International Journal of Advanced Science and Technology
Volume 9, August, 2009

Model of Business Service Management with Security Approach

[1]Feruza Sattarova Y., [2]Sattarov Shavkat Y., [3]Tadjibayev Furkhat A.
and [4]Tai-hoon Kim

[1,4]Hannam University, Multimedia Engineering
[2]Tashkent Financial Institute, Bank and Credit
[3]Tashkent University of Information Technology, Economy and Management
mymail6585@gmail.com[1], taihoonn@empal.com[4]

Abstract

In this paper a structure of business service management integrated with security management is offered. Our BSM model with security approach is the hierarchy of data management in any growing business. It creates a logical flow of data from its inception into the organization through the management levels. Thus, allowing for proactive business decisions to be made on a consistent basis. The end result is an increase in both corporate flexibility and profitability. It encompasses the process and use of Customer Data Management, Customer Relationship Management, Enterprise Resource Planning and Business Insurance all supported by a robust Service Desk.

Information is an essential resource for all businesses today and is the key to growth and success. However, we need to ensure that the information held on our IT systems is secure. The impact of a security breach may be far greater than we would expect. The loss of sensitive or critical information directly may not only affect our competitiveness and cash flow but also damage our reputation - something which may have taken us years to establish and which may be impossible to restore.

In our paper we introduce a structure of Business Service Management (BSM) with security approach offering an advanced model of integrated secure BSM model.

Keywords: *Secure Business, Business Service Management, Steps to BSM*

1. Introduction

Business Service Management (BSM) is not a product or a technology. We cannot buy BSM, and it does not come out of any box. Still, one vendor might proudly proclaim, “BSM is software that essentially forms a dynamic link between business- oriented IT services and the Information Technologies (IT) infrastructure components that support those services.” This contradicts one of the original developers of the term, who likes to say that BSM is a “mindset, not a product set.” However, that hasn’t stopped many vendors from jumping on the BSM product bandwagon. It also hasn’t stopped numerous analyst firms from weighing in either. In fact, one notable firm states that BSM is IT managers “understanding the metrics their business users employ to decide if IT is providing value, and linking these metrics and associated business services to IT infrastructure components.” [1-2] From this point of view BSM isn’t software after all—it’s metrics and component monitoring.

The reasons for BSM are many; however, the primary driver is IT commoditization. IT commoditization refers to the fact that businesses today are more and more dependent upon

IT services. As the cost for hardware and software falls, the ease with which it may be interconnected is increasing dramatically. This presents business with many alternatives to the traditional IT organization, because many businesses can simply acquire and install systems on their own that were traditionally the purview of an IT organization. In many organizations, such ad hoc business IT systems are then connected to traditional business IT systems. The result is an incredibly complicated environment that shows no signs of decreasing in complexity.

But there is a problem. The existing scattergun approach to IT security that involves organizations deploying and utilizing a range of point-based protection solutions is not good enough. It is inefficient, and often leaves security holes that are ripe for exploitation. Small and medium-sized businesses aren't immune to security threats.

As more business processes move online and business users become more demanding, IT is expected to continually improve the quality and management of the services that support these business activities. As business dependence on IT increases, so does the need for IT to be accountable, meaning IT must understand how business evaluates the services IT provides. Service must be measurable and business priorities and user success must be the ultimate arbiters of quality. To ensure accountability and shared goals, both IT and business stakeholders need visibility into the quality of services IT provides.

In this work we try to work out and implement the security activity in seven steps with security approach. Traditionally, the focus of IT has been on operations — on managing applications and services in the most efficient manner at the least cost. Today, this focus is proving far too narrow. IT concerns are not necessarily the concerns of the business; and the language that IT uses to describe its concerns does not translate well to the business side of the organization. This only widens the gap between IT and the business — preventing the alignment that’s required for IT to help the business execute its strategic initiatives.

Business and communication over the Internet offer tremendous market potential in today's highly interlinked world. The Internet is an ideal channel for electronic businesses offering an inexpensive, flexible, and efficient way for entities to trade and communicate with each other. For an organization to succeed in this new economy the level of security is crucial in this very large but albeit a dangerous network. This document focuses on Security auditing as a first step in the process to ensure that your guard is up round-the-clock and you are always one-up on those unscrupulous elements lurking in the dark corners of the web.

Security breaches or other unexpected interruptions can happen anytime to anyone - whether you are a large enterprise or a small business. That’s why it is very important to implement security precautions in business.

2. Related research

2.1. Why align business management with information technology service management?

According to research conducted by HP, 99 percent of chief executive officers (CEOs) say that information technology (IT) is essential to business competitiveness, but only 31 percent of chief information officers (CIOs) believe IT is sufficiently aligned with business objectives and strategy [3]. This disconnect is nothing new. IT has long acted as a siloed department within the larger business it serves. But as businesses increasingly look to IT to act as a strategic partner, this gap needs to be closed.

Traditionally, the focus of IT has been on operations— on managing applications and services in the most efficient manner at the least cost. Today, this focus is proving far too narrow. IT concerns are not necessarily the concerns of the business; and the language that IT

uses to describe its concerns does not translate well to the business side of the organization. This only widens the gap between IT and the business—preventing the alignment that's required for IT to help the business execute its strategic initiatives. The concept of business service management (BSM) sheds light on this problem and offers a path toward more effective IT/business alignment.

Traditional network management systems focus on measuring and monitoring the technical metrics and trends of IT applications and infrastructure. The primary users of these systems are technicians and systems administrators in the IT operations organization. Although these systems enable the IT operations team to identify problem areas from a technical point-of-view for a given piece of the infrastructure, significant gaps exist in determining the business impact of a specific problem. If a router and a server fail at the same time, these systems offer no way for the NOC operator to determine which of these is more critical or which business services have been impacted by the failure of these devices.

Additionally, newer technologies such as SOA, Virtualization, Cloud Computing, Portal Frameworks, Grid Architectures and Mash-ups within an enterprise make troubleshooting and monitoring of enterprise services very difficult. A single business process or service may be supported by a number of composite applications, all of which could be dependent on a diverse set of distributed computing and communications elements. An isolated issue anywhere in this complex web may impact one or more tasks in the business process. Traditional network management systems and technology-centric monitoring approaches are incapable of determining the business impact of an issue in such a complicated infrastructure environment.

The Information Technology Infrastructure Library (ITIL), a set of IT management frameworks and concepts, has recently identified BSM as a best practice for IT infrastructure management and operations.

IT Service Management (ITSM) is the term used to describe managing the workflow and activities within an IT organization. ITSM presents an evolving and integrated approach to managing IT services. The concept of managing by service is relatively simple—in order for the IT service provider to add value to its enterprise and consumers, the IT provider must focus on end-to-end service delivery. This requires the provider to understand the marketplace within which the consumers of its services operate. From a normal corporate or enterprise perspective, this means the IT department must understand not only its business customers and users, but also the marketplace where the enterprise offers its products. IT value arises at the boundaries between the enterprise and its marketplace. IT services provide an indirect value—the IT service facilitates the interaction of business customers and users with enterprise end-customers and end-users.

BSM is the term used to describe the strategic direction required for ITSM to be successful. BSM, simply stated, aims to manage IT investments in ways that matter most to the success of the enterprise and its marketplace. BSM also means making decisions in IT based on what is best for the enterprise. It spans all technologies and all organizational boundaries. BSM, focusing on process integration and automation, leads IT Service Management and design.

The new imperative in IT management is the ability to manage the technology infrastructure within the context of the business services that depend on it. Whether called Business Service Management (BSM) or end-to-end IT Service Management (ITSM), the goal is to understand how the health of individual components within a service's ecosystem relates to users' quality of service (QoS) and the company's business requirements. The quest for BSM can be difficult. Not only is understanding the interdependencies between system

components confusing, but battling organizational barriers to cut across internal technology silos can be formidable.

2.2. Security management in business

Information is an essential resource for all businesses today and is the key to growth and success. However, we need to ensure that the information held on our IT systems is secure. The impact of a security breach may be far greater than we would expect. The loss of sensitive or critical information directly may not only affect our competitiveness and cash flow but also damage our reputation - something which may have taken us years to establish and which may be impossible to restore.

Information also needs to be protected if you share it with other organizations. For many businesses, the Internet has replaced traditional paper-based ways of exchanging information. It can be sent and received faster, more frequently and in greater volume.

However, the Internet brings its own security issues which businesses must consider. Some of the threats posed by hackers on the Internet include:

- Gaining access to sensitive data such as price lists, catalogues and valuable intellectual property, and altering, destroying or copying it;
- Altering your website to damage your reputation or direct your customers to another site;
- Gaining access to financial information about your business or your customers, for the purposes of fraud.

Here are some more statistics on security in a business.

43% of organizations say their information security function is now part of their organizations' risk management function. (*Ernst & Young, November, 2006)*
The average loss per phishing victim jumped from $257 in 2005 to $1,244 in 2006. (*Gartner Inc., November 2006)*

1 in 3 workers jot down their computer password, undermining their security. (*Nucleus Research and KnowledgeStorm, November 2006)*
73% of computers use spam blockers. (*Arbitron/Edison Media, October 2006)*

Roughly 1 in 3 computer users has been a victim of viruses, spyware or phishing. (*Consumer Reports, September 2006)*

U.S. consumers spent $7.8 billion over the last two years for computer repairs, parts and replacements because of malware attacks. (*Consumer Reports, September 2006)*

The average cost of insider data breaches is $3.4 million per business per year. (*Ponemon Institute/ArcSight, September 2006)*

1/5 of all e-mail messages received by corporate servers are spam. (*Panda Software, September 2006)*

1 in 20 e-mails are infected with malware. (*Panda Software, September 2006)*

64% of small businesses say they've taken action to better protect customer financial information. (*VISA USA/US Chamber of Commerce, July 2006)*

72% of businesses express concern about information and/or physical security of company assets located off-premise. (*Runzheimer International, July 2006)*

Asia is the top spam-relaying continent, responsible for 42.8%. (*Sophos, June 2006)*

US users land on malicious websites about 285 million times per month by clicking on results from the five major search engines. (*McAfee Inc., May 2006)*

85% say handheld devices used in their organization should require security protection. (*FierceWireless/BluefireWireless Security, April 2006)*

68% of information security professionals at large organizations say laptops pose the biggest security risk. (*Enterprise Strategy Group, March 2006)*

Computer security threats, including viruses, worms and Trojan horses were up 48% in 2005 from the previous year. (*Sophos, January 2006)*

Phishing grew from an average of 2.99 million messages, to 5.70 million. (Symantec Internet Security Threat Report, October 2005)

People who bank online are less likely to become victims of fraud and suffer an average loss of $551 compared to $4,500 for paper and mail bankers. (Javelin Strategy & Research, December 2005)

20% of consumers terminated a relationship with a company after being notified of a security breach. (Ponemon Institute, December 2005)

Total cybercrime losses in 2005 were $130.1 million; the majority of the losses were due to viruses, unauthorized access to computer systems and theft of propriety information. (CSI/FBI Computer Crime and Security Survey, October 2005)

12% of respondents say their confidence in a company had actually increased after they were notified of a personal data security breach; 58% said a breach had decreased their sense of trust and confidence in the organization. (Ponemon Institute LLC, October 2005)

Anti-spam product and service revenues are expected to reach $1.7 billion by 2008. (IDC, July 2005)

More than 90% of internet users have changed their habits to try and reduce their exposure to spyware. (Pew Internet & American Life Project, July 2005)

Over 80% of internet users no longer open attachments from unknown sources. (Pew Internet & American Life Project, July 2005)

60% of internet users who report computer problems do not know the source. (Pew Internet & American Life Project, July 2005)

25% of internet users say they always read user agreements, privacy statements or other disclaimers before installing or downloading files from the internet. (Pew Internet & American Life Project, July 2005)

63% more computers were infested with malicious code--i.e. spyware, adware, etc.--in the first six months of 2005 than all of 2004. (McAfee, August 2005) [4].

The factors and statistics listed above are not negligible.

The existing scattergun approach to IT security that involves organizations deploying and utilizing a range of point-based protection solutions is not good enough. It is inefficient, and often leaves security holes that are ripe for exploitation. Small and medium-sized businesses aren't immune to security threats. If we use e-mail for communications, have mobile employees or remote offices, or maintain a Web presence, our business is at risk.

2.3. Business Service Management (BSM) Model

The new imperative in IT management is the ability to manage the technology infrastructure within the context of the business services that depend on it. Whether called Business Service Management (BSM) [2], [5] or end-to-end IT Service Management (ITSM), the goal is to understand how the health of individual components within a service's ecosystem relates to users' quality of service (QoS) and the company's business requirements. The quest for BSM can be difficult. Not only is understanding the interdependencies between system components confusing, but battling organizational barriers to cut across internal technology silos can be formidable.

So how does a busy IT organization begin the quest? One of the most popular best practice frameworks is the Information Technology Infrastructure Library (ITIL) [6-7], which outlines extensively what technology departments should do, but not how to do it. Several vendors offer proprietary implementation maps based on their own products, but at BSM Digest, it have been taken a vendor-neutral approach to the problem and adapted this simple seven-step framework to ease the way. In the first Inventory step the elements in the infrastructure are identified and cataloged. If we don't know what we have, we cannot manage it how appropriately. For most companies, the first step toward business service management is a thorough accounting of the assets or configuration items in their infrastructure. New innovations in automated discovery technologies are making it easier to identify and catalog elements within complex infrastructures. Many companies have opted to federate this inventory along with configuration information and basic component dependencies into a configuration management database (CMDB), one of the fundamental pillars of ITIL.

In next step the elements are instrumented properly for continuous monitoring. Once we have an inventory of all the configuration items in the environment, the next task is to make sure they are all properly instrumented for continuous monitoring. Monitoring technology has evolved dramatically from basic availability management – simple up/down notifications – to more elaborate performance management products that can track hundreds of key performance indicators for each individual system. Plus, a new generation of end-user monitoring and transaction products are making it easier than ever to understand user experience and quality of service.

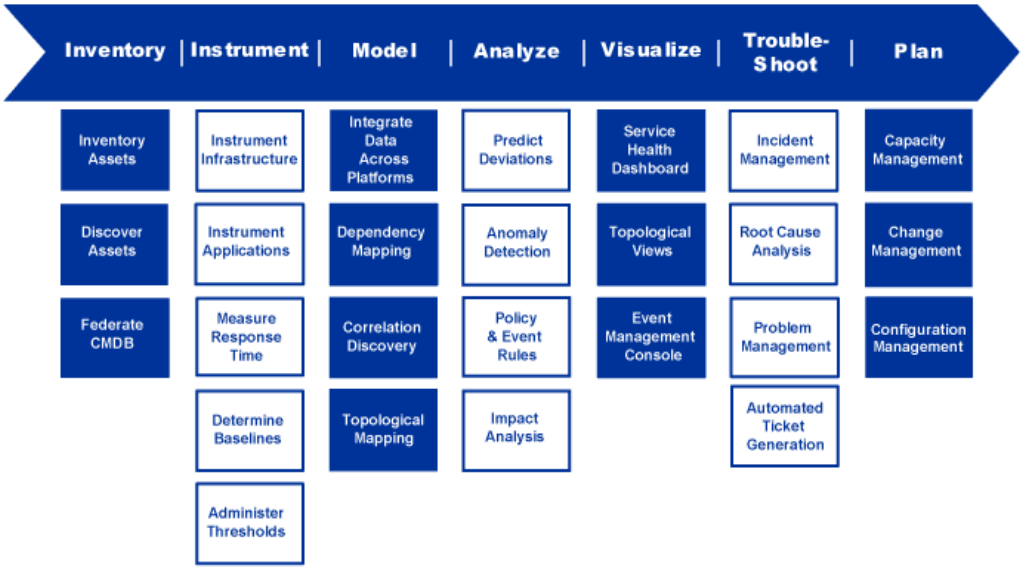

Figure 1. 7 Steps to Business Service Management [8]

Proper instrumentation requires two phases of implementation. First is the deployment of instrument applications and distribution of their monitoring agents (or the new-breed agentless monitors). Second is the active administration of baseline and threshold settings for every monitored metric on each configuration item. Traditionally administrating monitoring applications has been very time-consuming, but new BSM tools are automating many of these previously manual tasks. In third step (Modeling) services and applications are mapped to the elements that support them. Comprehensive inventory and instrumentation allows you to begin pulling together the elements of your infrastructure in ways that make sense for

managing your services. Within the modeling process, IT mangers begin to map applications to the network elements that support them and the performance dependencies between them. In the same way that a doctor analyzes multiple biologic measurements – temperature, heart rate, blood levels, cholesterol, etc. – in context to one another to assess how a patient's organs are performing and thereby diagnose his overall health, a network manager can model groups of system elements to diagnose the health of key business services. This process of modeling services is fundamental for creating service level agreements tied to business requirements. In the forth step analysis should be held. Here understanding normal behavior patterns and detecting performance anomalies is important. Analysis techniques and technologies allow IT managers to understand the normal operating behaviors of the systems and the services they support. Accurate analysis enables them to establish policies and event rules that notify them of conditions that portend service degradations. As the culmination of the Inventory, Instrumentation, and Modeling steps, effective analysis allows the timely detection of system and service anomalies and the immediate assessment of their impact on quality of service. Until recently, analysis has been a time-consuming process bottleneck for many organizations, but new automated real-time analysis technologies are streamlining this step. Whether done manually or automated with new BSM technologies, timely analysis is a critical step for successfully managing IT infrastructure within the context of critical business services. Step five gauges the environment's end-to-end status in real time. A new breed of BSM tools is emerging that finally makes it possible for CIOs to maintain real-time dashboards that track the end-to-end health of their critical business services. These applications provide easy-to-read views of configuration items and consolidated event management consoles to facilitate administrators' troubleshooting responsibilities. As infrastructure environments grow more complex, the importance of having simple user interfaces for visualizing them increases. IT operations teams and their business customers need intuitive ways to quickly assess service health and pinpoint developing problems before they impact service quality. In Troubleshooting step problems are identified and resolved quickly. When performance anomalies and service degradation occur, system and application administrators must effectively manage incidents and analyze their root causes. This goal is only achievable if the flow of incoming alerts from the monitoring infrastructure is small and qualified. While managing events has historically been a slow, hand-picking process, new innovations in dynamic thresholding and multi-variable data correlation are significantly helping increase the accuracy and manageability of system alerts. Once the true problems are identified, system administrators still need the ability to rapidly drill-down to the source of the problem and trigger the appropriate remedial actions. Root-cause analysis remains the biggest challenge of Incident Management. Fortunately, vendors are now introducing tools that offer accurate root-cause analysis capabilities via integrated end-to-end fault and performance management, advanced analytics, and rule-based techniques.

Effective reduction in Mean-Time-To-Repair (MTTR) relies on accurate problem description, routing to the appropriate technical support tier group, and prompt resolution. Building a known incident database based on past experience and letting administrators consult these known incidents during troubleshooting can drastically reduce MTTR. This requires diligent incident post-mortem sessions where subject-matter experts record the symptoms of the problem, spell out its root-cause, and explain how it was resolved. A tight integration with trouble ticketing systems using intelligent filtering and routing capabilities is also a contributor to efficient incident and problem management.

With each innovation, the industry is moving closer than ever to its long-term objective of automating problem diagnosis and trouble ticket generation and its vision of autonomic, self-healing systems and automated service provisioning.

In the last step enhancement of IT and business objective synchronization over time is performed. Ultimately, the goal of every IT organization is to minimize the number of problems affecting systems and services, not just addressing incidents in an effective manner. There are two ways to meet this objective: proactive monitoring and proactive capacity, change, and configuration management. Effective planning is the key to achieving both.

Proactive monitoring uses short and medium term forecasting capabilities to identify performance degradations before they become incidents, and then promptly alert on them. System and service behavior modeling technologies typically include predictive engines that allow you to forecast the occurrence of a problem with a high level of accuracy. However, this technology will only be efficient if the back-end support processes are capable of analyzing and reacting fast enough.

Proactive capacity management refers to the ability to accurately analyze the infrastructure's current load, identify trends, and take the necessary configuration management steps to increase computing capacity on over-loaded systems or implement efficient load-balancing.

This model can be improved by adding some security points and precautions. It will grant the existing model a higher reliability.

3. Proposed model of business service management

In the model we propose, we add security management to the existing BSM model. The model we propose unifies business management, IT governance and security management. It provides an effective service approach. Our proposed model gives opportunity to manage change and configuration dynamically to any part of the infrastructure, applications, and client systems without disrupting service. This assures a seamless service life cycle. It also offers a strengthen alignment with business goals.

Our integrated BSM model with security approach provides with advantages listed below:

1. Ensure conforming throughout the service life style.
2. Encompasses the process and use of Customer Data Management, Customer Relationship Management, Enterprise Resource Planning, Security Management and Business Insurance all supported by a robust Service Desk
3. Present information on exactly how well IT services are supporting business-critical processes.
4. Helps IT address service problems that span multiple components, as opposed to one group "pointing the finger" at another when users experience problems. Reduce mean time to repair (MTTR) service problems in line with understanding the dependencies among business processes, IT services, and underlying IT infrastructure.
5. Makes the technology easier to manage in relation to policy, and makes costs easier to calculate.
6. Manage change and configuration dynamically to any part of the infrastructure, applications, and client systems without disrupting service. This assures a seamless service life cycle.
7. And of course, insured business.

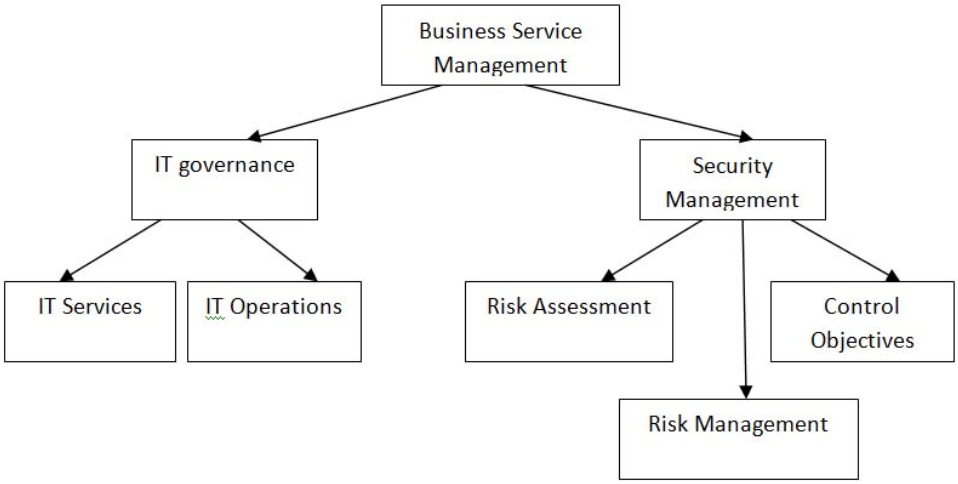

Figure 2. Integrated Business Service Management with Security Approach

In our proposed model in the second step of business service management we added an issue of identifying the hazards. It is very important, because if we instrument infrastructure, applications, measure time, determine baselines, administer baselines, but do not identify possible hazards we are at a great risk. To identify hazards first we must do these:

1. We must have state of knowledge about the risk and treatment options; consider acceptability in terms of both individual and societal tolerance.
2. Determine how big and high is the risk as a function of probability and consequence.
3. Analyze cost of fixes. It can be done by comparing levels of risk found in analysis with previously established criteria, examining costs and benefits of control for most serious risks, studying economic impacts and finding options for response and recovery.
4. Checking the availability and suitability of fixes – deciding whether risk can be accepted. Here we can decide to accept, reduce or transfer the risk.

In the step of analyzing along with predicting deviations, anomaly detection, analyzing policy events and rules and impact analysis evaluating the risks is also added.

Analysis step is a critical step for successfully managing IT infrastructure. So in this step it is also important to evaluate the risks knowing the hazards. Security is good when the threat is avoided. Troubleshooting the risks is very important, but avoiding them long before they occur is much more effective, that helps to save time and resources. So in the fifth step we propose to hold a risk avoidance management. When the security threats occur it will be managed in troubleshooting stage and it is the final step in troubleshooting after identifying the incident, analyzing the root cause of the problem. And finally, at the last step of building BSM when planning the business it is very important to secure your business.

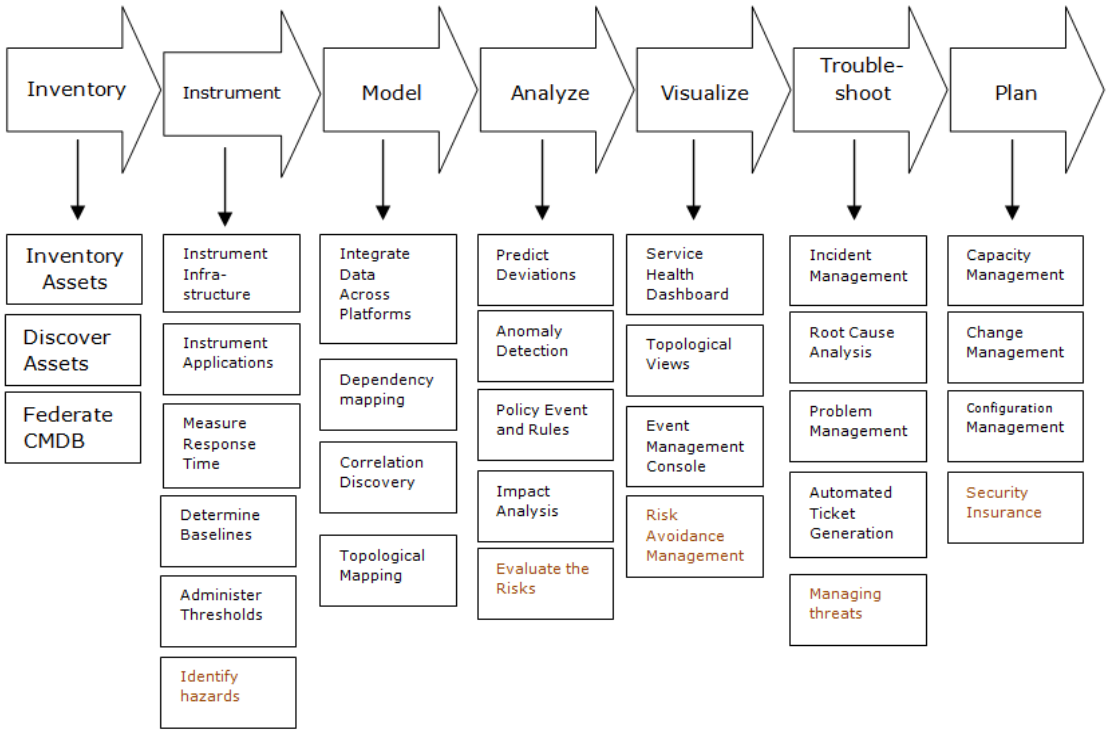

Figure 3. Seven steps to BSM with security approach

4. Conclusion

As a conclusion we will mention that, our integrated BSM model with security approach is the hierarchy of data management in any growing business. It creates a logical flow of data from its inception into the organization through the management levels. Thus, allowing for proactive business decisions to be made on a consistent basis. The end result is an increase in both corporate flexibility and profitability. It encompasses the process and use of Customer Data Management, Customer Relationship Management, Enterprise Resource Planning and Business Insurance all supported by a robust Service Desk.

The disadvantage of this model can be its being complicated to manage, but it gives an effective solution to reduce time and resources, and reliability.

Information is an essential resource for all businesses today and is the key to growth and success. However, we need to ensure that the information held on our IT systems is secure. The impact of a security breach may be far greater than we would expect. The loss of sensitive or critical information directly may not only affect our competitiveness and cash flow but also damage our reputation - something which may have taken us years to establish and which may be impossible to restore.

Security breaches or other unexpected interruptions can happen anytime to anyone - whether you are a large enterprise or a small business. That’s why it is very important to implement security precautions in business.

In our paper we proposed a model of BSM with the concept of securing and insuring the business.

Acknowledgements

This work was supported by the Security Engineering Research Center, granted by the Korean Ministry of Knowledge Economy.

References

[1] Hank Marquis, Founder and Director, NABSM, Instructor "Business Service Management: What It Is and Why You Should Care" Global Knowledge Training LLC 2008

[2] Hank Marquis "Business Service Management: What It Is and Why You Should Care" Global Knowledge

[3] "How to transform IT into a strategic business partner" white paper, 2007 Hewlett-Packard Development Company, L.P

[4] Cyber Security Statistics, 2007;

http://www.entrepreneur.com/encyclopedia/businessstatistics/article82010.html

[5] Sarah Meyer "Business Service Management Links IT Services to Business Goals "CA SOLUTIONS MARKETING, January 2008

[6] http://www.itil.co.uk/

[7] http://en.wikipedia.org/wiki/ITIL

[8] Katherine Chalmers The 7 Steps to Business Service Management, May 2006 http://www.bsmdigest.com/