Scaling the Digital Mountain

Enabling a Secure, Agile, and Efficient Organization

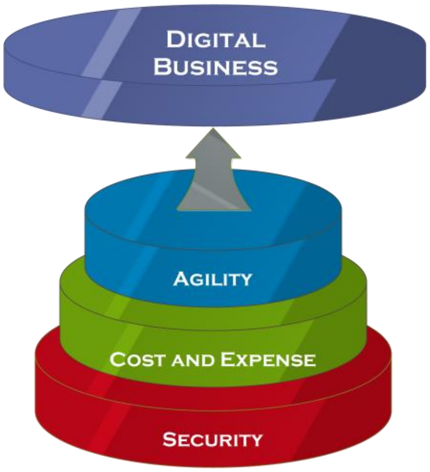
> *"We realized three years ago that if we wanted to still be in business in 10 years that we were going to have to transform our business into something that could respond quickly to market changes. Our customers were online, and we needed to be there too. I suspected that if we did not, our organization would not be a billion-dollar company anymore (sic), but an ex-billion-dollar mark on history. As I told my Board of Directors at the time, we can either be on the cyber highway, or we can be broken and discarded."*

CEO, International Retail Conglomerate, Feb 2018

INTRODUCTION

Do you want to be in business in 3 years? That may sound like an inane question, but it is the basic question that faces every organization that exists today. The transformation of business into a participant in the digital market is going on right now, and it is a race. The organizations that understand the foundation of this new world are embracing the opportunity while others are lagging. Above all, the organization and their customers have to be *safe,* protected in their dealings, and secure within the safeguards of their data.

In an environment where customer interaction is slow and controlled, businesses have the luxury of updating applications and service offerings on an annual or biannual basis. Those days are gone. The 24-hour-a-day availability afforded by globally dispersed and expanded markets means that a larger mass of customers is pushing different and sometimes conflicting customer demands.



DIGITAL MARKET FOUNDATION

Each and every organization attempting to compete for customer business and loyalty faces daunting moving targets. To stay in that game, the less agile organizations are being pushed to adjust their attitudes toward innovation and attention to the individual consumers who comprise their customer base.

Constant innovation and "fresh" offerings have become a requirement if a business is to be worthy of buyer consideration. In many retail, end-consumer markets, customers are bombarded by organizations that release updates frequently, so an organization that only provides innovation slowly and unresponsively to the same customer demand has lost the advantages previously gained on quality or range of product.

In the market today, customer loyalty only goes so far. It has to be reinforced and reaffirmed every day and every hour.

This competitive metric pushes flexibility and market responsiveness to the top level of business requirements. Trying to blend that into a commercial interface which is cost-effective and secure has stymied many organizations. For the less adaptable, the attempt to rearchitect the organization while straining existing infrastructure and organizational procedures to their maximum capability has resulted in significantly adverse effects, and in some cases, complete failure.

In the worldwide digital marketplace, getting customers and keeping them requires innovation and agility. Without that type of responsiveness, an organization will not survive for very long. It will simply be run over by its competition.

DIGITAL TRANSFORMATION

> *"We went from being the Flintstones to the Jetsons in 9 months."*
>
> David Giambruno, Senior VP & CIO, Tribune Media

The transformation train is coming, and the question is will your organization be on it. This is a big shift in how business is conducted, and it requires the best tools and targeted expenditures. The evaluation of the components that will be incorporated into an organization's infrastructure is especially critical at this point, where the whole commercial world is in an uproar.

Matching up customer needs and product offerings in this situation is crucial but is complicated by the driving urgency. Organizations with products or services that are able to address some of the challenges in that evolution are scrambling to understand exactly how their offerings can best help their customers.

The overriding need within the growing digital business market is security. This encompasses not only the safeguard of an organization's digital assets, such as finances and processing integrity, but the stewardship of customers' information. Woven into the fibers of business on the web is an implicit base of trust between those providing products and services, and those choosing to buy. Any continuing customer loyalty and success in digital business has to be based on this foundation of confidence.

Another basic tenet of conducting business in the increasingly digital landscape is the speed at which an organization responds to the marketplace. Whether it is a demand by customers for new features or functions, the opening of a new market, or remediation of problems and issues, those conducting business as a digital participant have to be able to support increased speed. The aspects of speed range from faster time to market through the organizational flexibility that allows a business to amend its procedures and offerings better to communicate with its customers and serve them. The days of slow response are over. Those that will prosper in this digital world are the organizations that move quickly and continue to evolve.

The third priority in digital business is controlled expenses. Increased operational efficiency matches the lowest cost against the required functionality, producing a lean and cost-conscious organization. Whether the costs are from the provision of goods or services, or from the necessary expenses for securing the assets, the balance of revenue and expense continues to determine the overall health and viability of the digital business.

The digital transformation of an organization to a strong player in the marketplace requires coordination of changes, a whirlwind of many evolutionary pieces going on at the same time. It makes sense to start that journey with the best foundation possible.

SECURITY – KEEPING CUSTOMER TRUST

> *"Cyber-confidence is crucial for finance. Consistency between security and threat is a key factor in Reputation and Customer Trust."*

Stéphane Nappo, IBFS Global Chief Information Security Officer & Board Advisor, Paris, France

Customers need to be able to trust an organization to protect the information that it collects from them and uses to conduct its business. Failure in this area erodes an organization's reputation faster than any other factor. It is perceived as a betrayal in an unspoken contract between buyer and seller.

Customers that feel betrayed by a business are far less likely to go back to that organization. In a study of over 175,000 organizations, more than 78% of customers refused to go back after a breach if the organization did not own up to it immediately and explain precisely what it was doing to remediate the vulnerability and repair whatever damage has been done. Trying to cover up the incident was seen by over 95% of the customers responding to the questions as a mark of disrespect for them as individuals. Or as one respondent put in his notes, "Why would I want to do business with the merchant that has shown that they don't see me as a person? Why would I want to do anything with someone who doesn't value me?"

> *"No sooner had we replaced a large number of servers and paid out millions of dollars in recovery services in an effort to fix the problems from a ransomware attack (sic) then we were hit with a second one. It came seriously close to putting us out of business. For a financial firm to be non-operational for days at a time destroys a lot of the reputation we have spent so long building up. We spent millions of dollars trying to recover and estimate that we were successful only to 75%. Not only did we spend millions of dollars internally, but we will spend tens of millions of dollars to convince our customers to come back."*

CIO – Medium-Sized Financial Services Firm

How much is the viability of an organization worth? What would the loss of 35% of customers do to the bottom line? This is the realistic offset to the hassle and expense of cybersecurity. If customers don't trust an organization, they're not going to do business with it.

The horrendous data breaches that have been bandied about in the news over the last couple of years have shown the dangers of the digital marketplace. Not only is an organization conducting its business exposed to constant attacks, but when those attacks are successful, it is not just the intellectual capital and assets of the company have been risked, but the information of their customers.

The impact of breaches on customer confidence and follow-on sales has been tracked, and an analysis of that data shows that after a significant incursion that the average customer fall-off exceeds 41%.

This results in an immediate and long-running drop in revenues. It also further exacerbates the already damaged reputation of the business. Depending on a series of remediation factors, those customers may never return. If they do, it will only be after a significant outlay of service, equipment, and personnel expenses to reestablish a trusted position and woo the customers back.

The cost of getting a customer back after a breach can be as much as 18.6 times what it cost to get them initially. Any market expansion will have to deal with reestablishing reputation so that new customers feel confident enough to engage with the business, after the demonstrated vulnerability and failure.

In other words, being successfully hacked is extremely bad for business.

AGILITY – MARKET SENSITIVITY

> *"It's no longer the big beating the small, but the fast beating the slow."*

Eric Pearson, CIO, International Hotel Group (IHG)

One of the primary metrics for success in the digital marketplace is the ability to respond to the aggressively changing audience that the worldwide market exposes. When an alteration in that landscape emerges, it is frequently the first responders that can reap the benefit of the opportunity for market share increase and higher revenues.

An increasingly mobile and distributed digital mixture is driving new and complex challenges for business. The requirements raised by these challenges vary. They include diverse areas, such as scaling to handle activity surges, constructing security to protect process and data, and stabilizing performance to ensure consistent response time, all while delivering data for insights and transaction personalization.

In this environment, the hidden layers of infrastructure and best practice matter. The underlying IT and business choices are more critical than ever, although equally invisible. The combined influences of those characteristics build into an overall metric of customer experience (CX), and that is what establishes market share and creates customer loyalty.

> *"Ten years ago, we were considered an innovative company because we updated our product offerings twice a year. Right now, we are lagging our competitors because we are only rolling out new releases every 6 to 8 weeks. The feedback we are getting is that our customers think we are not keeping up with the rest of the market. It is absolutely imperative that we react faster to our competitors or we will lose customers. Once we lose them, they don't come back easily or cheaply. Today's customer has a view that is highly subjective, incredibly fast, and extremely critical. Our ability to show constant innovation in response is more crucial than it ever was before."*

CMO - Very Large Insurance Company

As more commerce is conducted in real time, end-user visibility of the results from IT infrastructure effectiveness and efficiency increases. Any shortfall in applications that exhibit public lack of quality is reflected in customer abandonment and market erosion. Slower response in either application performance or customer support can have far-reaching, sometimes catastrophic results. This is not only a single sale or transaction effect, but an extended trend for a customer's reaction to the virtual marketplace.

The change in visibility of service delivery quality is altering how organizations select their IT infrastructure. Where shortfalls in quality are tied more directly to revenue flow, the basis for determining appropriate expenses and costs undergoes a radical shift. This means that a compelling evolutionary step in IT infrastructure selection, configuration and management is taking place. The operational structure is reforming, as the vision of the underlying relationship among computation, storage, IT staffing in its support of business alters. The complexity of cloud deployment versus on-premise operations has only complicated this.

The end user CX combines two very disparate perspectives, both of which are equally important. The intuitive design of the customer-facing application and the unseen platform that delivers it are not separate in the customer's mind. The user takes them as a whole and evaluates them as such.

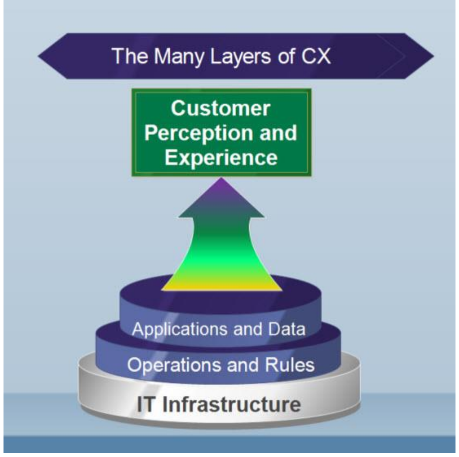
A CEO's awareness of slipping market share or declining profitability would typically result in cost-cutting. However, when CX is included in the mix, the effect on that market perception must be considered when appropriately targeting costs. Where before it would have been a compelling business case to just look at disposable and inexpensive components, now the effect on CX of system reliability can easily override short-term costs.

There are significant contributions to CX that have nothing to do with platforms or applications. Those are no less important to the success of an organization operating in cyberspace. These dimensions are more controlled by organizational posture and processes than anything related to the actual computer. They can loosely be summarized as:

- Importance of the end user to the organization
- View of the customer as an individual
- Flexibility to provide individualized responses to the end user

All three of these relate to how the organization's valuation of the customer is viewed.

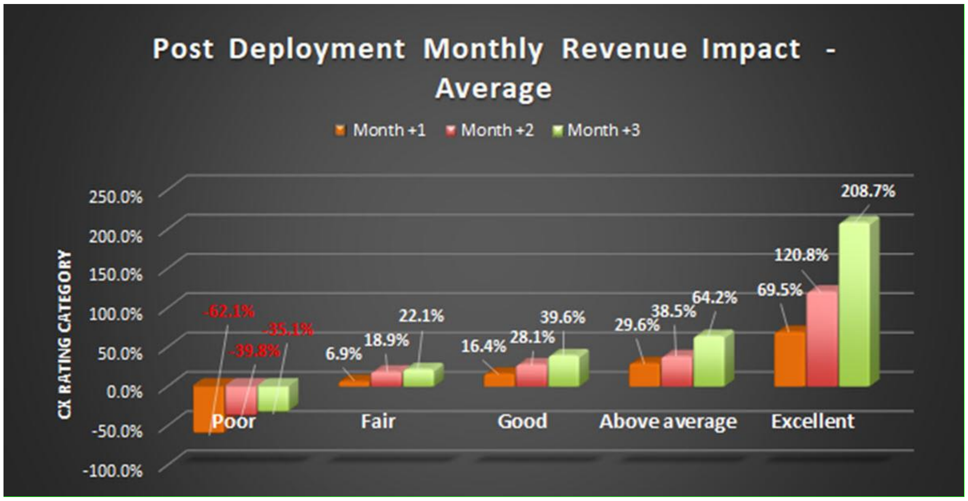
The support of the concealed IT infrastructure as it enables business can be further broken down. A targeted goal of competency, valuation, and viability is created by a layered supporting structure that includes the applications and data, the operational environment and the supporting IT infrastructure.



The composition of each layer can positively or negatively affect the other layers. Since CX is a blended result of the synergy among all levels, it cannot easily be pulled apart to focus on a single component. Any can result in a ripple effect that significantly influences the outer rings of business and customer interaction, and CX. Whether it is the application providing an interface to the customer's actions, the rules that allow quick credit decisions, or the hardware that delivers data quickly and consistently, all levels are essential.

At the base of overt CX is timely delivery of actions that have the end user as the focus. Since CX has a direct impact on the net revenue, the virtual marketplace has increasingly focused on this aspect.

The justification for this focus can be seen in a graphic representation of 14,071 sites that deployed new applications in the last 6 months. These have been grouped by CX rating categories of 0-5, corresponding to a subjective range that typifies the experience from poor to excellent. The average monthly revenue change starting from a base of the first month is shown to give an understanding of how CX affects the cash flow and net revenue of an organization.



The impacts are averaged relative to the starting month but show a relationship between the overall CX and income. The deployments that offered suboptimal experience show that revenue levels never successfully regain lost ground against those deployments with better-perceived CX.

The two customer quotations below show the radically different picture from the opposite ends of the CX value range.

> *"Our new retail product offering went online seven months ago. We spent millions of dollars on advertising campaigns, development, and hardware. Our marketing department did an excellent job and got the word out and things looked great… for the first three days.*
>
> *The overall system had six outages in the next week and we lost at least six hours of availability. The carnage on social media and to our customer support organization was horrendous. The optimistic estimates, based on the first three days were totally invalidated by the problems we had. Once we figured out the problems, we couldn't react fast enough to recover.*
>
> *The first month's revenue didn't even reach 10% of what we expected. To further worsen the picture, we spent over $400,000 in an effort to expedite equipment, get the assistance from vendors and other service providers, etc. In addition to that disaster, we ended up spending an additional $150,000 to try to explain that we fixed the problems in a way that does not make us sound totally incompetent. The ongoing sales have not even reached 50% of what we expected monthly for the very first month because we can't get our customers to come back."*

COO - Large Retailer

The risks of a poor launch are offset by the rewards that can be realized by a successful and stable deployment. The opportunities for revenue and new customers are immense, and the need for competitive positioning drives organizations to continue to learn more about the methods that work well for them.

> *"We had a deployment of a new sales product application about nine months ago. We were pleased with (what) the worker teams did and very happy with the minimal problems we had post-deployment. The market reception has been very good to the new system and it shows. Currently, we are running about 60% higher volume than was projected and it has become our most profitable*

> *channel. We are trying to roll out incremental changes and expansions every month, which is definitely helping to keep the momentum going. Customer feedback is very good and I think that helps a lot."*

LOB VP - Services

These two anecdotal experience points are echoed multiple times in the large number of customer quotes received as part of ongoing data gathering, reinforcing the critical nature of CX to organizational success. The functionality, personal focus and performance components of the CX view are magnified by other aspects but tend to blend into a single perception of market success.

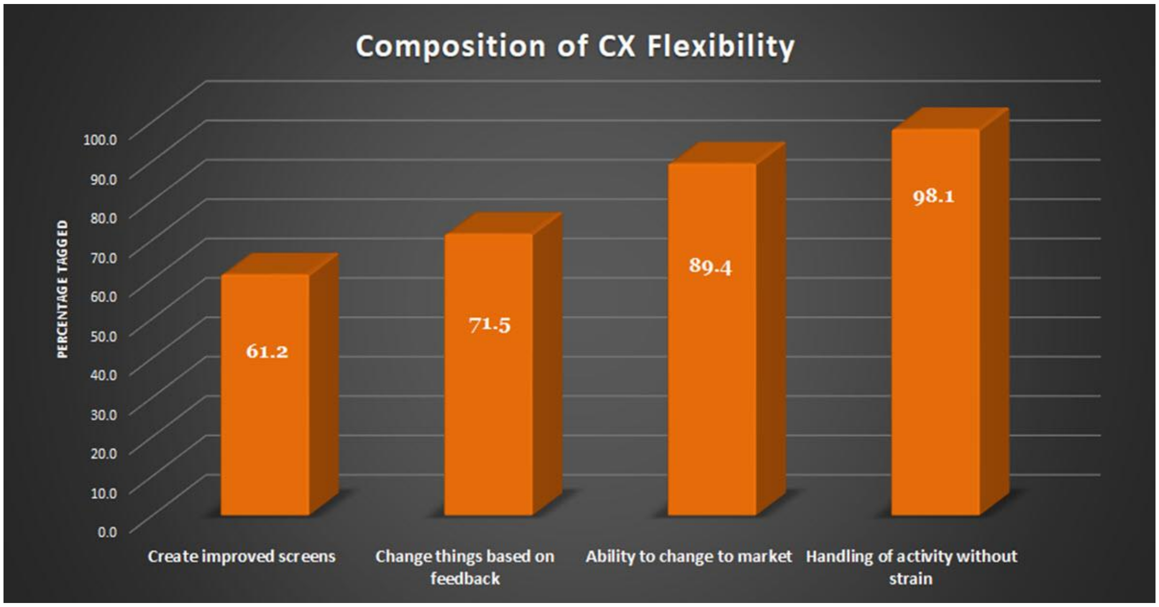
> *"It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is the most adaptable to change."*

Charles Darwin (1809-1882)

The market demands flexibility. Precisely what that flexibility might be is another blended perception. Information provided by over 140,000 globally dispersed end-users on digital market expectations demonstrated that all wish flexibility, but that term has differing combinations of reactive and proactive ingredients. The reactive is displayed in the organization's willingness to modify interfaces, rules, and processes based on customer feedback. The proactive is represented by the ongoing efforts to provide customers with the newest "toy" or fad as quickly as possible.

Although this view of flexibility is tightly coupled to speed but is not all that drives it. The part that is not sheer velocity has two main aspects. The first of these is visibility to the evolving and changing offerings. The second is consistency in delivery.

As shown in the chart below, the flexibility and resiliency of the organization to handle unexpected loads without displaying the load to the customer are essential. A response and delivery time that is similar for repeated customer interaction allows the user to have their underlying expectations met. Additionally, there is minimal inconvenience to the customer stemming from erratic or delayed delivery of the desired service or offering. When that lack of consistency occurs, there is a trackable loss of customers.



It is evident in the analysis of the customer responses that this mass expectation of flexibility is critical to CX and hence to success in digital business. What this signals is the onus placed on the organization to create a highly mutable development organization, expandable customer support group, and the foundation of resilient processing architecture.

Part of the changing paradigm of the very agile digital market is visible and speedy responsiveness to change. The evolution in applications and offerings may be due to customer feedback, changing regulations, alterations in other vendor's interlocked technologies, or a myriad of other things. It is no longer adequate for an organization to make the changes. They must also make visible their willingness to respond to their customers.

That visibility addresses the need of a customer to feel relevant to the organizations with which they interact. Where it is no longer a matter of cheerful clerks or attractive brick-and-mortar stores, the communications of the organizational attitude around their perception of their customers is vital for customer adherence.

Communicating that viewpoint in cyberspace can be challenging, but its essential nature means that this is something that an organization cannot bypass addressing.

COST – 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. Sometimes referred to as "effective spend," this metric 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. The calculation is typically based on money (cost), people (headcount or Full-Time Equivalent - FTE), or time and effort, all versus revenue.

The dynamics of digital business complicate this calculation primarily due to the inability of most organizations to tie their commercial behavior to customer response. In a group of over 190K organizations, less than 1.4% of the organizations had a formal method for associating their commerce to customer reaction. That lack of tie-in increases the difficulty of internal analysis into potential areas of improvement and the value of the change to the organization. However, without a good understanding of the connection of customer reaction to revenue flow, businesses are at a disadvantage and may spend far more money than necessary in the ongoing operations of commerce in cyberspace.

With less reliance on physical locations, the efficiencies of spending become one of the most powerful tools for increased net revenue. It is one of the strongest attractions of the digital marketplace. If organizations do not leverage the opportunities that this environment offers, their competitors will.

STRATEGY IN CYBERSPACE

The trend and scope of the dangers continue to accelerate, keeping in step with the imperative to operate in the new landscape of a digital world and the possible opportunities that exist there.

To many organizations, the challenges are overwhelming. They are struggling to find stable footing for their cyber business, continually fighting with failing machines, security breaches, and erratic performance. The constant fire calls drain the energy from the organization while depleting its coffers and result in more business volatility than has been seen in decades.

The new face of due diligence and the demands of rapid market response show how inadequate current organizational approaches and postures are to address the increasingly aggressive nature of the digital market environment.

Driven by customer demands and business dangers, a change is needed. Ultimately, the necessity for change can be encapsulated by a single question.

Do you want to be in business in three years? If the answer is yes, then a paradigm shift is needed. And that shift needs to address the need for flexible and responsive market reaction that is secure and can scale to the variable demands of the successful digital business.

SOLUTIONS FOR A DIGITAL BUSINESS

The strategy and challenges of crafting an organizational path that successfully navigates the chaos of cyberspace to potential customers require an understanding of the different components that need to be incorporated along that journey. That translates into a need to have information on both business and security and how they interact.

The behavior of any specific IT platform solution that supports and enhances optimal customer experience and the rigors of digital business must include both technical and business considerations. Since the impact of platform selection on digital business performance is reflective and difficult to quantify, IBM asked Solitaire Interglobal Ltd. (SIL) to provide an objective review of the IBM LinuxONE offering.

SIL has been gathering data on market evolution and production behavior for over 40 years. Supporting more than 6,000 clients and performing over 100M predictive models each year, SIL has also run the Global Security Watch (GSW) for the last 22 years. That member service has allowed SIL to build a repository that exceeds 550 PB of data at a very granular level. That data is mined every hour for trends, comparisons, and threshold that help organizations succeed.

SIL gathered additional data to supplement its extant data repository and performed analysis to clearly articulate the benefits and relative costs seen reflected in customer-reported productions where organizations have deployed IBM LinuxONE. This analysis has been primarily directed at the incremental value, both positive and negative, of platform use from a business perspective. With this information, business leaders can better understand the tie between IT platform and the impact on revenue and customer response to their organization.

Digital business and security go hand in hand, so any analysis has to include extensive correlation between the two. SIL has been monitoring aspects of business and security for over 22 years. The collection of information via the GSW provides thousands of organizations with trend and risk information on an ongoing basis. This constant feed of anonymous data on what has become the critical landscape for businesses today has provided a fertile ground for many studies over the years.

A recent study showed that both the rapidity of market demand for change in response and the number and size of threats active in cyberspace have grown hand-in-hand. As the market potential has enlarged, it becomes a far more attractive target for criminals. Whether those criminals are sponsored by nation-states trying to affect other nations' stability or for more straightforward financial gain, cyberspace has become ultimately attractive to and highly dangerous for business.

GSW is a member service that has tracked the detailed evolution of security threats and the associated effect on business on a worldwide basis for decades and currently collects reported information from more than 12.1 million organizations. The data from the GSW provides a broad 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 primary focus relates to the impact on the business operation, organizational assets, and prevention and remediation costs.

Using data from customer experience responses, IT operational details, business performance, and security, SIL examined the positioning of IBM's LinuxONE in the digital business market. The results of that examination have been grouped into three areas: security, agility, and cost. These areas incorporate the main focus objectives that organizations operating in cyberspace regard as the most relevant.

SECURITY AND RISK

Risk within a deployment comes from many different areas, but the foremost of these is successful incursions into the systems and infrastructure of an organization. The prevention of that is the principal duty of the security personnel within a digital business.

To these personnel, there is no acceptable loss. Every breach, every violation, every breaking of the protective shell is potentially catastrophic. With the number of attacks increasing on an hourly basis, organizations are frequently bombarded by unrelenting attempts to destroy, steal, and prevent others from using the commercial services.

In that battle, the baseline characteristics of the infrastructure play a prominent role. This is especially true when the underlying architecture of the technology is designed to make it difficult for hackers to succeed.

In general, hacking is opportunistic. Just like a burglar will go for a more vulnerable victim to rob before a difficult one, many hackers attack obvious targets. The complexity of this has changed considerably with the rise of organized crime's participation in cyberspace. For these criminals, the focus is less on easy targets than it is on those that provide the most value for the crime. Adding another layer of complexity, nation-states are now more heavily involved in theft and destruction as part of undeclared cyber warfare. These three very different profiles of cybercriminals have increased the complexity of the dangers of cyberspace to a new level.

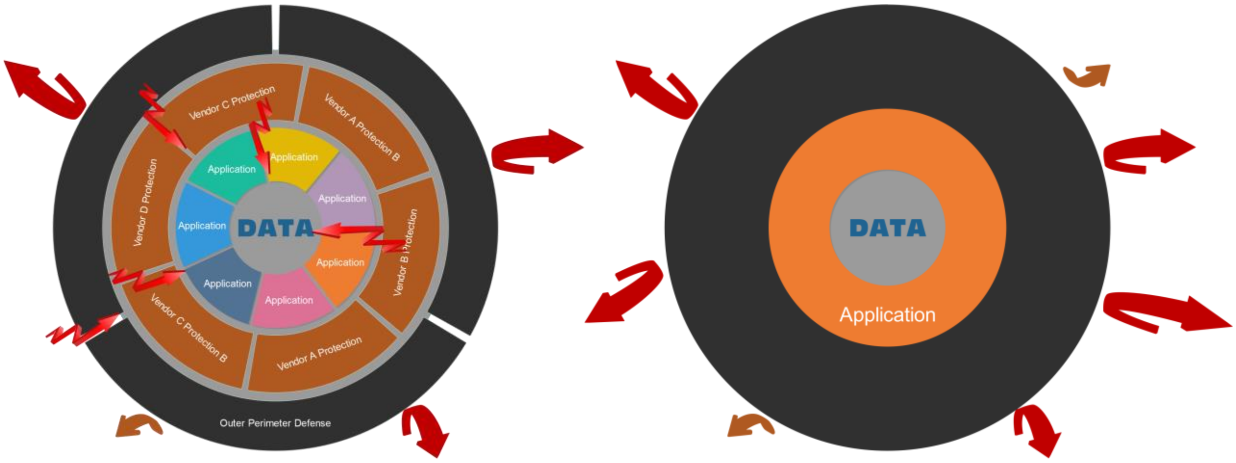
If breaching protection is too difficult, hackers frequently turn their attention to easier prey. Additionally, many enhancements in the hacking community are designed around new, sophisticated tools and techniques, including virtual robots that relentlessly pound on security walls looking for a chink in the protections. This is where the difference in architecture plays a significant role.

BOLT-ON VERSUS INTEGRATED SECURITY TOPOLOGY

Many of the available architectures in the commercial space use a philosophy of bolt-on security. Individual organizations have a choice of how to assemble their own security protection and can pick among the myriad of offerings.

The weakness is that with bolt-on security there are always conductivity joints, places where one piece of the protection has to talk with a different product. By the very nature of those joints, they provide vulnerabilities and opportunities for hackers to get in. However, that is intrinsic to the design and is touted as "flexibility and choice" by those that employ it.

An alternative to bolt-on security is a fully integrated stack. In such a digital construction, the joints are structural and not optional. There are fewer joints and weak places, limiting vulnerability points and assailable logical surfaces.



Bolt-On Security **Integrated Security**

The success of LinuxONE security is based on the implementation of an integrated stack. It implements the concept of protection that allows no purchase for those that would climb in, no chink in the armor to be exploited. Although not infallible, it provides a significantly smaller assailable surface.

The success of this architectural choice for security is demonstrated by the fact that SIL's GSW has recorded *less than 0.01%* of successful security incursions against LinuxONE implementations per 1,000 deployed applications than the other architectures.

During this study, the main behavioral characteristics of software and hardware were examined carefully, across a large number of actual customer systems (13M+). 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 data 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.

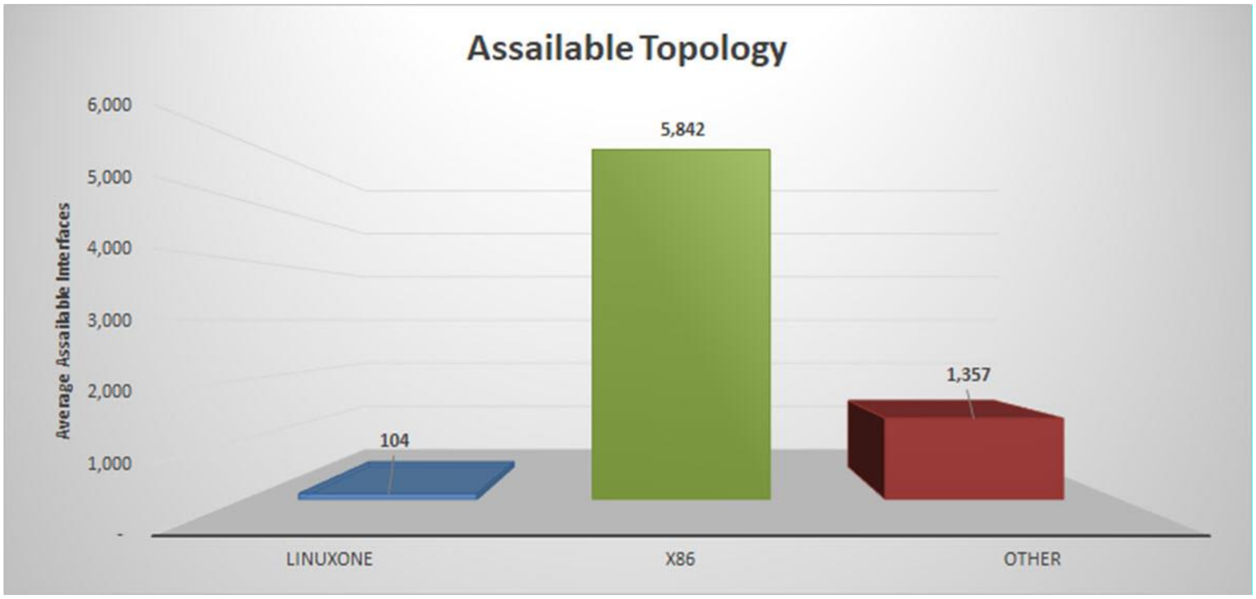
Over 164 million data points of detailed incursion activity and impact from the GSW provide a foundation of expectable costs and exposure, which is essential to understanding security and asset protection in today's marketplace.

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 essential, 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 leaders have to make daily.

ASSAILABLE TOPOLOGY

One critical factor in risk and vulnerability in the security arena is that of assailable topology. This quantifies the relative weakness of different architectures.

The assailable topology varies among the foundational architectures significantly. A general analysis of a group of over 131K organizations illustrated this difference, as seen here.



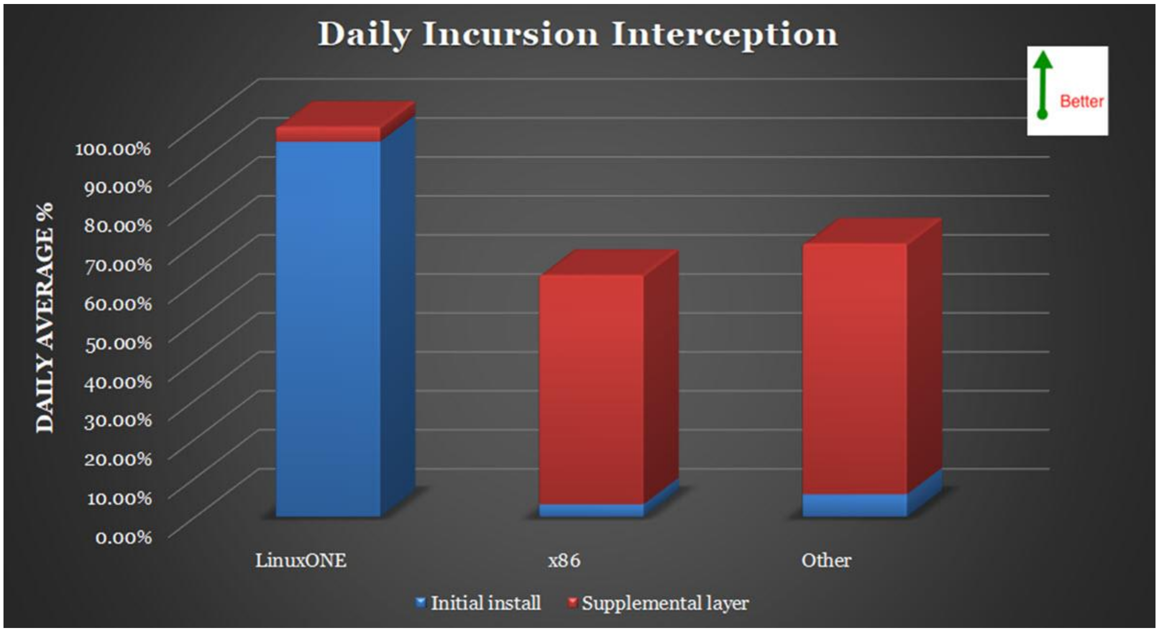
The most significant difference stems from the base structure and realized strategy behind the platform architecture, chip design, operating system, and method of stack integration.

The nature of embedded LinuxONE 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 efficient strategy pulls the policy control and definition to a more centralized point. The highly integrated and embedded LinuxONE security stack provides a significant advantage in this area. Coupling that firm foundation with the flexibility of LinuxONE seamlessly blends the core platform strengths with the architectural choice.

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 attacks 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 included. 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 setup and the supplemental layer, expressed as a percentage of incursions that have been blocked.



Based on initial installations, the foundation LinuxONE security solutions provides as much as *15.74 times* the interception level of alternative platform solutions. Additionally, the LinuxONE solution offers a base, foundational protection that exceeds 96%, 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.

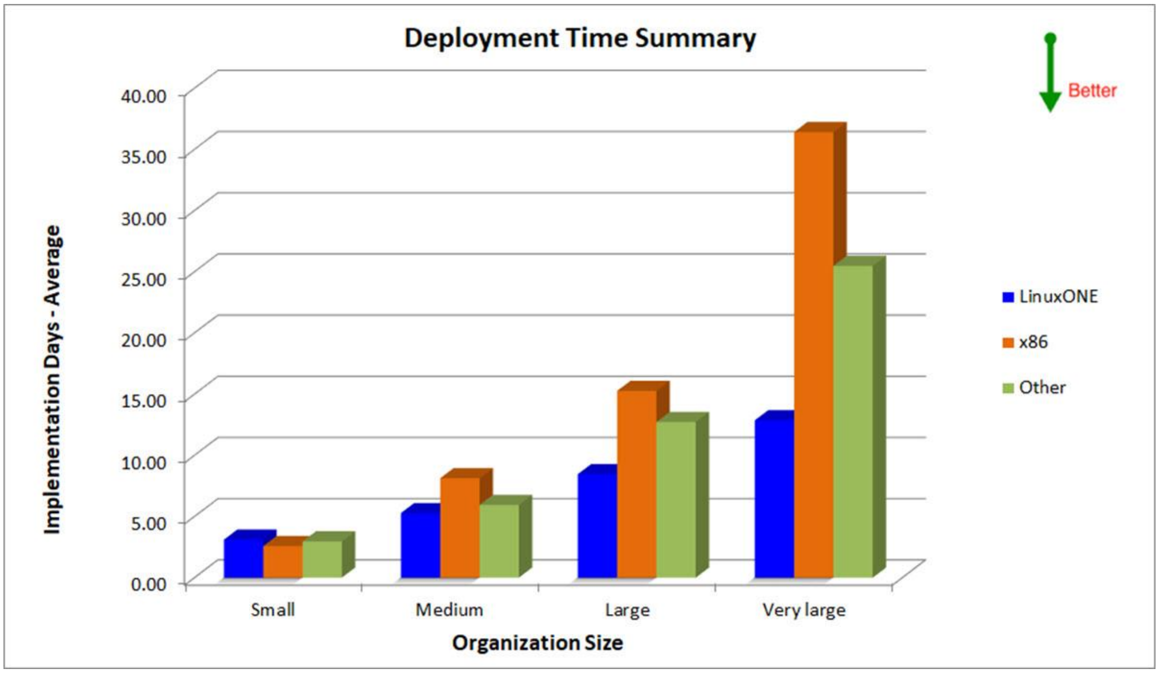
The combination of intellectual capital and automated services, coupled with the architectural design of the LinuxONE cybersecurity solutions, results in the interception of a significantly higher percentage of incursions. The LinuxONE platform delivers base incursion interception that is as much as *61.4%* 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 crucial differentiation, this study is focused on an examination of vendor solutions that combine platform hardware, software, middleware, and operating systems.

AGILITY AND FLEXIBILITY

Customers in cyberspace expect responsiveness. Whether that optimized reaction to needs or problems is driven by innovation or by market changes, failure to perform in this area puts a business at a significant disadvantage.

To understand the differentiation that a specific platform makes in this arena, the millions of experience points of the organizations reporting into SIL were analyzed and summarized in the chart below. This graph shows the average deployment time based on a normalized 200 function point application. To avoid any confusion that continually updating tools provides, the analyst deployments are restricted to those that were implemented in the last calendar year.



There is a substantial differentiation when it comes to the amount of time that it takes for an organization to deploy a new version or new application based on the underlying architecture. The optimizations built into the LinuxONE platform augment provisioning, testing, and other factors to produce agility that averages as little as *35.3%* of those required by other platforms.

This increase in agility is significant since most organizations will deploy tens if not hundreds of updates and releases during a calendar year. Any savings in time from initiation to deployment translates directly into reducing cost and increasing responsiveness to the customer. Since that metric has been shown to be one of the most important when working in cyberspace, this factor is worthy of note.

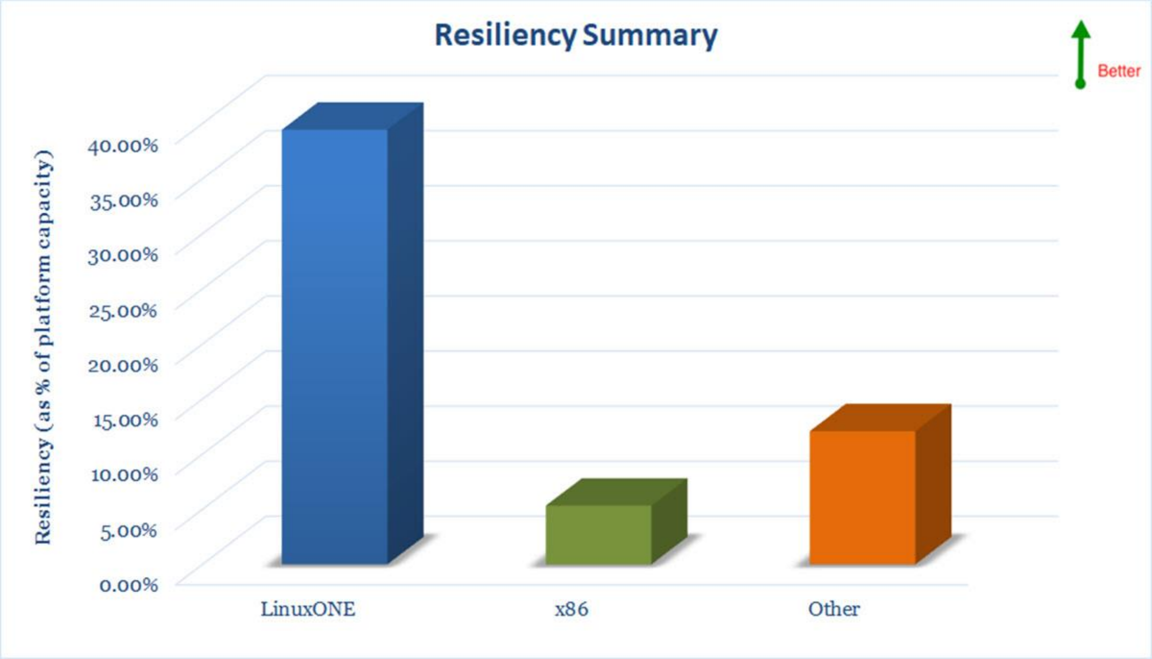
The demand by customers for flexibility in the digital world translates into contributions from both IT and business. On the business side, the term is applicable primarily to strategy and approach. The willingness for an organization to change direction and follow market or customer requests and demands is one of philosophy.

In addition to the operating principles that govern an organization's direction, business flexibility means modifying offerings and products so that they are always relevant to the customer base. None of those are tied explicitly to the IT platform that enables them.

The portion of flexibility that is contributed by physical and virtual platforms is that of broad-scale adjustability. As requirements for localized support are defined, the platform must be able to be efficiently reconfigured. If demand surges either seasonally or because of highly favorable market response, the platform should be able to service those demands.

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 LinuxONE deployments and the remainder of the solutions. The reported, average resilience of the LinuxONE 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 lower total cost of ownership (TCO) and total cost of information (TCI), another commonly used business metric.

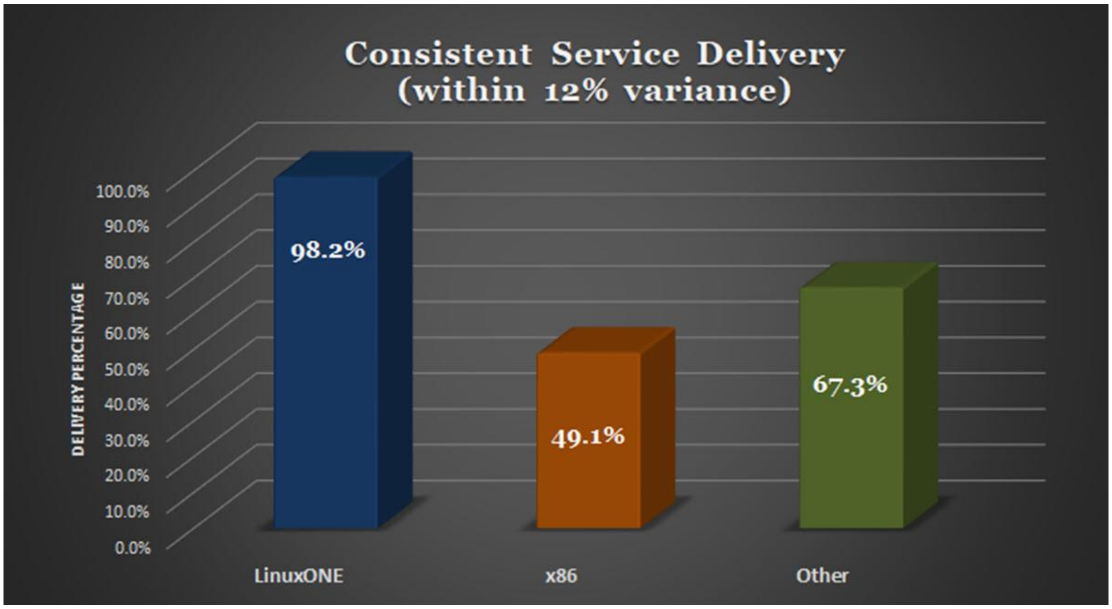
Another aspect of the flexibility is the ability for the delivery of consistent customer experience. It has been shown that predictable and consistent behavior is a cornerstone of customer satisfaction. Erratic or widely varying behavior unsettles buyers and leads to a higher number of support calls and complaints.

The delivery of consistent response time is primarily platform dependent. Although application design provides a framework for the overall traffic of data to and from the customer, the consistency is controlled substantially by the internal capabilities of the infrastructure.

An analysis of over 17 million complaints of poor response time showed that the threshold for recognition of varying response time is approximately 12%. With that in mind, the performance of the platforms in the study was examined to see what portion of transaction response time fell within those parameters.

It should be noted that the applications reviewed covered a broad spectrum of customer, vendor, and internal applications. There was no attempt to normalize the behavior since what was being determined is the variance within each application for the same activity.

In addition to variance in the percentage that fell within the threshold of detection for consistency, the amount of variance that was observed in the protection behavior was significantly different among the different architectural groups. The influence of the same mechanisms that allow the IBM LinuxONE solution to support the consistent delivery also dampens the swing of variation.



The LinuxONE solution shows up to *2 times* the percentage of consistent delivery of transactions compared to the other architectural groups. Additionally, while the other solutions showed variations as wide as *17 times* the average response interval, the largest variation recorded for LinuxONE was *36.2%*.

The comparison of erratic and inconsistent delivery of digital services shows that the IBM solution is far less likely to trigger customer dissatisfaction.

COST AND EXPENSE

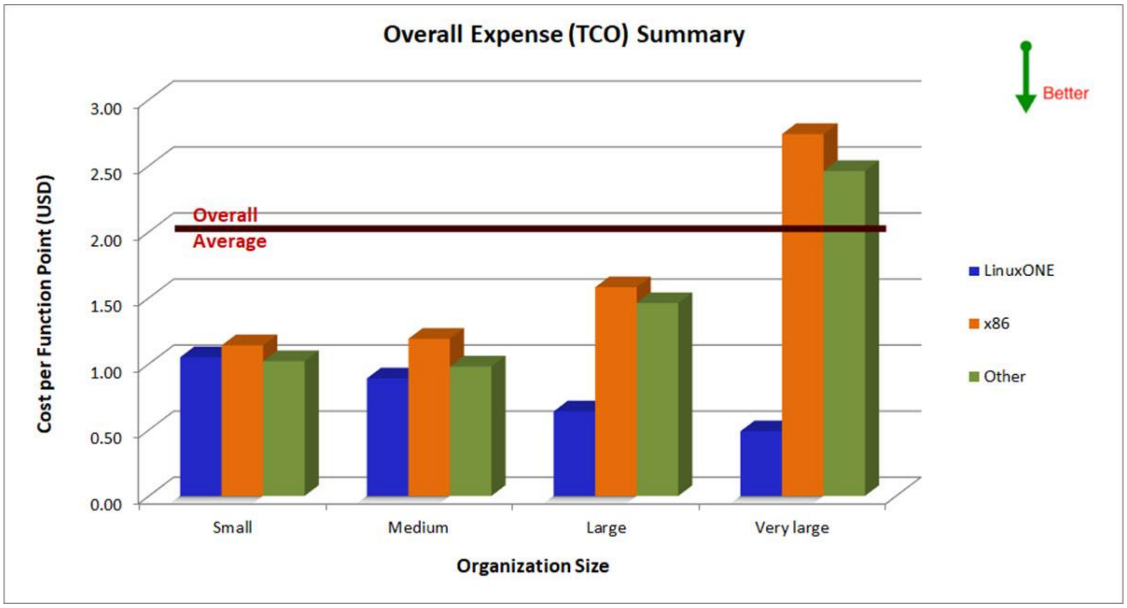
Cost is a primary metric in business. Optimizing revenue while minimizing cost is the game that industries play on an ongoing basis. While there are many different ways to examine cost and expense, the most portable metric when reviewing this portion of the financial profile among disparate companies is to TCO and TCI. Since both of those can be normalized using a standard workload unit such as function points, the method of comparison works from very small companies to very large ones.

Part of the justification for conducting business in cyberspace is the control and limitation of expenses. Without the overhead of a series of brick-and-mortar locations, the digital market is far friendlier to the bottom line.

TOTAL COST OF OWNERSHIP

TCO provides one of the leading business-side metric for operational efficiency. This high-level metric aggregates all of the expenses within the organization that contribute to any aspect of operations. Once again, the projects and their expenses have been normalized based on a standard basis. This enables large and small organizations to be more accurately compared.

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 LinuxONE. A declining pattern of unit expenditure translates into the efficiency of scale, where the leveraging of framework and foundation allows a cost-efficient model of financial investment. As seen in the accompanying chart, the expenditures for LinuxONE security implementations are lower by as much as 82.12% than for those of other platforms.

This stems partially from the combination of architectural components and highly scalable platform. The efficiency of this synergy is demonstrated as the architecture is more heavily loaded as a significant drop in cost for work unit is realized. This footprint is present in all situations where the structure is designed for highly scalable environments but is more commonly 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 LinuxONE VMs give a good return on our investment dollar. They have a lower incremental cost per VM and also are much faster to provision and modify. That translates into lower personnel costs which is the big challenge in my organization. If we have a system that has to be brought up in a big hurry, it's definitely going on LinuxONE. Easier to get the cost justified, faster and easier to get deployed."*

CTO – Medium Manufacturer

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

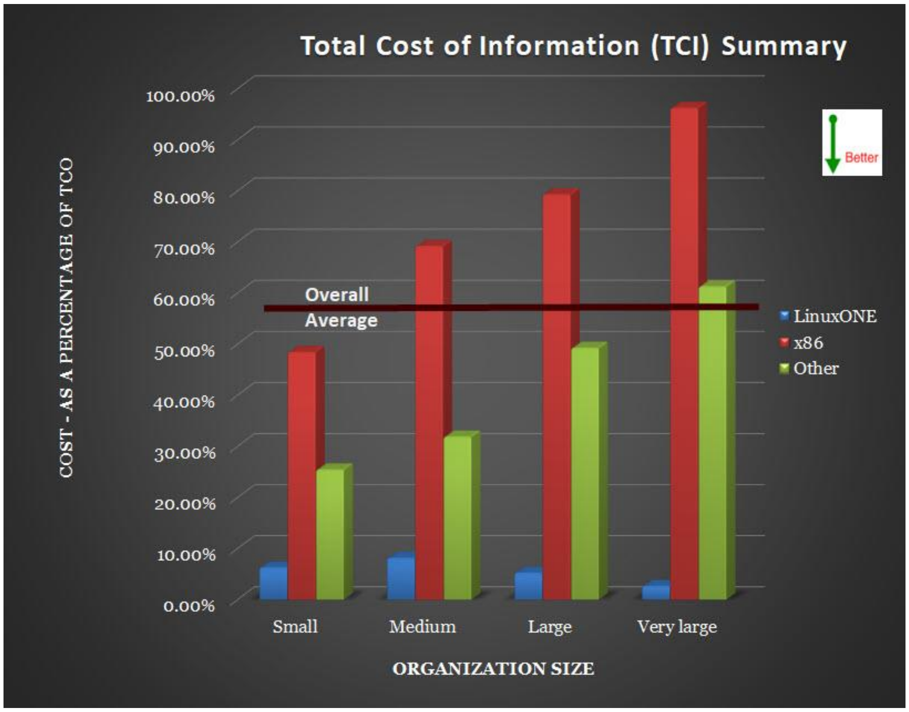
TOTAL COST OF INFORMATION

The costs associated with digital business include both the traditional metric of TCO and the newer metric of 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 measurement 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 LinuxONE implementations show as much as *92.04%* lower TCI over a wide range of organization sizes. Since this metric is a key driver to new implementation costs, the smaller factor reinforces the efficient scaling present with the LinuxONE 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 mainly 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 that 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 LinuxONE security configurations are lower than the x86 and other security options on both the traditional expense basis and on the reflective expenses due to incursions. This represents the difference between a highly integrated security stack versus bolt-on, where the latter carries increased susceptibility and vulnerability.

STAFFING

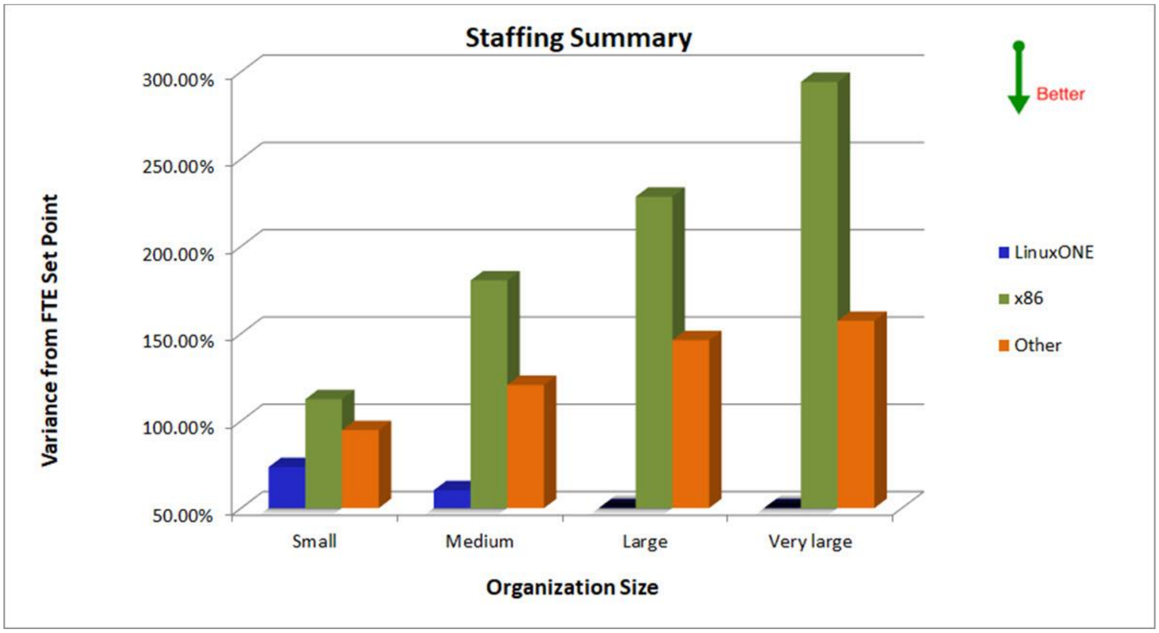
An underlying factor that shows itself in many other areas is the efficiency of the interface between the system administrator and the infrastructure. It includes software, hardware and operating system components, and the subsequent effect on staffing. As staffing efficiency increases, the level of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

> *"We are very pleased with the LinuxONE environments! It is proving to be much more stable and problem-free than our other Linux environments. For about the same workloads, we have four full-time people on LinuxONE but need 13 full-time and two part-time people on the x86 boxes. We have more VMs now on LinuxONE because it is faster and easier to setup and configure."*
>
> CIO – Medium Manufacturer

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 broad 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.

Since different architectures have varying sets of implementation standards, it is essential to keep the rigor of those standards in mind when reviewing the staffing. The noticeably lower staffing level for the IBM LinuxONE deployment and use is directly attributable to the integrated nature of the operational stack. This is of particular note as an organization increases in size or if an organization is on the path to a cloud service delivery model.

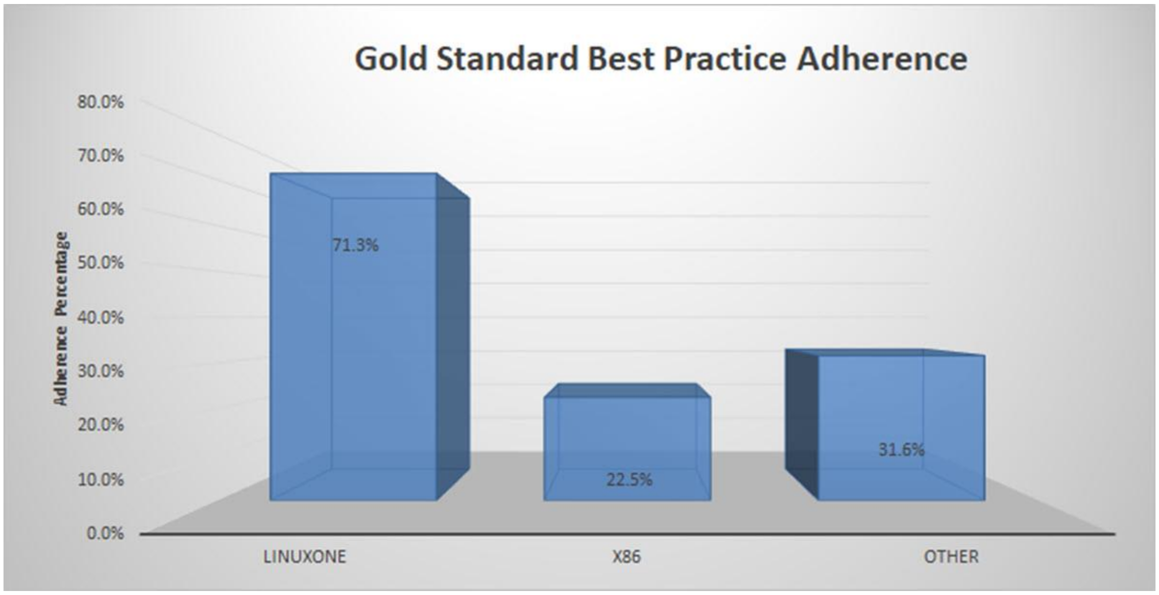


Based on the detailed customer reports, deployment on LinuxONE requires 61.07-88.05% less operational staff time than other alternatives.

The efficiency inherent in the recorded production behavior of the operational staff shows that the load on individual people is less. From an industrial psychology point of view, it’s crucial that the individual can perform their job with a minimum number of context switches. This lowers the incidence of errors due to confusion and means that the expertise of the personnel can be applied to following best practices.

Since best practices in the respective areas of system administration, security, and operations are a significant factor when limiting risk, the time to perform proactive evaluation and fully implement best practices is a considerable safety factor for organizations. There is nothing to note a disparity of professionalism or skill in different organization’s personnel. However, inefficiency in the tools provided for a job is highlighted by a lower level of best practice implementation. People do not have enough time to not only complete what they need to do on a day-to-day basis but do the proactive and strategic actions that allow them to avoid problems rather than merely fighting fires.

An analysis of best practice adherence among the reporting organizations and sites shows that there is a compelling pattern developing along architectural lines. The efficiencies in toolsets, integration in the architecture and software stack, and other components combined to build a telling picture.



The net effect is that the LinuxONE deployments are more than *3.1 times* likely to have followed full gold standard best practices than other architectural deployments. This represents a significant risk reduction factor and has a ripple effect throughout the rest of the operational activity.

INCURSION COSTS

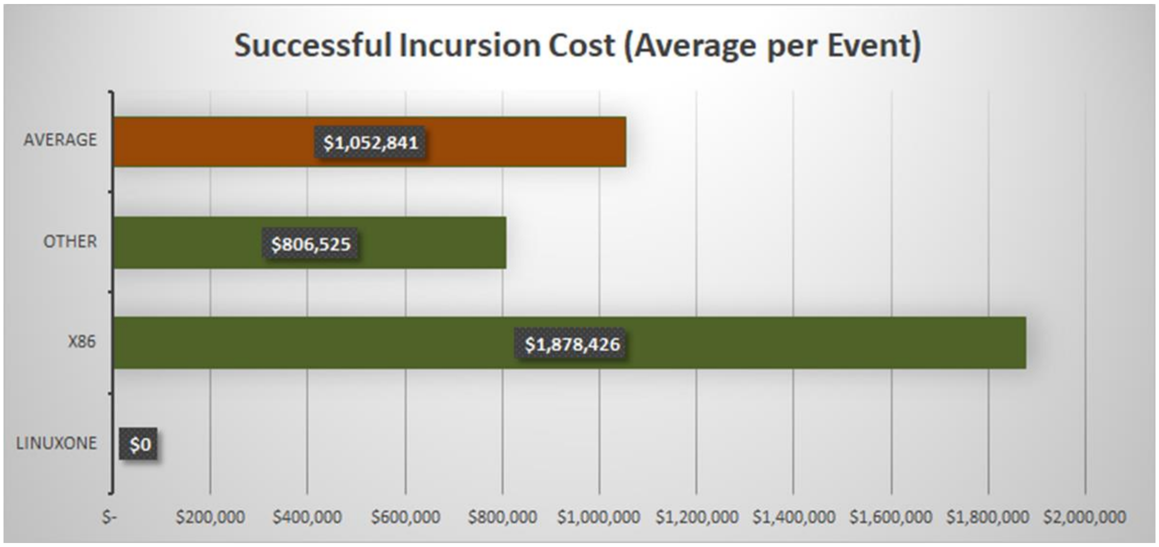
Another factor that expresses itself in cost is a contribution that many only consider in the security arena. However, the costs are a business issue and should be evaluated by those that examine business cases. This cost is centered around the price of incursions.

An 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 primary IT spheres: I/O, network access, memory management and overall regular 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 significant damage.

Examining the average cost per successful incursion shows a significant financial impact based on architecture. The data summarized in the following chart excludes only those security violations that result from stolen password usage.



The average cost of an incursion is increasing, and the rate of that increase is accelerating. Expenses associated with incursions are more than 650% higher than they were ten years ago. 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 LinuxONE deployments demonstrates the synergy of all of these factors.

COST OF RISK

The increasing damage to business from cyber criminals has given rise to specialized cyber insurance policies. This burgeoning market is on a constant journey to capture enough data to accurately rate the risk and exposure of their clients in their business endeavors.

In addition to a complex mixture of required protocols and components, most insurance firms offering this type of policy need their clients to provide substantial set-asides, funds held inactive, to fund a reasonable response to successful incursions.

It is extremely notable that, due to the low likelihood of security incursions on the LinuxONE systems, the financial set-aside for those systems is as little as 3.2% of that which is required for customers running on alternative platforms and solutions. Compared to an industry average of 14.7% percent, that represents a significant business advantage.

This provides a clear, concise, and cross-industry perspective of financial exposure and projected costs when doing business in cyberspace from a group whose business is to calculate risk and exposure. The impact of that set-aside is only a harbinger of the total picture.

Executives faced with these requirements are learning to look more to total cost of ownership rather than being concerned only with the acquisition expenses. Or as one CEO sent an email recently, “Acquisition is once, set-asides can last forever. And I certainly don’t want to have $7.5 million held out of my operating budget for one system forever.”

This is definitely thought-provoking for executives and should be considered in any business case evaluation of platform selection or deployment.

CONCLUSION

> *A federal appeals court in Washington, D.C. has ruled that consumers may sue companies that fail to safeguard their personal data. EPIC filed an amicus brief in the case, in support of the consumers, arguing that if "companies fail to invest in reasonable security measures, then consumers will continue to face harm from data breaches." The appeals court agreed with EPIC that the lower court was wrong to dismiss the case.*

Electronic Privacy Information Center, DC Circuit Upholds Right of Data Breach Victims to Seek Legal Relief, August 1, 2017

The current release of the LinuxONE 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.

Companies that are actively conducting commerce in cyberspace and those that have moved to a cloud model have an immense sensitivity when it comes to cybersecurity. The security surrounding an organization’s data and other intellectual capital is quickly becoming a primary focus, as our world becomes more and more connected. With this increased integration comes more considerable challenges, as organizations struggle to protect their market advantage and finances. IBM has a long history of asset protection and highly secured deployments, and with that maturity comes features that have been built into the LinuxONE solution that are absent from other solutions.

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

Quick Summary

Category	Commentary	Quick Byte
Time to Market	Getting a system up and running with LinuxONE averages as little as *35.3% of the time* required by other platforms.	Get your systems up-and-running faster.
Flexibility	The reported, average resilience of the LinuxONE implementations is as much as *7.41 times* of the other options.	More easily handle unexpected activity spikes.
Flexibility	Customers running LinuxONE realize up to *2 times* more consistency in the delivery of end-user requests than recorded on other platforms.	Help improve customer experience by consistent delivery.
Total Cost of Ownership	The TCO for LinuxONE implementations is lower by as much as *82.12%* than for those of other platforms.	Greatly reduce TCO compared with competitors.

Category	Commentary	Quick Byte
Total Cost of Information	LinuxONE implementations show as much as *92.04% lower* TCI over a wide range of organization sizes.	Decrease costs of working with information.
Staff	Fewer FTE are required to run LinuxONE systems than other architectures by *61.07-88.05%*.	Do more with fewer staff resources.
Risk and Costs	Financial set-asides required by cyber insurance firms are as little as *3.2%* for LinuxONE implementations compared to other architectural choices.	Reduce required set-aside funds.
Risk	SIL risk profiling sets the LinuxONE platform risk rating at less than *1/20* of any of the alternative solutions.	Significantly reduce security risks.
Security Effectiveness	Based on initial installations, the foundation LinuxONE security solution provides as much as 15.*74 times* the interception level of alternative platform solutions.	Experience the most secure application environments with an integrated approach.
Security Effectiveness	LinuxONE customers report harmful incursion rates that are *less than 0.01% per 1000* deployed applications compared to other architecture choices.	Deploy a base security platform that's more effective than the competition.
Staff	LinuxONE implementations are more than *3.1 times* likely to have followed full gold standard best practices than other architectural deployments.	Free up time and resources to drive innovation.

The shifting nature of digital business is 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, significant architectures such as x86, IBM's LinuxONE platform, and other products were compared.

The overall finding of the analysis was that the industry is experiencing a resounding change in the considerations that businesses will incorporate into their choice of computer architecture.

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 7,600 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 industry 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 538 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 16M models annually in support of both ongoing subscription customers and ad hoc inquiries.

METHODOLOGY NOTES

In order to understand the impact of LinuxONE 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, 13,041,692 environmental setups were observed, recorded and analyzed to substantiate the findings. Customer experience was obtained to match against the deployment data. Over 8.1M 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 (24.17%), distribution (11.38%), healthcare (7.56%), retail (14.00%), financial (21.91%), public sector (7.61%), communications (11.47%) and a miscellaneous group (1.89%).

The geographies are also well represented with North America providing 41.38% of the reporting organizations, South and Central America 10.61%, Europe 23.68%, Pacific Rim and Asia 21.23%, Africa 3.04%, and those organizations that do not fit into those geographic divisions reporting 0.07% 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

IBM, IBM LinuxONE, LinuxONE, IBM Z, and z Systems are trademarks or registered trademarks of International Business Machines Corporation in the United States of America and other countries.

Other company, product and service names may be trademarks or service marks of others.

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