens some of the desperately needed protection.

The full impact of the faster encryption engine and the ability to encrypt information in bulk creates a fully pervasive solution that runs more than ***18.4 times faster*** and at only ***1/20 of the cost*** of other solutions.

Although pervasive encryption is feasible on the Z mainframe, it is not currently possible to implement on other architectures. The most restrictive of the architectures, tied to the x86 solutions, would require 7.32 *times* the current capacity to execute the workload necessary for pervasive encryption on a single server. The requirements for this type of solution will require significant advances in those alternate platform chip design, operating system foundation, and other internal platform capacity restrictions. Such advances are long term changes in chip design and manufacturing, with typical lead times of 2-3 years, assuming that the base technology can be created.

If that is not done, then the demands of pervasive encryption cannot be met on those platforms. The systems that are resident on those platforms will continue to run with higher risk and exposure profiles, demand an excessive amount of personnel time and expenditure and consume disproportionate amounts of organizational resources.

Applying encryption in a pervasive layer would significantly reduce the percentage of the platform that has to be devoted to the security processes themselves. For the analyzed organizations in a recent SIL study, organizations that deploy pervasive encryption on IBM Z can reduce overall processing overhead by as much as 91.7%.

The exposure to cybercrime is also so large that the shifting cost basis has to include the substantial possibility of hacking incursions damaging organizational assets.

Workload and speed of response are very important when it comes to security. The faster an organization can respond to a threat, the less likely that an incursion is to do damage. The response speed is a key metric to not only preventing adverse effects but also to minimize the impact. In the comparison of selective versus pervasive encryption within that same study, 87.2% of the incursions would have avoided the need for any response at all as the pervasive model automatically mitigates the need.

For those that required a response, the speed of the response was much faster on the pervasive side. The reduced complexity of the security architecture meant that fewer commands would need to be issued to address the same problem. In the tests, the speed of response required only 14.2% of the time required for the selective encryption response.

Assailable topology is also reduced. With fewer assailable layer points, threats can be addressed in a more comprehensive and less complex fashion. This lower complexity also could significantly reduce the risk of future hacks. The assailable topology measured for the test against a group of medium-sized clients went from an average of 2,423 assailable points down to 196. This represents an overall reduction in threat surface ***by nearly 92%.***

With a pervasive model, SIL explored the risk of incursions and exposure using a blended measurement and emulation mechanism to test out new technology. Providing the same number of protection aspects to data using selective versus pervasive encryption showed that the combination of fewer manual tasks and the increased speed

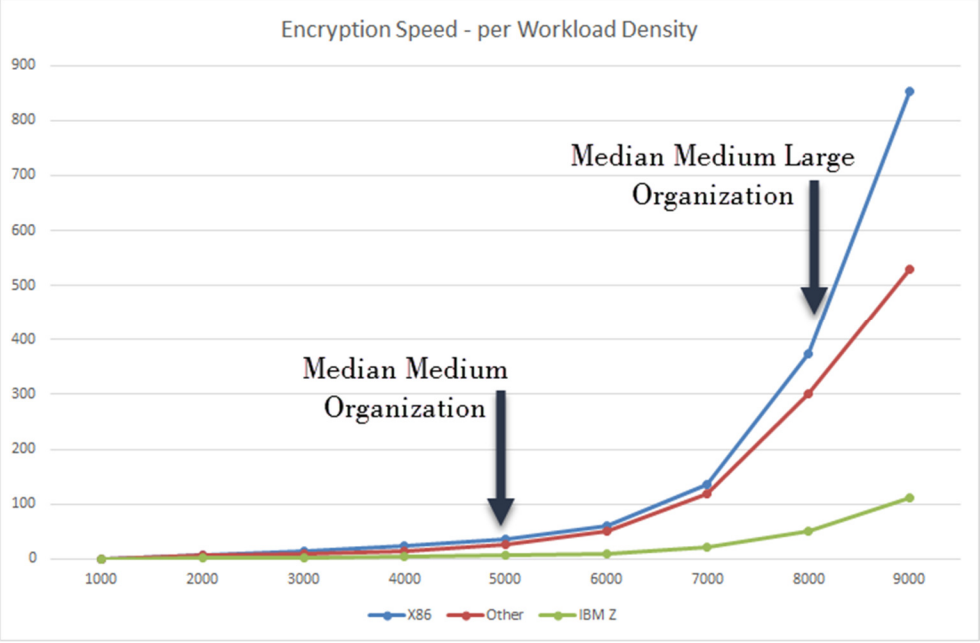
produced cost savings as much as 81.63% less than x86, depending on a variety of factors.

With the elimination of the platform proliferation facing many organizations today, the savings is not just in the platform costs. It extends to the personnel required to operate the equipment, perform the security tests, and manage all security resources. The reduction in personnel is even more substantial than that of the equipment. Where today the security personnel load for IBM Z requires approximately 80% less staff, the use of pervasive security will allow that staffing level to remain static while the alternate platforms will continue to grow each year substantially.

In that environment, a pervasive approach to encryption is cost justified. If the market pushes for such a shift in perspective, then the vendor efforts that have been devoted to bolt-on solutions could be better targeted toward the necessary architectural and fundamental changes necessary to enable pervasive encryption. Those changes will be more challenging for some architectures than others.

While the IBM mainframe architecture can deliver individual transactions 2.87-3.24 times faster than x86 speeds, the inclusion of the pervasive topology and approach increases that multiplier significantly. Since the underlying activity flow allows the pervasive model to deal with batches of transactions as a unit, rather than individual encryptions, the savings in capacity demand are substantial and is reflected in the speed.

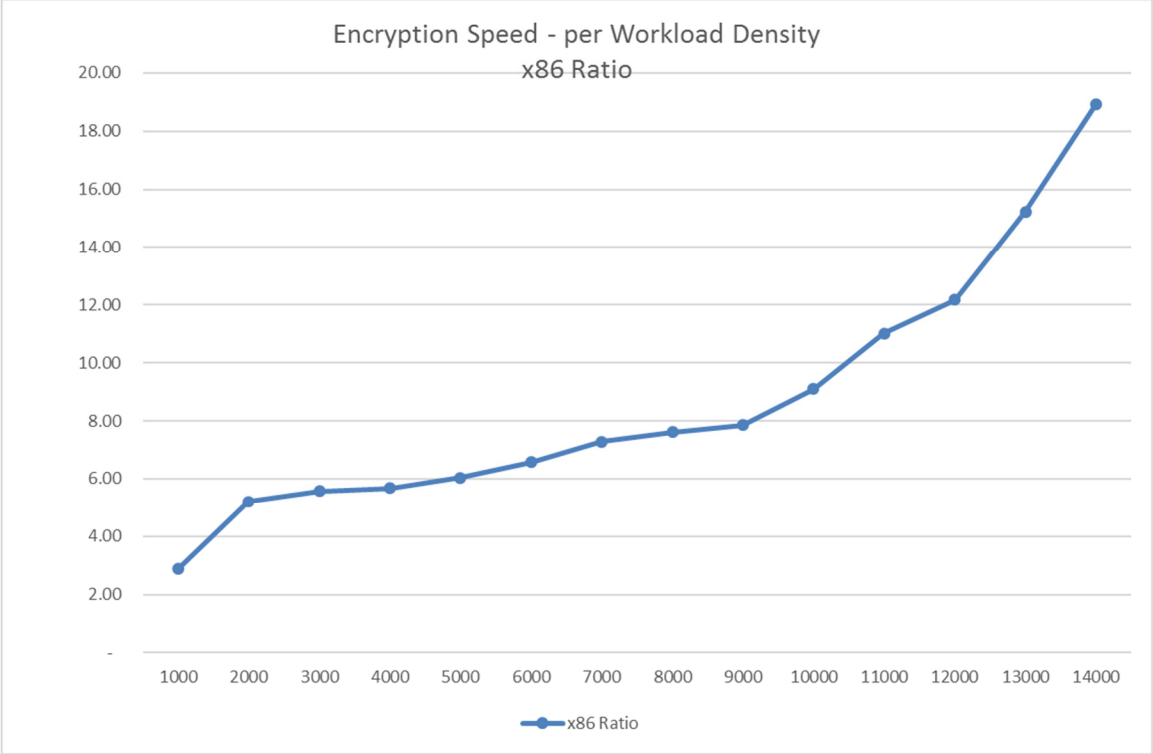
This approach to encryption efficiency adds another order of magnitude of speed onto the faster encryption engine, resulting in encryption that is 18.4 *times* faster than alternate platforms. The efficiency affects the costs also. The resulting operational cost for pervasive encryption is 5.1-8.0% of the cost of other options, which is a significant saving.



Additional savings are realized when the inability of the other platforms to scale to any significant demand is factored in. The sharp fall off in performance is severe and renders any sizable solution untenable for any platform but IBM Z. The density of the requests for encryption quickly overwhelms the other platforms' ability to deliver timely

responses and create significant wait times for completion. Such an impact rapidly renders SLAs and performance expectations unreachable. As can be seen in the following graph, the higher the density of requests, the more the overhead on the other platform engines rises. More of the available resources go to dispatching and other system activity. When the demand for pervasive encryption reaches high enough, the entire system becomes unresponsive.

The differentiation of architectural responses can be seen in the summary chart below.



The rapid fall off in x86 performance is indicative of the limitations of the current architecture. Adding on additional processors or threading provides a limited relief for a small amount of parallelization. Unfortunately, this is a self-limiting approach, since the overhead increases with each additional thread, rapidly negating the initial improvements.

SIL chose to thoroughly explore this complex issue by taking 117,000 organizations detailed activity from the last 14 months. In each of those situations, and emulated environment was created and exercised on a daily basis using customer supplied information.

The model was first stress tested by ensuring that it could replicate the reported results from the real production workload. Once that was verified in accuracy, the workload and activity were then transferred to a simulated mainframe using first selective encryption, and then pervasive encryption.

The same activity load was then compared on all three of the situations. Of the 1.16 B incursions that were captured and reported by the submitting clients, none of them would've occurred successfully if attempted on IBM Z with the pervasive encryption capability exploited.

The selective encryption model showed a significant protection also, with 92.1% of the incursions being blocked. However, the selective encryption actually was slower and used more system capacity. The efficiency of encryption was greatly enhanced by switching to the pervasive model.

This type of protection speaks directly to an organization's bottom line. The incursions reported by these customers over the 14-month period represented over $1.3 billion in costs. The costs included system time, personnel, remediation expenditures, and market loss mitigation efforts. Of the 1.16B incursions analyzed over 14- months in this study, pervasive encryption would have prevented the entire $1.3B in costs associated with those incursions.

It also would significantly lower an organization's security or application's risk profile. Since an increasing number of insurance providers require financial set-asides based on operational and application based risk profiles, anything that lowers risk will help avoid a significant financial impact on the organization. Many such insurers are asking companies to have financial set-asides as part of their IT budget. This started about seven or eight years ago and is gaining momentum today. Currently, the risk factor for the mainframe architecture is up to 80% lower than that which is required for systems that are based on x86 computing farms and other architectures. This percentage is calculated based on the overall IT budget since all aspects of the computing environment are affected when such incursions or security failures occur. An organization with an IT budget of $12M would see a difference in required set asides of $764,400 for x86 versus $160,524 for IBM Z.

One area of interest was the subset of incursions that relied on the theft of encryption keys. The stolen information was part of the public and private pairing used in the industry to secure intra-platform activities. This exposure was completely eliminated by the hardware encryption model that is present in the Z solution. With no need for handshake pairing, there were no reported successful incursions in the 14-month window of the study.

Since the impact of the thefts of other encryption keys totaled more than $6,587,500 in the study timeframe, that safeguard is another substantial advantage for the pervasive security solution.

MSP

This type of encryption also has a significant effect on those offering cloud services or any managed service provider (MSP). Inherent in cloud architecture are additional dimensions of danger based on the architecture itself. Any type of shared memory or shared resources expose the overall machine to damage not only from their own security incursions but from those of others. Sometimes known as "sideways hacking," the isolation offered by the mainframe coupled with the comprehensive and integrated encryption, would significantly affect both the customers of the MSP and the bottom line of that organization. Since MSPs frequently are locked into price contracts, any incursion that is traced to the MSP can radically affect their net profitability. Pervasive encryption would change his foundation and risk profile substantially in these cases.

RECENT EVENTS

During the time of the SIL study, there were several significant events in the security world that are germane to the challenges addressed by encryption. A weaponized virus was set loose that mimicked a ransomware attack. In actuality, it was a weapon, made to destroy. The damage from this deliberate attack was comprehensive and considerable.

Governments, hospitals, airports, and businesses were targeted, attacked, and damaged. The costs on this are still being tabulated, and will probably continue for many years. The net impact, however, was that this type of attack can and will happen again. The type of encryption that this new advance represents, coupled with the integrated Z architecture components, would've stopped it since the ability to subvert the file control is a protected aspect of the Z security layer and would therefore not be vulnerable to hacking attacks.

The trillions of dollars in effects would have been saved and the people physically hurt, and businesses that have been negatively impacted would have been safe. This fundamental change in the security paradigm for the industry is profound.

At this point in time, no other chip architecture can support the pervasive encryption model. This is due to the technical limitations on bandwidth and overhead. It will be a challenge for those architectures to tool up and build out this capability, but it is one that the industry sorely needs.

NET EFFECTS

The TCO of the encryption will require companies to look at their IT budgets. Since much of the IT budget is weighted toward application development, averaging 41.5-68.2% for the organizations within the study, any change that allows this to be reduced has an immediate effect on an organization's bottom line.

By moving encryption as a foundational security aspect to the center of a computing environment rather than making application changes to enable encryption, the net effect on the IT budget would be a reduction of approximately 22.1%.

Conclusion

> *"The implications of this mean that the cyberattack could be interpreted as an act of war, according to the organization. On Wednesday, NATO secretary general Jens Stoltenberg said a cyber attack could trigger Article 5, the principal of collective defense."*
>
> Luke Graham |@LukeWGraham, Friday, 30 Jun 2017 | 9:50 AM ET, Tech Transformers, A CNBC Special Report

The current release of the IBM Z platform has a substantial advantage in terms of TCO, performance, and risk compared to the other platform options on the market today. The current level of available selective encryption and the resistance of the native platform to common threat vectors provides organizations with a significant foundational safeguard.

However, the advent of pervasive encryption radically changes not only the safeguard that's available on the Z offerings but the industry in general. This paradigm shift is a challenge to any other offering that tries to address business today.

Companies that are actively conducting commerce in cyberspace and those that have moved to a cloud model have a huge sensitivity when it comes to cybersecurity. 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 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.

Some highlights of the findings from the study can be seen below.

Quick Summary

Category	Commentary	Quick Byte
Speed of Response	The same standard activities on Z consume up to *85.80%* less clock time than those executed on other platforms.	Faster security response is delivered by Z.
Risk	SIL risk profiling sets the Z platform risk rating at less than *1/20* of any of the alternative solutions.	The security risk is significantly lower when deploying on Z platforms.
Security Effectiveness	Based on initial installations, the foundation Z security solution provides as much as *8.5 times* the interception level of alternative platform solutions at 93% less cost in overall expenditure, and with 81% less effort.	IBM Z provides the most secure application environments.
Security Effectiveness	The Z platforms deliver base incursion interception that is as much as *20.74%* better than the alternate platform solutions with fully augmented security.	The base security delivered by Z platforms is more effective than the augmented solutions on alternate platforms.
Staff Effort	Time and motion studies show that Z security solutions require *81%* fewer tasks to implement standard protection levels.	IBM Z requires less staff effort to secure.
Remediation	Remediation costs on Z security deployments average *98.82%* less than the alternative platforms.	Repairing security damage is less expensive on Z.
Total Cost of Security Ownership	The TCO for Z security implementations are lower by as much as 83.72% than for those of other platforms.	Your security expense dollars bring you more on a Z.
Total Cost of Information	The IBM Z implementations show as much as 84.83% lower TCI over a wide range of organization size	Working with your information on Z is less expensive.
Pervasive Encryption	IBM mainframe architecture can deliver encryption up to 18.4 times faster, for only 5% of the cost of other platform solutions.	IBM Z makes pervasive encryption possible.
Risk Mitigation Funding	An organization with an IT budget of $12M would see a difference in required set asides of $764,400 for x86 versus $160,524 for IBM Z.	Lower risk on a Z translates into less financial set-aside for cyber insurance.
Uniqueness	At this point in time, IBM Z is the only architecture that can support the pervasive encryption model.	IBM Z provides unmatched encryption capabilities.

The shifting nature of cyber business is only getting more fluid. More rapid changes, active attacks, and a challenging risk management role, all combine to present dangers in addition to opportunities.

In the analysis that SIL has just completed, the original purpose was to examine the real-world impact on business security based on platform architecture. For that purpose, major architectures such as IBM's Z platforms, UNIX, and x86 products were compared.

The unexpected finding was an earthshaking change in the industry.

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 5,900 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 a better understanding of IT-centric organizational costs and behavioral characteristics. The OPMS has continued to build SIL's heuristic database, currently exceeding 475 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 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., the 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, 9,602,042 environmental setups were observed, recorded and analyzed to substantiate the findings. Customer experience was obtained to match against the deployment data. Over 6.3M 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.

Since a portion of this study examines the impact of emerging technology on the overall performance, cost, and risk of a significant number of organizations, detailed operational emulations were performed with customer-supplied data. This emulation exercised the virtual environment for those organizations for a period of 14 months of daily activity, as supplied by the participants. The results from that exercise have been included in the findings presented in this paper.

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 was 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 (26.55%), distribution (19.87%), healthcare (4.67%), retail (12.83%), financial (22.16%), public sector (6.54%), communications (3.88%) and a miscellaneous group (3.50%).

The geographies are also well represented with North America providing 32.05% of the reporting organizations, South and Central America 10.58%, Europe 33.62%, Pacific Rim and Asia 15.62%, Africa 4.74%, and those organizations that do not fit into those geographic divisions reporting 3.38% 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 a 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.

ZSL03452-USEN-00