Security Management
2I1506

Assignment 2

Symantec
Managed Security Services

Group 5
Zoupas Alkiviadis (PL)
Kocaer Kerem (SD)
Hibner Allan
Islam Mohammed Hedayetul
Zhao Ying
Khan Mohammed Mahfuzur Rahman
Loizou Savvas
Wijk Tobias
Saeed Tariq
Zoran Milinkovic

Symantec Managed Security Services

Introduction

Identifying Symantec's KPIs and conducting a risk analysis based on them is a complicated task which would normally require workshops conducted by a special team and participated by managers from different areas. This report aims to cover the most important KPIs measuring the MSS Service, and propose mitigation approaches to the most important risks that we have identified threatening these KPIs. The identification of KPIs has been based on research about Symantec and MSS in general, and has been done with the following steps: First, we have researched the strategic objectives, value drivers and stakeholder needs of Symantec. Then, we have identified seven Corporate Goals covering the things identified in step 1. Finally, from these goals, we derived the KPIs linked to the goals. The next phase was to identify risks that exist for Symantec that could affect the previously found KPIs and values, and to offer mitigation plans for them. We have also prioritized five of the risks as the most important ones that need to be taken care of first. All these phases have been conducted by group workshops, where individual research reports have been presented and discussed.

Corporate Goals

The seven corporate goals of Symantec, related to or affecting the MSS service, are presented in this section.

Leader in MSS to Enterprises

Symantec is a world-leading organization concerning providing software, solution and service to help its customers to protect their information security in their organizations. Symantec's MSS product allows its customers to outsource their security management cost-effectively. The main customer group of MSS in Symantec is large enterprise, since MSS is mainly dealing with the entire security management, monitoring and response needs in the whole organization. It can be profitable if the company targets big enterprises as its main customers because MSS is customized according to the infrastructure of big enterprises and it is also more cost effective to provide a large scale service. The more customers like large enterprises Symantec has, the more profit it can earn. What size of entity can be a large enterprise? According to the Commission of European Community, the entities which have more than 250 occupied persons and which have either an annual turnover over 50 million Euros, or an annual balance sheet total exceeding 43 million Euros can be considered as large enterprises.

Now Symantec has already achieved a lot in trying to become leader in MSS to enterprises. According to Vendor Rating by Gartner, Symantec's product MSS is rated as positive. That means the company demonstrates strength in specific areas, but is largely opportunistic. Its potential customers will consider this vendor as a priory alternative. After acquiring Riptech in 2003, Symantec has kept Riptech's reputation for service delivery. Symantec also acquired company @stake, so it can offer a better vulnerability/threat alerting capability and professional services to round out its managed security service offering. Since, in this product category, there is only one direct competitor Tivoli, Symantec has great opportunity to expand the market and gain leadership in this area. Symantec can benefit a lot from being the leader in MSS to enterprise, such as increasing income, owning a large amount of stable customers, producing cost-effective, well-known MSS provider in the world (even the whole company can become famous).

"State of the art" in MSS

"State of the art" in MSS means that Symantec wants to provide the best managed security service to its customers. Currently, Symantec has the most advanced technology available and an experienced team of analysts ready to respond to threats. It has also built and refined the most sophisticated advanced-warning system in the security industry. Symantec pioneered integrated security, by combining advanced virus protection, firewall, spam/content filtering, intrusion detection, and vulnerability assessment into unified, interoperable solutions. Symantec combines world-class enterprise administration tools with their industry-leading security products and services in order to achieve best information management. To reach the state of art in MSS, Symantec still needs to be innovative in creating new products and services as well as timely applying them to the market. It will benefit from the state of art goal in terms of increasing product quality,

reducing costs, building up product reputation, and ultimately become more competitive.

Financial Growth

It is the estimation of the amount of growth yet to occur in the company. Every company's mail goal is to increase financial growth and to the excess of revenues. It is obvious that profit is the main target for every company, since it enables more investments and it gives employees better wages. Consequently, Symantec should look for as more profits as possible compliance, with a complete respect of fairness.

Extend services/products

Symantec's understanding of the market and its flexibility is reflected in the diversity of its business areas. With more diverse portfolio of services, Symantec can attract more clients. The area of computer security is constantly evolving. For that Symantec should extend its services and build new products in advance that counter these new threats. By keeping this, Symantec proves to the clients that it struggles to make its products and services better. Of course this growth will give a certain amount of assets. With extending services/product Symantec should provide the latest technology to its clients in security field where every minute a new threat is evolving. The customers of MSS come in all sizes and have different needs and equipment. In order to be able to service those who are in need of MSS, Symantec needs to be able to extend its service to different hardware, geographical layouts, cultures and security needs.

Customer Satisfaction

Symantec has as a goal to improve its relationship with its clients. The trustworthiness of the company must be preserved at all costs. Trust can be won by providing good customer services. Symantec should respect them and constantly try to keep them satisfied. The focus should be on providing an exceptional customer support. In order to keep its clientele satisfied, Symantec should be able to handle them in the most successful way in the smallest time period. In order to inspire trust to the customers and provide consistently good service, Symantec needs to apply standards for its internal work. For customer satisfaction Symantec should provide quality of service and speed of reaction and anticipation. New threats and new kind of threats appear all the time. Symantec has the capability to respond timely to counter the new threat and distribute solutions in time to customers. An indicator of performance in this area is the number of complaints from customers due to inadequate service over a chosen interval.

Protect Reputation

The reputation is one of the major business factors. With a good reputation, a company may gain more customers and make better profit. Symantec has a reputation as one of the most trusted security service provider. Symantec has earned its reputation providing high quality services to some of biggest world companies, and providing high quality products to end users. Today, a lot of companies don't believe in outsourcing and use their own methods to protect their systems. The corporate goal is to protect and augment Symantec's reputation providing and increasing high quality services. Any damage on customer's side will affect reputation and may lead to a decrease in the number of customers and loss of money. Educating and training people in the security area, as well as hiring people with security certificates increase Symantec's reputation. Symantec also needs to follow all trends and standards, and applies certificates regarding to the security area. With high knowledge of security and certificates that Symantec has gained, trust and reputation to Symantec will be increased.

Have, keep, maintain, satisfy the best security employees

To be able to remain as the leader in MSS services, Symantec has to retain the 'top' security employees that have high competence and experience. Symantec should pay attention to the quality of people it hires, by performing thorough interviews and background checks. It should also do whatever is necessary to keep these employees the bests in the business, by offering continuous education with trainings. Moreover, it should keep these employees satisfied so as to avoid employee turnover.

Key Performance Indicators

The KPIs that we have identified are explained below.

Percentage of MSS market share

The reports show that Symantec's market share of the worldwide security industry increased from 14.7 percent in 2000 to 21 percent in 2001, leading the list of the world's top 21 security software vendors. The growth of Symantec's market share was underscored by the expansion of its lead over the second-place company from 1 percentage point in 2000 to seven percentage points in 2001.

Symantec's Managed Security Services business continues to expand according to reports (dated Jan 15, 2003) with 95 new or extended deals in the United States. Companies from different sectors of the market, from government to health care and insurance, have showed their wiliness to buy the product from Symantec to boost their security services. Moreover according to reports(dated March 30,2005), Symantec showing its confidence has added Monitored and Managed IPS(Intrusion Prevention System) to increase its lead from its closest rival in the industry. The current perspective being to be flexible and to improve its sales to capture a greater audience of the agnostic approach to managed security services of its customer. This will help to provide differentiation between its rivals and affect its competitors like VeriSign and ISS.

As a Key Performance Indicator according to the above, the performance of Symantec has increased with time as it has managed to increase revenue for the company. Moreover it has been able to attract new companies from different sectors to take Managed Security Services from Symantec. Also with success of the services, it has the confidence to add more features (such as Intrusion Prevention System) to the basic services of MSS thus adding value to its services.

Percentage of Conformance to International Standards

Several standards apply to different entities and processes. We can divide these standards into two categories: those related to the experience of employees and the standards for MSS.

Experience of Employees:
Symantec Professionals are highly experienced. They are certified by the BS7799 standard. This certification ensures translating Symantec's unsurpassed global intelligence into effective network security for its clients.
Analysts and engineers in Symantec are familiar with a broad range of security issues which are required in almost all industries which include energy, finance, insurance, and health care etc. Symantec understand the unique challenges that can arise in either case, and knows the best practices and certification standards needed to establish competence needed for various industries across the world.

Standards for Managed Security Services:
Symantec Managed Security Services leverages its exclusive competence over global intelligence to offer fast and accurate analysis of security data to protect its customers. Symantec's Security Operations Centers have been fully audited and certified by independent third parties to meet industry leading standards including BS7799 certification and SAS70 Type II audits.

As a key performance Indicator, this factor is important since it proves that Symantec is informed on all Security issues and keeps informing itself and its employes by requesting certification. It also proves that Symantec is a healthy and trustworthy organization. A very important thing especialy in the Security business relates to how a customer gets informed about a potential or an imminent threat. This aspect relates to how Symantec has set standards to inform its customers according to its classification of threat. A wrong mode of notification will severely hamper its business.

Income/Expenses for mss services

This KPI is the value you get when income is divided by expenses. For the MSS-services, this KPI should include direct incomes from customers buying MSS services, meaning the price they pay for said services. The expenses are a bit more complicated, since they include: share of cost for support, machines, salaries, office-space, extra costs generated by incidents, insurance of part of risks for that customer and so on. This can be used for each customer or for the whole company, and is a good indicator on how profitable the MSS-services are. Especially used customer-wise it can be used to fine tune business, since we can identify less profitable

customers and see what we can do to increase the income/expense ratio for that customer. It is directly related to the “Financial Growth” Goal of our company.

Churn rate

For this KPI, churn rate is used on the customer base. It is a measure for the number of contractual customers that are leaving Symantec for a certain period of time divided by the average total customers over that period of time. It is an indicator on customer dissatisfaction or satisfaction. In a business you want as low churn rate as possible for example a few percent. If you have a high churn rate it means that customers are leaving the business and many new customers are acquired but none of them stay loyal very long. Therefore you want a low churn rate as possible and hence a stable customer base. In a business like Symantec’s, you can prevent high churn rate with contractual binding periods, use of proprietary technology or their unique business models and solutions. Churn rate could be a good metric measure for their prosperity and position in the market.

Response Time

Response time is a critical key indicator in providing security services. It measures a time period starting from when a vulnerability is found to when Symantec responses with a protection solution for the vulnerability. Many companies depend on this factor, especially companies with a lot of employees, where the risk that a vulnerability may be exploited is bigger, since there are always some people that are not skilful in working on computers.

Uptime 99.99%

This KPI shows (in percentage) how long Symantec security system is up during one year. Symantec needs to have a high uptime of the security system to provide security support to customers. There are some factors that may decrease system's uptime, like DDoS attack or malfunctions of hardware, to all Symantec's security operating centers (SOC). Another example that may cause in decreasing uptime is an ISP network downtime, where Symantec does not have influence. For keeping a high percent of system uptime, Symantec has created redundant systems with many SOCs and sensors that can take over a work of and work as an affected part of the system.

Improvement in IT Security Training

To focus on organizational security, improvement of IT security training is a must. Leading companies like Symantec try to maintain the KPIs. IT security staff need to understand in-depth training for technical person about product and systems where non-technical staffs needs to know the general understanding of what is in place. It helps to stretch the security technology investment by growing and keeping good people. Develop a good training program as an effective recruiting and retention tool,

- identify and evaluate the training the security professionals need,
- help to get good technical training for people to optimize deployment and management of your security tools,
- Strengthen organization's security stance with vendor-neutral security solutions teaching,
- Use certification programs to validate staff's security expertise and take corporate information protection to the next level with employee security awareness education.

Percentage of Employee Turnover

The employee turnover is a good tool to represent the percentage of employees which leave the company for another one (compared to the total number of employees). The continuity of a business company is really reliant on the solidity of the workforce. A high staff turnover might create a bad atmosphere in a company, thus affecting the work’s quality.

Media coverage good/bad percentage

Media is nowadays becoming more and more close to people; people are getting in touch with media everyday, and they mostly get information from media such as newspaper, TV, Radio, Internet and so on. Good media coverage will apparently influence a company’s reputation. And if a company has high percentage media coverage from the positive side, people will trust this company and willing to buy its product or service. To the opposite, if a company has high percentage media coverage from the negative side, the company’s reputation is also negative affected, and people will not consider buying products from this company. For example, if one day media reports to public that Symantec’s security system broke down

because of a virus or hacker, Symantec's reputation and market will be highly negative affected; customer may not want to buy Symantec's product in a certain period. So we can see that media coverage percentage from both positive and negative side is a very important KPI to all the companies. Symantec has a good reputation globally, and it has won lots of favorite media coverage from positive side. In order to keep its high reputation, Symantec still need to avoid bad news in the media and win more good news about Symantec.

Percentage of False Positives

A false positive occurs when a product incorrectly reports that it has found a positive result where none really exists. If it products too many false positives, then clients will lose confidence that products have no capability to protect the network. Ultimately, the clients are buying protection from intrusions. This KPI is a counter of how often successful intrusions are reported to them over a period. Symantec should keep improving constantly to improve their response. For a decrease in false positives Symantec should improve development life cycle of their products. Strong internal research is essential to keep abreast knowledge about threats. Further, constant quality can only be assured by applying security management standards in Symantec's daily work.

This KPI is directly related to the "Protect Reputation", "Financial Growth" and "Customer Satisfaction" Strategic Objectives of our company. Due to too many false positives, Symantec will lose their assets in the form of its clients. This lose can directly influence our company's reputation, financial gain and customer satisfaction.

Successful Intrusion Attacks Attempts/ Total Intrusion Attacks Attempts

In order to be able to evaluate security that is established in a specific protected part, values such as the above KPI are highly necessary. The specific KPI indicates the percentage of the Intrusion attempts that proved to be successful, comparing the total number of intrusion attempts. The metric takes place by the end of every year and measures the total number of attacks in a specific protected part. Then it separates the number of the attacks that actually had a minor impact, and results a percentage of attacks that proved to be effective. Effective MSS services are able to show the specific KPI by the end of every year with even lower values if not zero.

Successful Disputes Percentage

Percentage of successfully resolved MSS disputes. This KPI is computed by dividing the disputes that are associated with the Service Level Agreement of Managed Security Services and were resolved to our benefit by the number of disputes that have arisen from MSS and we have to face each year. This KPI illustrates how well our legal department is operating in the MSS contract section. It is directly related to the "Financial Growth" and "Protect Reputation" Strategic Objectives of our company. Since outsourcing MSS is a high risk transaction we should protect ourselves with the right SLAs. Most of the disputes today end up with a fee for the side that loses them. This fee can first of all greatly influence our company's financial gain and second have a bad influence on our reputation. We should take all of the necessary steps to create tailored made SLAs for each of our clients. Our SLAs should work to the partnerships benefit by clearly covering all problematic areas of this kind of cooperation. Therefore we will minimize the number of disputes that arise by making our contracts more concrete and detailed.

Risks

Our risk analysis is focused on operative risks, and includes some business strategic risks. Below is, for each of them, a description, an estimation of its qualitative severity and a mitigation approach.

Market Trends Change (Fluctuations)

Market Trends change includes customer demand change, new technology or new operating system appearance, the foreign exchange fluctuations, the introduction of competitive products, seasonality and so on. All the above factors can cause fluctuations in company's sales. It is a dynamic risk which means the company can benefit from this risk if it deals well with it. If the market trend changes, Symantec can still take proper actions accordingly in order to stay competitive and profitable. According to an interview with Jonah Paransky, senior manager of security product management for Symantec Managed Security Services (MSS), the MSS market shows significant promise. As In-Stat puts the market at nearly $5 billion by 2006 and Garnter predicted that about 60% enterprises would outsource at least one perimeter technology by 2005. Yankee Group believes that enterprises might turn to MSS providers to provide most of their security solutions in the next five years and will outsource approximately 90% of their solutions by the year 2010.

Symantec predicts that there will be continued growth and penetration of managed security services in large enterprise market, and more enterprise organizations look for partners which can effectively integrate into their environments. Enterprise organizations will also focus on looking to partners that can help them cope with the rapidly changing threat landscape. At last, enterprises will focus on requiring comprehensive global threat intelligence gathering and sharing. So we can see that currently the market trend of MSS is optimistic.

The KPIs that are influenced directly from this risk are:
- Percentage of MSS market
- Percentage of standards conformance
- Income/Expenses for MSS services

First, if the markets demand increases, the Symantec MSS market percentage may increase if the customers think their product is the best. So in this point of view, market trend change will influence the percentage of MSS market share. Second, percentage of standards conformance will also be affected by market trends because when, for example, there is a new operating system with different standards in security requirements coming to the market, it might cause less standards conformance. According to this KPI, we can predict the risk, or we may accept the risk and find a way to solve it. Finally, the market trends will influence the sales, production costs, advertising costs and other expenses. For example, if there is a new technology, the company product might become outdated, therefore negatively affecting company's income.

Severity

This risk is medium because market trend change is sometimes unavoidable, if a company can predict it and take actions to meet the new market trend, the company will keep stable or even more competitive.

Mitigation

From a business perspective, to mitigate the risk resulted from the changing MSS market trends; we will need to try to anticipate the future market dynamics as much as possible and to remain flexible in our production as well as service. It is very important to understand our target customers' needs and expectations by certain mechanisms such as market research, surveys, company visits etc. We should have a backup plan for a possible future market shrink, for example, we can try to retarget our customer group or offer a new attractive product and service. When the market's transition between new releases of operating systems occurs, we should have a quick and timely response mechanism in order to meet the new requirements from the new systems as well as from the customers. As for foreign currency exchange rates fluctuation, we can use certain derivative financial instruments to manage this risk.

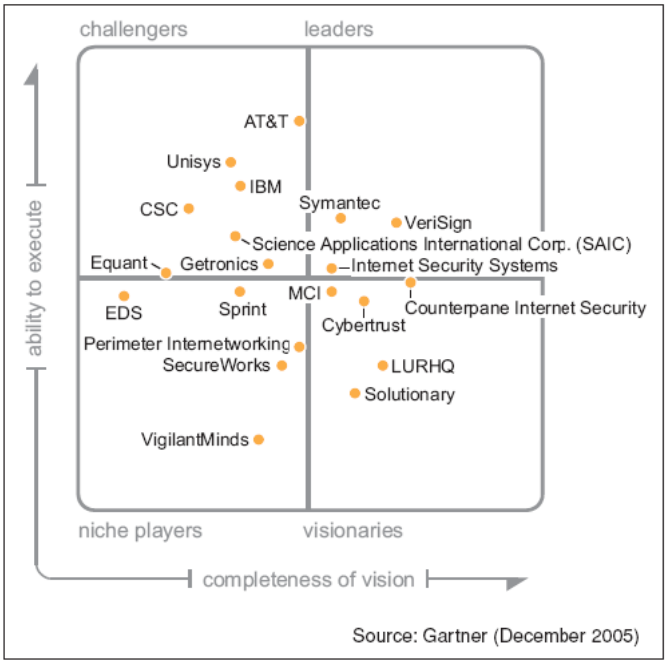
New Competitors in the Market

Companies that offer the same products and services or those with similar functionalities are considered as the competitors to Symantec. The MSS market is competitive and subject to rapid technological changes. Competition is a dynamic risk because certain level of competition can stimulate the innovation of the company and improvement in quality and cost reduction in the company's operation. Failure to outperform

the competitors can cause the company being forced out of the market or even bankrupt. Competitors to Symantec in North America MSS market (2005) as the figure shows:

MAGIC QUADRANT

Figure 1. Magic Quadrant for MSSPs, North America, 2H05



From the Figure, we can see that Symantec is one of the leaders in the MSS market and has a high ability execute. There are potential challengers coming out which are also its new competitors, such as AT&T, IBM, CSC, Unisys and so on. We can see that new competitors in the MSS market become a problem to Symantec.

The KPIs that are influenced directly from this risk are:
- Percentage of MSS market
- Income/Expenses for MSS services
- Churn rate (satisfaction)
- Improvement in IT Security Training
- Percentage of Employee Turnover

First, new market entrants and niche players are likely to compete with Symantec in gaining MSS market shares. This may negatively influence Symantec's percentage of the MSS market. This competition will affect the income and expenses for MSS services provided by Symantec depending on how well it responds to the competition. For example, Symantec may reduce the product price to attract customers which will cause income decrease. Symantec may also put more money to promote their product which may cause expenses increase. Customer satisfaction is the key element in wining the competition; therefore Symantec should focus on meeting the customer's needs and expectations or even exceed their expectations in order to have satisfied customers. Furthermore, Improvement in IT Security Training will better equip Symantec's employees to provide the best technical service and better educate its potential customers, so it is also necessary for the company to stay competitive. In addition, competitors are likely to affect Symantec's employee turnover by offering better salary and benefits to lure them away and if there are too many competitors there will be a shortage in labour market as well. This is a dynamic risk which influences so many KPIs; we can mitigate this risk in order to gain a positive result from the competition.

Severity

This risk is also medium because the appearance of new competitors will have two opposite sides to influence your company: to stimulate your company to do better or your company being forced out of the market. It will depend how the company perform with the competitors. So the risk is medium.

Mitigation

To mitigate the risk brought about by the new and existing competitors. We should concentrate on our core competences and try to keep our customers satisfied. Symantec's competitiveness depends on its ability to

deliver products that meet customers' needs by enhancing the existing solutions and services and offering reliable and standardized new solutions on a timely basis. To optimize the limited resources, we should focus on the principal competitive factors in Enterprise Security and Enterprise Administration segments are quality, employment of the most advanced technology, time to market, price, reputation, financial stability, breadth of product offerings, customer support, brand recognition, and sales and marketing teams.

To test this mitigation plan, we can do a survey to certain groups of customer. With the survey we can find out if the customers are satisfied with our MSS product and willing to purchase our product and if our core competence is sustainable. For example, the questions in the survey can be "Are you satisfied with MSS offered by Symantec?"; we can also list some other competitors in the survey and ask which company customers prefer to choose as their first alternatives.

Malfunction of hardware/software

Malfunction of software and hardware are static risks that are always present in IT systems. Symantec has a large amount of data that come to the system, and need to be processed. Large amounts of incoming data keep Symantec's hardware and software always working, which may cause in malfunctions of them. There is also a risk of improper use of software or hardware that may lead to malfunctions of the system. Quality of hardware and software is an essential factor that may improve and mitigate malfunction of used hardware.

KPIs that are influenced by the risk:
- Response time
- Uptime 99.99%
- Income/Expenses for mss services

Malfunctions of software or hardware may result in extending response time if the entire system is affected in the time of reporting an attack or some vulnerabilities. If the malfunction of a vital hardware or software is not detected in the time, the problem may cause in decreasing percentage of the system uptime. Replacing of affected part of the system costs Symantec in buying a new hardware/software and affect annual revenue.

Severity
Depending on the affected part of the system, the severity may be assessed from low to high.

Mitigation
The one way to mitigate this risk is to buy certified and brand products that have been tested and which life warranty is quite enough until Symantec decides to replace old equipments. After some period, Symantec should replace old equipments with new ones and reduce risks of malfunctions. Symantec has already resolved influence of this risk to KPIs with redundant systems, more SOCs and sensors, that may replace functions of the affected malfunction hardware/software.

Employee Risks (Lack of competence, background checks)

From a security perspective, lack of knowledge comes with the lack of security awareness. Lack of security awareness is one major risk for the security of a company. Employees that do not keep a related background to IT security knowledge, and have privileged access to systems or information, can be used or tricked by outsiders in order to help them take control of important information. Generally, people that have major security responsibilities and do not include the appropriate skills and knowledge, people that facing lack of competence with no background checks have no adaptability, no productivity and comprise a weakness in the security of the company.

Influenced KPIs are:
- Improvement in IT Security Training
  Lack of competence is mostly due to lack of knowledge. Because of the lack of IT security training the staff is mechanically working without any useful knowledge background. The KPI is related to the above risk since any IT security Training to the staff will bring different values and results to the above risk
- Successful Intrusion Attacks Attempts/ Total Intrusion Attacks Attempts
  The increment of the percentage of the number of the successful intrusion attempts, could be and mostly is, due to the lack of security awareness that the untrained staff has. As already mentioned, people that have privileged access to systems or information can be used or tricked by outsiders in order to help them take control of important information. This might have an impact in the increment

of the intrusion attempts.

- Response Time

  The time of a problem that occurred and the time that has been corrected, is highly related to knowledge that the staff should keep in order to take effective actions to solve the occurred problem. An employee without updated training and with no background knowledge checks, will take more time to solve a problematic situation if he/she is not aware or familiar of the circumstances that he/she is facing.

Severity

Risks that occur by the lack of knowledge of the employees are risks of a medium level of severity, since employment by Symantec concerns people with certified knowledge in matters like security is. If Symantec starts to hire only certified people, that can be considered as a dynamic risk, since the profit that will bring is good reputation.

Mitigation

The only way to mitigate the above risk is to perform seminars and IT security training to all the related personnel in order to be aware of all the new methods and be prepared to take effective actions when needed. The personnel apart from the knowledge that should have received, should also have background knowledge checks in order to be able to ensure their knowledge in a way that will not effect the company negatively. People with high security responsibilities should include in their resume relevant certifications that ensure their ability and their knowledge in the specific field. Tests and background knowledge checks should be also given to certified employees in order to prove updated knowledge for new security features.

Cultural Differences- Social skills

Analyzing through a business perspective of an MSS service, communication is one of the most important features. Any lack of the ability to communicate effectively, to be able to understand, to explain and to reason suggestions can lead, not only to business risks but also to operational risks. If there is no ability of communication, then difficulties will occur during accomplishment. Social skills define the ability to communicate, to understand, to cooperate, to adapt knowledge which leads to productivity. Cultural differences could be a reason for the lack of social skills which could lead to lack of trust, cooperation and moreover to lack of communication. Apart from the above reasons, cultural differences can lead to hostile activities among the personnel due to racial discrimination, this is a result of fanaticism which could be catastrophic for the company.

Influenced KPIs are:

- Percentage of Employee Turnover

  Employees could leave their positions and quit their jobs because of cultural differences with their colleagues. This could be a result from as already mentioned before, racial discrimination, or generally political differences between their home countries. The KPI's value can easily be influenced by "cultural differences" reasoned situations. The lack of social skills could also result for an employee to quit his/her job because of the lack of the ability to communicate and get on well with his/her colleagues.

- Response Time

  The response time could also be effected, by the above risk. If a problem occurs, and the employee that is responsible for its solution, lacks of the ability to understand how the situation goes, or faces problems to explain it, delays in the response time will occur.

Severity

People nowadays receive a high level of background education. Fanatic people comprise just small minorities with no negative impacts. Symantec has a large diversity of cultures within the organization and know, from experience, how to deal with that, so the impact would not be so catastrophic. Moreover, this risk is not that common these days. Hence, this risk should be considered as low severity.

Mitigation

Problems caused due to Cultural differences are usually caused by people that lack of general brad knowledge and keep narrow minded thoughts. A way to avoid such problems is to interview and discuss with future potential employees while they are being interviewed for getting hired by the company. By establishing principals and policies in the company, employees will have to keep up with these policies and try to

compromise with them. Another way to avoid such problems is build a “company culture”, to try to bring employees together and closer to the company’s policies and principals by inviting them to activities where they would get to know each other in a more friendly way. This way can also be effective to problems caused by communicative skills because people will be able to understand each other like they are from the same native.

Data Integrity and Confidentiality

We use this risk to illustrate the problem of keeping security data gathered from clients secret and accurate. This data is huge in volume, and needs to be processed in 2 layers: first an automatic layer that filter the data, then a “human layer” which looks at interesting data to see if there is any problem. Because of the huge amount of data and the layered process, it is absolutely essential that all data is correct, so that the right decisions can be taken. We also have to protect this data from people that are not authorized to see it, since it could expose what security measures are implemented in a given client company.

The KPIs that are directly or indirectly influenced by this Risk are
- Percentage of mss market
- Income/Expenses for mss services
- Media coverage good/bad percentage
- Successful Intrusion Attacks Attempts/ Total Intrusion Attacks Attempts

The KPI that will be most directly affected is Successful Intrusion Attacks Attempts/ Total Intrusion Attacks Attempts. If integrity of data is breached, we can no longer rely on this KPI since we don't know the true numbers. If it becomes publicly know that Symantec has problem with Date Integrity or Confidentiality, they will get much negative media coverage. It may lead to loss of current clients and deter future prospective clients from buying MSS-services from Symantec, thus affecting Percentage of MSS market and Income/Expenses. There may also be a direct effect to the latter if the client seeks damages.

Severity:
The severity is high, because for any breach that occurs we can not be sure about the information that were lost or changed. Furthermore if it becomes publicly known the companies profile will be affected. We can not provide Security Services without having secured ourselves first.

Mitigation:
To minimize this risk, we need to always use the most state of the art technology and software together with an exceptionally gifted staff. Even then it's not possible to guarantee it won't happen, so we need to be able to react quick and to have a insurance that can cover some of the costs. Good PR and CR departments is also of high importance.

Design Faults/Flaws that can lead to CIA problems

This risk covers the problem that due to design faults/flaws in software/hardware that is made or provided by Symantec, there is a breach in the customer's security, affecting confidentiality, integrity or accessibility of customers data or services. This risk will always be there, as no system can be 100% secure.

The KPIs that are directly or indirectly influenced by this Risk are
- Percentage of mss market
- Income/Expenses for mss services
- Media coverage good/bad percentage
- Successful Intrusion Attacks Attempts/ Total Intrusion Attacks Attempts
- Uptime 99.9%

This risk will influence more or less the same KPI's as the “Data Integrity and Confidentiality” risk. However, there are some differences: a breach in the customer's security will almost always lead to some kind of penalty/damages being paid to the customer, thus Income/Expenses is more directly affected. There is less risk of Media coverage, since both Symantec and the affected company will want to resolve this as quietly as possible. Also, if there is a problem with availability, the “Uptime”-KPI will be negatively affected.

Severity:
We consider this risk as having a high severity, because it would have a high negative effect on the KPIs

mentioned above.

Mitigation:
As with the "Data Integrity and Confidentiality" risk, Mitigation depends on having good hardware/software, expert staff and responding quickly to any trouble, as well as having insurance for the losses that may affect Symantec.

Wrong requirement in RFP and problems in SLA agreements

This affects Symantec whenever they encounter a new customer and the two parties wants to sign a legal binding contract. It becomes a problem when the customer specifies the wrong requirements and don't know exactly what kind of service they want Symantec to provide. Therefore it is always important to beforehand state very clearly that both parties understand and agrees on the contract. A Service Level Agreement (SLA) handles issues like uptime/downtime, maintenance, integrity and accessibility. In an SLA it is important to be specific in what you agree upon in the agreement regarding what services you are obliged to fulfil. In case of disputes regarding, for instance, the accessibility there can arise problems if you haven't properly stated for how long your service can be down before you break your part of the contract.

Influenced KPIs
- Income/expenses for mms services
- Uptime 99.99%
- Disputes

If a contract is misunderstood it could have economical consequences. Symantec could face a high, unexpected, cost if the requirements change in the developing process. But it could also generate an income when renegotiating the contract and new or different ideas have to be implemented. The uptime 99.99% state the SLA agreement and that is what they are obliged to fulfill. If Symantec are unable the will have to face the cost. That part of the SLA agreement you usually want to bargain with and have as few digits after the comma as possible. It is unusual to have more than two digits. That would mean the downtime for their services could only be for a couple of hours a year. That is a very costly service and requires both advanced servers (management system) and skilled personnel. The disputes are of course if any of the parties' breaks their part of the contract and the matter will have be taken care of in a court of law. That is a time consuming and costly experience, and could also result in bad publicity for Symantec.

Severity
All form of contracts and legal agreements are serious business. If they are poorly managed and written without good legal knowledge it could be the downfall for a company. However, Symantec has already good knowledge and staff about this matter. Therefore we will consider this to be a medium risk to our company and business.

Mitigation
For us to mitigate this risk in the most successful way we have to constantly upgrade our routines when handling with legal contracts. To always be sure of covering all possible loop-holes we will have to check our standards and administrating routines. Our legal advisors will be well selected and always be at "the top of the game" in their business. They should be very well trained in legal matters and experience in handling those issues is also of great importance. In order to minimize the risk in misunderstandings in the contract between our customers, we have to offer them good packages of services. So they can choose what they want and pick the best solution for their needs. And also give them help in deciding in what services they are in need of, if they are uncertain of that matter. Educate them in a helpful way rather than in a demanding and "big brotherly-way".

Legislation/standard changes

Symantec are operating in several countries all over the world. The work by the American legislation and standards, which are the most currently used ones in their market. If a new legislation or standard is claimed and starting to dominate the business, all companies will have to adapt to it. It could also mean they have to produce their services in another way than before. It is therefore very important to always be one step ahead and try to figure out how the market is going to change. An example is the new SOX act, which changed the ways of accounting your business for all companies. It could be costly and catastrophically not to keep up with the market changes.

Influenced KPIs
• Percentage of mms market
• Income/expenses for mss services
• Churn rate
• Media coverage good/bad percentage

If the standards or the legislation on how to conduct your business change, Symantec could loose a piece of the market to competitors, if they haven't foreseen it. Usually you now about a legislation change but it can be more difficult to predict which standard everyone is going to use. If the loose some percentage of the market it will result in income loss as well. And their services will not be as highly acclaimed as before. This will also affect the churn rate on their customers. If costumers are choosing competitive companies instead, Symantec's churn rate will go up which means instability. If all these events occur it will also generate bad publicity in the media. In the end their reputation is damaged and they will have to struggle to get back on top again.

Severity
We consider this to be a medium risk to Symantec. It could be devastating to loose market percentage because you don't choose the right standard or have a bad business model. On the other hand since we are leaders in this domain the first to adapt to any changes will be us. Furthermore the financial strength that we have will allow us to adapt faster than any other small competitor.

Mitigation
We should always have employees who are well informed on the market (standards, legislation) situation and its upcoming changes. Therefore we should have a team of employees who are specialized on the subjects and are the best to be able to perform change management in the company. Symantec is now one if the leading brands but that doesn't mean that they will conduct the standard changes or always be sure of being in the leading position. The business goals should be many and of variation kind to prevent from getting stuck in a corner of the market. They should strive to own the whole market, and then legislation changes won't be a problem. Their business should be easy to adapt to any new situation.

Bad business choices

Symantec need high quality strategic and practical guidance about how to work with emerging companies to maximize the performance of their employees and gain income. This includes well-defined practices to evaluate, select, contract with, manage, and terminate relationships with emerging companies. Otherwise it is a risk to Symantec in which Symantec may have more expense then income.

Tremendous risks are associated with the investments an organization makes for new service. Markets, competition, government regulations, financial conditions and technologies all change extremely quickly. Symantec should keep up with these changes with respect to their services and products for gain income otherwise it loses their assets.
Symantec will make investments on behalf of many clients, not just one. Shared investment spreads risk, and significantly reduces the risk born by a single company. This is a Strategic Risks and it is also a dynamic risk. Therefore the KPIs related with this risk can be positively or negatively affected.

The KPIs that are influenced directly by this Risk are
• Percentage of mss market
• Income/Expenses for mss services
• Media coverage good/bad percentage

First of all good business practices will increase the number of clients and reputation that leads to percentage of MSS market. For handling more clients and providing more service may be fall our income and rise expenses because we will have to get more stuff to handle the increased traffic and services our clients. Depending on the performance of company and way we handle the situation we can receive good or bad coverage from the media.

Severity:
Impacts on reputation – *medium*

- The loss of customers will in long term harm the reputation of the company and make the market share decrease.
- Goodwill of the company will also decrease.

Impacts on customers – *medium/high*

- More and more customers will choose the other competitive company, which will lead to a decrease in diversity of clients. The number of customer complaints might also increase.

Financial impacts – *high*

The market share loss and loss in earnings per share will give the company financial problems.

Globally, we would say that this will decrease the faith in us among customers and hence our market share. This has a direct impact on Symantec's revenue stream and should be classified as Medium

Mitigation

For us to successfully mitigate this risk we will have to choose good business strategies. Before starting any new service we should completely analysis the market, threat for which we are starting new service. In order to minimize this risk we should choose a team that consists of 3 peoples from management and two from security specialists. This team wills analysis all things before starting new services. From the report of this team we will get a better idea of how a possible feature risk might work and prepare our systems to counter it successfully.

Inadequate Log keeping

Symantec MSS operates on different vendors' products. So Symantec need to keep all customers log and keep all product information, these products comprises of IDS, Router, and Firewall etc. which generate enormous amount of log data. In MSS this log data is sent to Log Management Unit which then transfers them to SOC/Operations.

At service level different data analysis are possible which could reveal important company information. Inadequate log always harmful for any MSS provider by this way they can't justify the customers. As a MSS company their main source by which they provide managed security that is proper log keeping. If they can not maintain proper log of clients, then this might arise security problem and also arise some business losses for Symantec. We can divide these losses into three categories: productivity losses, indirect losses, and legal exposure. This risk is a static risks because it may not have a positive result.
Improper database security management leads towards to revelation of Company Secret Information and also inadequate log does not cover all vendors' data.

The KPIs that are affected are:

- Successful Intrusion Attacks Attempts/Total Intrusion Attacks Attempts,
- Dispute,
- Decrease in False Positives

Severity:

The severity can reach very high because Symantec will take MSS related actions with the help of logs. If log are not properly kept and secured, then problems will arise.

Mitigation plan:

The mitigation plan in handling such kind of issue is should be transparency i.e. the Symantec should precisely indicate in their contract which sort of long file(s) they want to get access to the particular devices in their contract. Moreover, the service provider should be accountability to the client. All these issues should be stated in the contract and should be according to the national, international and IT legislation currently in practices.

Internet Epidemic

We use this risk to illustrate the possible outbreak of malicious software in the computer world through the Internet. A past case like this one was the Blaster worm. This is a technology risk and it is also a dynamic risk, since Symantec might find itself in having to deal with thousands of high security threats in a small time

frame (for example a day) and subsequently fail or manage to perform exceptionally and prove that it is a leader in the Security market. Therefore the KPIs related with this risk can be positively or negatively affected.

The KPIs that are influenced directly by this Risk are
- Response Time
- Income/Expenses for mss services
- Media coverage good/bad percentage
- Successful Intrusion Attacks Attempts/ Total Intrusion Attacks Attempts
- Uptime 99.99%

First of all an increase in the number of threats per day can influence our response time and deteriorate it. Our income might fall and expenses might rise because we will have to get more stuff to handle the increased traffic and service our customers. Depending on the way we handle the situation we can receive good or bad coverage from the media. A new malicious software program spread across the network can result in more successful intrusions at least until the moment it is detected and the affected systems are patched. Therefore our Successful Attacks/Attempts KPI will rise. Finally an Internet Epidemic can influence our own systems and subsequently force us to shut down systems valuable to our business. Our uptime will be negatively affected and our clients will remain unprotected with everything else this will have as an effect. As far as our assets are concerned we might have a financial loss or gain after the situation is over. As we previously mentioned this type of threats are cross-platform viruses, worms, spy ware and finally the most exotic of all the probability of a worldwide breakdown of the Internet maybe occurring due to a protocol, hardware, software design malfunction or bug.

Severity
Focused on the impact this threat can have to our business we would have to rate it as a high risk from a qualitative perspective. The results would be catastrophic or greatly influencing for our company. However, if we take a quantitative look, we see that this kind of epidemics doesn't appear so often, so the probability of an internet epidemic is quite low. Hence, we would put it as a medium risk because of it's low frequency.

Mitigation
For us to successfully mitigate this risk we will have to fine tune our sensory mechanisms. This mechanism can be either sensors established in the Internet. The sensors can monitor Internet traffic and give us early warnings especially if we fine tune them to look for certain information and events. For example if a corporate network is suddenly infected by a virus, maybe this can be a first sign of a coming outbreak. On the other hand our R&D department should try to study all the latest trends in computer science and system security so that we are always informed about whatever new is constructed and researched. We can furthermore plan so that we have the required back up personnel and systems to successfully counter any threats and inform our clients. If we prepare to face crisis that might surface we will have the right policies and mechanisms set in place to counter this Risk.

In order to test if our approach to mitigate this risk is the correct one we can do several simulations. We can have a training exercise for our personnel and systems in frequent time periods and with different difficulty levels. The results of these tests can be used to calculate what effect our actions will have on our KPIs. For example if during a training we fail to notify our customers successfully we might suffer income loses, or receive bad publicity. There are consultants and analysts who can by a list of our actions and their results identify the future effects on our KPIs.

Mitigation Plan

In the previous section, a mitigation plan for each risk has been proposed. However, due to resource and time constraints, it is not possible to mitigate all of them. Hence, we propose in this section a selection of the five most important risks that have to be mitigated in the first place. This choice is mainly made according to their severity level (qualitative impact), but also by having their frequency in mind, and their "meaning" for MSS.

The five risks that have to be mitigated are:

- Malfunction of hardware / software
- Inadequate log keeping
- Data integrity and confidentiality
- Design faults/flaws -> CIA problems
- Wrong requirements in RFP and problems in SLA agreement

References

(1) *"Managing Infomation Security Risks"*, Alberts, Christopher et al, Pearson Education Inc., 2002
(2) *"Symantec 2005 Annual Report"*, Symantec, http://library.corporate-irnet/library/89/894/89422/items/163589/Final_Symantec_2005_10Kwrap.pdf, 2006-04-25
(3) *"Using Key Performance Indicators to Maintain Strategic Focus"*, T. Birrittier, http://www.businessintelligence.com/ex/asp/code.117/xe/article.htm, 2006-04-25
(4) *"Business Assurance and the Changing Role of IT"*, C. Grieves, http://www.ebizq.net/topics/tech_in_biz/features/6694.html?&pp=1, 2006-04-25
(5) *"Selecting the Right Key Performance Indicators"*, A. McNeeney, http://www.mtonline.com/articles/0405meridium.cfm, 2006-04-25
(6) *"Outsourcing IT Security"*, M. M. Stephenson, http://www.protiviti.com/downloads/PRO/pro-us/articles/FeatureArticle_20030509.html, 2006-04-25
(7) *"Key considerations for outsourcing security"*, Symantec, http://www.symantec.com/symadvantage/020/mss.html, 2006-04-25
(8) *"Symantec Monitored and Managed IDS/IPS Services"*, Symantec, http://eval.veritas.com/mktginfo/enterprise/fact_sheets/ent-factsheet_intrusion_detection_services_06-2005.en-us.pdf, 2006-04-25
(9) *"Seven Keys to Growing Your Business"*, B. Tracy, http://www.entrepreneur.com/article/0,4621,324545,00.html, 2006-04-25
(10) *"SSA's FY 2005 Performance and Accountability Report"*, SSA, http://www.ssa.gov/finance/2005/Key_Performance.pdf, 2006-04-25
(11) *"The Power of Metrics: Key Performance Indicators: The Multiple Dimensions"*, K. Bauer, http://www.dmreview.com/article_sub.cfm?articleId=1011028, 2006-04-25
(12) *"Getting value from IT Investments"*, M. Blowers, http://insight.zdnet.co.uk/hardware/0,39020433,39243470,00.htm, 2006-04-25
(13) *"Twelve Value Drivers Help Ensure Success in Today's Tough M&A Environment"*, M. Graham, http://www.focusenterprises.com/publications/fnv1n4_12vd.asp, 2006-04-25
(14) *"Key Performance Indicators (KPI)"*, F. John Reh, http://management.about.com/cs/generalmanagement/a/keyperfindic.htm, 2006-04-25
(15) *"Employes"*, Symantec Web Site, http://www.symantec.com/about/profile/responsibility/employees.jsp, 2006-04-25
(16) *"Internet Security Training for Employees"*, Symantec, http://enterprisesecurity.symantec.com/article.cfm?articleid=613, 2006-04-25
(17) *"Reported Earnings - Earnings Per Share"*, ValueBasedManagement.net, http://valuebasedmanagement.net/methods_eps.html, 2006-04-25
(18) *"Working Capital Performance Solution"*, Jaros, http://www.jarostech.com/workingcapital.html, 2006-04-25
(19) *"COMMISSION RECOMMENDATION of amending Recommendation 96/280/EC concerning the definition of small and medium-sized enterprises"*, Commission of the European Communities, http://europa.eu.int/comm/enterprise/consultations/sme_definition/consultation2/153_sme_definition_25_6_2002_pp1_11_en.pdf, 2006-04-25
(20) *"Vendor Rating : Symantec"*, Gartner, http://www.symantec.com/content/en/us/about/media/industryanalysts/Gartner-Vendor-Rating.pdf, 2006-04-25
(21) *"Managed Security services"*, Symantec, http://eval.veritas.com/mktginfo/enterprise/brochures/ent-brochure_managed_security_services_10-2004.en-us.pdf, 2006-04-25
(22) *"Managed Security Services come down to Trust"*, ITBusiness Edge interview with J. Paransky, http://www.itbusinessedge.com/item/?ci=11719, 2006-04-25
(23) *"Symantec 2004 Annual Report"*, Symantec, http://media.corporate-ir.net/media_files/irol/89/89422/FileUpload/Symantec_2004_AnnualReport.pdf, 2006-04-25
(24) "*Magic Quadrant for MSSPs, North America, 2H05"*, Gartner, http://www.verisign.com.au/mss/Gartner-Quadrant.pdf, 2006-04-25
(25) "*Security Metrics: Creating Value and Tracking Performance"*, L. McCarthy, http://www.information-integrity.com/article.cfm?articleid=545, 2006-04-25
(26) *"Symantec Expands Lead as World's Largest Security Software Provider"*, Symantec News, http://enterprisesecurity.symantec.com/content.cfm?articleid=1784&EID=0, 2006-04-25
(27) "*Symantec Reports 29 Percent Revenue Growth in Fiscal Third Quarter"*, Symantec News,

http://enterprisesecurity.symantec.com/content.cfm?articleid=1920&EID=0, 2006-04-25
(28) *"Symantec Gains Added Vendor Neutrality with New IPS Support"*, Symantec News, http://enterprisesecurity.symantec.com/content.cfm?articleid=5511&EID=0, 2006-04-25