Security Management

2I1506

Assignment 1

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
Khan Khalid
Milinkovic Zoran
Saeed Tariq

Managed Security Services

Part I: Introduction

Company History

Outsourcing is a method totally familiar to Ericsson, since it was the main solution in recovering from the biggest crisis that the company faced in its entire history. In January 2001, Ericsson announced that it was pulling out of mobile phone production because of a pre-tax loss for the year of 21.1 billion SEK ($1.97 billion), there were warnings about further losses for the beginning of 2002. Comparing to the year 2000, when the company had made a profit of 9.373 billion SEK ($878 million), in 2001 the company's market value fell by 61%, that is about $50 million or 533billion SEK. The company's sales fell 32%. It was the first loss that the company ever had in its 130 year history. Ericsson branded phones in the future were going to be produced by Singapore-based Flextronics who was supposed to carry out all aspects of the production apart from the design. Other work would be outsourced to Taiwanese firms such as Arima and GVC. The shareholder value of that period faced a 13 percent fall since stock watchers had expected the company to abandon mobile phones and expected it to focus on other telephony infrastructure and network areas. Because of the crisis, some moves had to be done in order to keep the company alive. Factory transfers, outsourcing, many combination of redundancies, approximately 22.000 employees lost their jobs that year, most of them located in Latin America. More or less this is how SonyEricsson was founded in October 2001, when Japanese based Sony Corporation shipped about 6.8 million mobiles to Ericsson AB, and the joint venture was established. Like all telecom companies Ericsson has been heavily investing for the infrastructure of 3G third generation mobile phones and other devises, that are able to receive audio, video streams allowing web browsing and also other activities. Furthermore, most of the vast sums that have already been invested for the "3G global telecom industry competition" are basically spent in outsourcing services from different companies. Judging by the previous example, we can understand that outsourcing is a matter of a great importance for companies nowadays. It helps them focus on their core business, increases efficiency while reducing costs. Especially for Ericsson, a company that does not deal mainly with security, outsourcing services to other professional security experts that are able to take charge of all kinds of security issues can be essential. On the other side there are risks and problems associated with outsourcing, but Ericsson's extensive experience in the field of outsourcing could help to minimize this.

Core Business Segments

Today Ericsson business is divided into three main segments:

- **Systems – Mobile Networks, Fixed Networks and Professional Services**

  Mobile Networks
  Ericsson provides complete mobile systems solutions that can include radio base stations, controller, switching gear and other components. Assembly, integration and testing of parts are done in-house, but a large part of the module production is outsourced to companies in mostly low-cost countries. Ericsson is considered to be world-leading in the mobile systems area. Ericsson is also active in developing existing and new standards for mobile networks.

  Fixed Networks
  In this area, Ericsson is mostly active in Latin America and in Europe. Ericsson has been a player in fixed networks for a long time, and has seen and participated in the change from single-service networks (ex. telephony, cable-TV) to multi-service networks that can handle both data, voice and images. These new networks are IP-based and packet-switched, allowing for a high flexibility regarding which service can be provided over them.

  Professional Services
  Managed services, consulting and systems integration are examples of services Ericsson provide in their Global Services business. As an outsourcing-partner for a vast amount of network operators, Ericsson has had great success in providing network design, operations and maintenance. Ericsson also provides comprehensive managed services for the telecom industry, including content management and payment

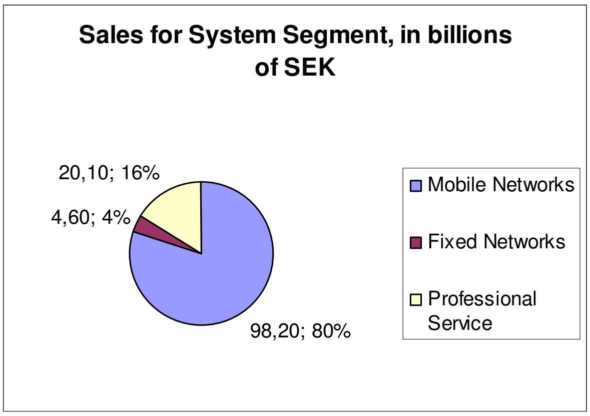
and messaging delivery solutions.

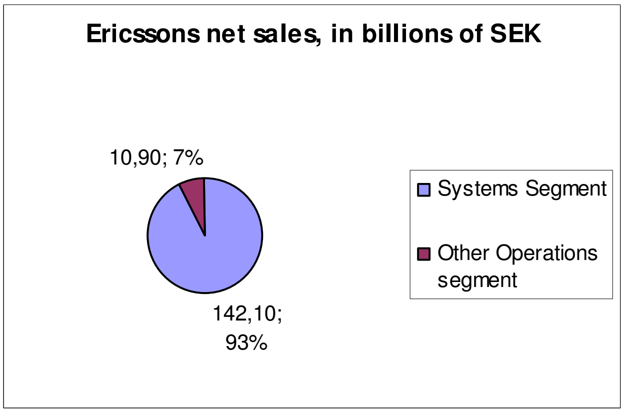
- **Phones - together with Sony (joint venture)**
  Sony-Ericsson
  The Sony Ericsson Mobile Communications have had great success in designing, developing and producing mobile phones, PC-cards and other accessories both for the private and business markets. Most of the production takes place in Asia.

- **Other operations**
  The business-units contained in the segments are quite small, constituting no more than 6% of net sales for the whole company. However, these areas are still considered important, as they provide added value for the other segments.

The biggest market for Ericsson is Western Europe, followed closely by the CEMA-region (Central & East Europe, Middle East and Africa).

Ericsson's total net sales for the year 2005 equalled to 151.8 billion SEK.





IT/IS threats and their effect on shareholder value

Malicious Software

Availability in Ericsson’s core business is an issue of great importance, concerning the fulfilment of the company’s expectations. Any lack of availability that occurs in companies internal systems has impact in different aspects. Malicious software like viruses, trojan horses, bombs and worms are a major threat against availability, they find use mostly in denial of service attacks. If a denial of service attack ends up with a worm getting transferred through the company’s intranet without being noticed on time and viruses waiting to get active among users’ pc's, the communication links will probably be destroyed, files will be corrupted, orders from clients would not be forwarded, outbound connections would be infected and Ericsson could face instability. Instability for companies like Ericsson means lack of reliability and bad reputation. The company’s stock watchers will get doubtful and the shareholder value will fall. On the other hand, spyware is a threat against confidentiality. If installed, spyware can expose crucial information that the company relies on their secrecy. For instance, secret internal problems that the company kept in files could find a great use in the hands of an opponent company. Future investment plans would be of great interest for business competitors.

Outsiders

A hacker is a person who is able to exploit a system or gain unauthorized access through knowledge and skills. Bad hackers are what we want to call outsiders. They organize and perform attacks that will bring out and expose important information by exploiting vulnerabilities and weaknesses of the targeted system. They can act either by their own will or for others instead. The others could be other competitor companies or individuals that are willing to pay these people not only to get the information that they want, but could also be interested in bringing out, expose or even transform files that contain important information for the company’s investments, the company’s clients, partnerships and business moves. The target system could be a server, a network or subnetwork that controls important features (data base, intranet, email server, etc). Weak security facilities in the network boundaries can bring the outsider more easily and make the target more attractive. Last year there was a similar incident that happened to Ericsson. A 26 year old Hungarian man was charged by hacking in both Sony Ericsson AB and Ericsson's intranets. Csaba Richter when questioned about the reason that he did this, he said that he was actually looking for a job by proving his skills and he was also claiming about the weaknesses he found in Ericsson's and Sony Ericsson's intranets. One of the charges that Richter was accused for, was "unauthorized handling of secret information" (6). Surprisingly Ericsson's clients were not affected by the attack; otherwise Ericsson would have a major negative impact. Outsiders can be a major threat in the company, since they have the will and the ability to control, destroy, expose and to manipulate any features that threaten the company's confidentiality. The shareholder value of the company is highly depended on features that keep the company's reliability and trust in high levels. Reliability is highly depended on the company's confidentiality. Factors that threaten the company's confidentiality are a major threat for the company's future vitality.

Insiders

Malicious outsiders with skills and knowledge of hackers are a major risk to the company. As mentioned above, they have to be considered as being able to do anything in order to bring down the security and control the system. At least the company knows from who should be protected. By upgrading security or bringing it in higher standards, by protecting important features of the company and by increasing the confidentiality and the security awareness of employees, malicious outsiders will have to try a lot harder for their least accomplishment. But the critical risk of the company is the malicious acts made by people that are authorized and are not trying to invade into the company's system; they compose a part of it. Insiders are the people that act from the inside of the company and are the most hard to allocate. They are almost undetectable because they usually belong to trustful parties, like personnel. Insiders like outsiders, usually don't act, because of their own interest. Other parties like outsiders, might support them financially in order to provide them with important information of their interest. A similar situation happened in Ericsson in 2002 when two men have been convicted for industrial espionage against Ericsson. One of them was an insider, he was working in Ericsson and he was selling information to a Russian Intelligence Officer. Any access, authorized or non-authorized, from an untrustful individual or party, can be a threat against the confidentiality of the company. As already mentioned this has a major impact against the company's reliability and expectations. Awareness against these kinds of circumstances is highly needed.

Other threats affecting IT/IS and their effect on shareholder value

Unauthorized access to facilities

When somebody accesses a facility he doesn't have the right to access. The threats arising from this are many: hardware theft, sabotage, industrial espionage and others.

- Hardware theft: this threat will directly affect Ericsson's assets, as new hardware will have to be bought, installed, configured and integrated. This may also be a part of the "Industrial Espionage"-risk, as an intruder may steal newly developed hardware.
- Sabotage: as with hardware theft, this risk has a direct impact on Ericsson's assets. Destroyed/broken hardware will have to be replaced/repaired, and the sabotage may also rend a process unusable, resulting in systems downtime, further security breaches and other problems. Except for the direct cost of the hardware, people working with the system that is down will be idle, as they can not perform their work, rending further economical damages.
- Industrial espionage: the purpose of the attacker may be to steal/copy documents, gaining access to unprotected computers (thus connecting with other security breaches mentioned above) in order to steal passwords, copy material and so on. The damages from this threat are not as direct, since nothing is actually destroyed. However, it may result in competitors knowing about Ericsson's plans and development progress, thus giving the competitor an unfair advantage and finally lower Ericsson's sales. It may also result in business-deals being lost, as an competitor know Ericsson's plans/development status and may use this information in making a more attractive bid in a deal.
- Physical danger to employees: except for the threats mentioned above, a breach in the facilities security could result in employees being physically/mentally harmed, in case of robberies, sabotage and acts of terrorism. The effects of this could be very severe:
    - People with key-skills being harmed/intimidated, setting back development/production or business operations.
    - Employees feeling unsecured, resulting in loss of productivity.

- Cost of threatening physical/mental damages of employees, and hiring replacements during treatment.
- Difficulties in employing future employees, if word of this threats becomes publicly known
- Could affect the stock-price of the Ericsson stock adversely.

Physical threats from insiders

In the last few years a new threat has emerged: small technical units with large storage memory (eg. Ipod, mp3-players, portable USB-hard drives). This threat is partly connected with the Industrial Espionage threat above, but there is a key difference: this threat is carried out from insiders, which may be disgruntled employees, managers and others working in the organization. This means that it's much more difficult to detect/prevent this threat, and it may go on during a longer time-period, thus making a larger economical impact.

Lack in security awareness

Another threat is employees not knowing how to act in a way that promotes security. Even the best technical security measures will amount to nothing if employees divulges information (passwords, other) to people not in the organization, or gives outsiders physical access to facilities. Examples of this can be:

- Somebody calls an employee, claims to be head of security in Ericsson and requests the users password for some reason.
- Somebody walks directly behind and employee entering the facility, thus being able to enter without passcard/password.
- An employee installing software sent to him from “Ericsson's Software Department”.

The effects of this threat could be severe, as it makes all of above threats easier.

Power Outages

In case of power outages, there will be several consequences:

- Activity standstill in the affected facilities: almost all of the activities taking place in normal operation will be interrupted, making productivity close to zero.
- Indirect productivity interruption: few of Ericsson's facilities are stand-alone, so if a facility is down, other facilities/departments depending on the operation of the dysfunctional unit will also incur a loss of productivity.

Equipment failure

As with the Power Outages-risk, equipment failing will more often than not affect other equipment and result in loss of productivity, except for the cost of replacing/repairing the equipment that is malfunctioning/broken. In case the equipment is in itself a security-component, the equipment failure could also lead to breaches of security as describe above.

Natural Disasters

Natural disasters often lead to partial/near total destruction of facilities and equipment, and can also lead to physical damage of employees, resulting in high direct costs. Except for the direct costs, a natural disaster will usually lead to loss of productivity and income, and affect other parts of the company depending on the facilities or equipment that has been destroyed/damaged. There is also a threat of data being destroyed permanently, which could cause irreversible damage to operations.

Concluding Remarks

In general Ericsson is an industry that provides services and solutions strongly connected with information technology. If we consider Ericsson as a living entity, we would say that the core business is the heart and mind. The shareholder value counts on the company’s vitality. Since the core business of Ericsson is highly involved with IS/IT, threats against IS/IT can be more than serious to company’s health.

Part II: Managed Security Services

Introduction

Now a day's enterprise security becomes more complex and dynamic. Both the business drivers and the technological drivers are responsible for this complexity. The business driver represents the increasing communication and transaction, where technology drivers represent the rapid growth. At the same time the vulnerabilities are rising fast. On the other hand, the Enterprise Security Groups face crisis because of flat budgets and compressed resources.

Definition

Managed security services (MSS) is a systematic approach which provides the security needs for an organization. The services performed as in-house are outsourced to a service provider that oversees other companies' network and information system security. The functionality of this service covers a wide area. The services that should be included in a good MSS are:

- Round-the-clock monitoring
- Management of intrusion detection systems
- Firewalls, overseeing patch management
- Performing security assessments and security audits
- Responding to emergencies (e.g. Incident management, including emergency response and forensic analysis)
- Anti-virus and content filtering services
- Data archiving and restoration
- On-site consulting

These services are provided by a number of vendors which reduces the burden of organization's administrator to performing chores manually. It's a better approach to avoid business risk. In conclusion this delivers an enhanced security posture, greater security operations efficiency, improved compliance and reduced security program costs. Therefore a good Managed Security Service Provider is necessary (MSSP).

Symantec Managed Security Services (MSS)

One of the reputed companies is Symantec which provides solutions to help individuals and enterprises assure the security, availability, and integrity of their information. They deliver real-time threat analysis, helping organizations establish compliance, minimize business impact, and reduce overall security risk at acceptable cost in the face of today's emerging threats. These services devolve the burden of real-time network monitoring, advanced security analysis, and global intelligence correlation to Symantec, while allowing businesses to maintain complete insight into critical business information.

Symantec provides the following services:

- **Monitored and Managed Firewall Services**: This service is the vital issue for security management where customers are provided with constant security monitoring, intelligence, and analysis of their firewall technology and firewall device. It also included configuration, performance, and fault management of firewalls and VPN technology.

- **Monitored and Managed Network-based Intrusion Detection Services** and
  Monitored Host-based Intrusion Detection Services: Intrusion Detection Systems (IDS) work by examining the traffic entering VLAN (Virtual Local Area Network) – the private network-within-a-network that connects the servers. It compares the traffic to a database of known attack signatures and abnormal behaviours and generates an alert by detecting a potential intrusion. A prime example of IDS is Snort. Customers are provided with constant security monitoring, intelligence, and analysis of their Intrusion Detection technology and device in addition to configuration, performance, and fault management of IDS management consoles and IDS Sensors.

- **Monitored and Managed Integrated Security Appliance Services**: Customers are provided with constant security monitoring, intelligence, and analysis of their gateway security technology and configuration, performance, and fault management of supported integrated security appliances.

- **Managed Internet Vulnerability Assessment Services**: It is a periodic assessment service that scans and assesses clients' Internet-connected systems such as firewalls, Web servers, etc. this service complements an organization's firewall security controls.

- **Managed Security Policy Compliance Services**: Symantec security advisors perform regularly scheduled audits to ensure continued compliance and identify non-conformance with a company's established information security policy. Symantec also helps organizations determine if their security posture is getting better or worse and more importantly, why.

- **Managed Virus Protection Services**: Virus protection is a serious concern for any organization. Improper protection can result in large data loss, leading to wasted time and resources, potentially even crippling the business completely. Symantec Managed Virus Protection Service provides expert management of antivirus and content filtering technology at the Internet gateway.

Symantec provides MSS not only to specific persons or companies, they also provide there services to governments and federal agencies. Since Symantec was founded by former U.S. Department of Defense security experts, they have all the required technical knowledge. Therefore they have gained valuable experiences in professional security approaches at a high level. Another pro is also that they are able to provide a 24x7 hours security service where they evaluate, analyze and respond to the situations.

- **Symantec Security Operations Centre Technology Platform:** The Symantec Security Operations Centre (SOC) Technology Platform features advanced data mining and security event connection capabilities that enable Symantec experts to actively observe security devices in real time.

- **Separate actual threats from false positives:** The SOC technology platform allows Symantec security experts to split actual security threats from false positives, with consistent results. This process drastically reduces the amount of data a customer must consider to stay updated on the state of their security.

- **Access comprehensive security information:** Through the Secure Internet Interface Web portal, clients have access to complete information from a wide variety of sources available to Symantec. This data is analyzed and presented in a way that makes the current security state of an enterprise understandable while allowing clients to maintain decisive control of their security infrastructure.

- **Global emerging threat notification:** Monitoring thousands of devices on behalf of hundreds of customers and thousands of users in 40 countries around the world, Symantec Managed Security Services has unique insight into the emergence of security threats. Armed with emerging threat intelligence, Symantec provides proactive notification to customers regarding high-risk security events.

Symantec provides MSS services in order to manage data security all over the world. They have a strong organizational backbone and reputation not only in the corporate level but also in defence level. The U.S. Air Force manages 500,000 client devices globally with Symantec LiveState Client Management Suite. They try to follow the standard by selecting skilled manpower as well high technology. They believe as we see from the following quote taken from "Symantec™ Managed Integrated Security Appliance Services" (8) brochure that :

> *"The breadth and depth of Symantec expertise enables customers to improve the security of their enterprise. In addition to global support from multiple SOCs that meet stringent industry certification and auditing best practice guidelines and standards, Symantec Managed Security Services is supported by Symantec™ Security Response, the world's leading Internet security research and support organization. This team, in turn, leverages the data provided by the Symantec DeepSight™ Early Warning services, which provides notification of vulnerabilities and*

exploits as they are identified. "

Concluding Remarks

To have a good MSS policy is very important in the modern business world. It should be at every company's interest to have a secure environment for their business. Not only for personal use but also for the customers well being. They should be able to rely on their trusted company to that their services are fully secured. The customers need to know that their company always tries to be in a leading position in the market in business strategies as well as in security policies and standards. In cultural aspects there is very important to be able to offer a good quality of security. A customer always need to feel safe and have some "proof" of the safeness that there are promised. When costumers feel safe and fully at ease they will be willing to conduct business and put their trust in the services. Therefore you need a provider who can meet up to all your requirements that should be in a good MSS. To evaluate and to analyze are the keywords in the process of choosing a provider.

Part III : Pros and Cons

Introduction

Outsourcing with MSS by cooperating with a Managed Security Services Provider (MSSP) is often a good choice to reduce or transfer information security risks. However, there are both benefits and drawbacks / business risks involved in such cooperation, and both have to be taken into consideration before making the decision. In the following part, we try to present, consider and weight the advantages and disadvantages for Ericsson in using MSS.

Benefits

Quick and effective Response
MSSP can react immediately and more effectively than most ordinary IT professionals. MSSP staffs are very quickly taking action against any security breach. They work with industry standards and are continuously educating themselves on best IT practices.

Costs
Costs may be the most important factor in decision-making. Reducing costs is, to some extent, another form of increasing the profit. It's rather uneconomic to build security management systems and hiring full time experts inside the enterprises by their own. An MSSP can provide the same, even better, managed security services for the clients with much lower expenses. As an MSSP may service several clients at the same time, the cost of hardware, software, hiring skilled personnel and experts, etc., can be shared by all the clients. Consequently, the relative work, such as procurement, specific budget, recruitment and training, can also be performed by the MSSP, which can save not only the amount of money invested but also people and other resources.

Compliance
Compliance found in almost every country where the myriad security-related laws and regulations today is a discouraging task for businesses. MSSPs don't only understand these complex legal requirements also provide solutions for bringing their security programs into compliance. By using MSS outsourcing companies gain access to compliance expertise and their solutions. MSS providers offer very detailed and defined knowledge of legal requirements and industry standards, but also have experience in developing and implementing the best of the security practices. They also give audit services to make sure clients remain in Compliance on an ongoing basis.

Knowledge and Skills
The MSSP can have experienced experts on information security and law working together to serve the clients. Their staffs includes specialists keeping close contact with the most up-to-date information security technology and related areas, and those who have high awareness of information security and keep improving their knowledge and skills through dealing with various cases for the clients. This is much better than relying on one in-house expert working with limited time to "recharge" his knowledge and only sees a limited number of security incidents.

Besides, the MSSP can hire specialists in different areas as needed, which is almost impossible for a company to do so by itself, considering the costs. It's much easier to recruit several persons each being expert in one field than to find one specialist on all the areas. In addition, one man's wisdom may be limited, while team work can inspire new ideas and comprehensive solutions.

Security Awareness
It is not easy for any organization to track and address every possible potential threats, vulnerabilities, attack patterns, intruder tools, and present best security practices. An MSSP can update their staff with new vulnerabilities in advance and obtain early access to information on their countermeasures. An MSSP can advise on how other organizations handle the same types of security problems. An MSSP is normally to have contact with highly qualified and specialized international security experts and other MSSP's. These security experts can be brought not only to bear to diagnose but also resolve client problems.

Facilities

The MSSP's can provide sufficient hardware, software and other facilities for the clients. Many MSSP's have special security operations centres located in various parts of the country. The maintenance and update work is the MSSP's responsibility. Secured, reliable hardware and software resources are managed by skilled personnel to service the clients.

Prosecution

The MSSP are often connected to law enforcement agencies all over the world and better understands about forensic analysis and also evidence required to easily support legal proceedings.

Service Performance

Companies make use of the advanced working standards of the MSS providers by outsourcing them to their security functions. MSSP provide management, monitoring, and support services through their security operations centres in near real time results 24 hours a day, 7 days a week and 365 days a year. This is a large contrast with an in-house service that may only operate during normal business hours. Should there be any emergency, a real-time monitoring can contribute to control the situation, resolve the problem quickly.
The MSSP's have to do their job to fulfil the contract obligations and get paid. Bad performance may not only result in lost of money, but also lead to bad reputation, even end of business.

Recruitment

Less number of qualified information security personnel puts much pressure on IT departments to recruit, train, compensate, and retain critical staff. The cost of in-house network security specialists can be unaffordable. In outsourcing MSSP's have responsible for the costs to hire, train, and retain highly skilled staff. An MSSP has to maintain security experts by offering good career opportunities and positions from entry level to senior management, all in the information security field.

Objectivity and Independence

The MSSP's can provide their clients with objective and independent perspectives on building up the security. They make over all security plans, take all the factors into consideration, and then offer integrated, coherent solutions for the whole company. Such a systematic approach contributes to reasonable usage of resources and can avoid unnecessary efforts and investment.

Service Security and Technology

MSSP provide the better service security solutions and technologies such as firewalls, intrusion detection systems, virtual private networks, and vulnerability assessment tools. They are most effective because they are managed and looked by skilled security professionals. Product's that are developed by the MSSP and used in the services of client organization increase the level of security.

Drawbacks

Dependence

By using MSS, the organization becomes operationally dependent on the MSSP. This dependence on an outside company for operation can cause a great harm to the business of the firm and may affect the business viability. One approach to minimize dependence is to outsource to multiple providers, but this comes with additional cost and management with additional responsibilities.

Ownership

Although security is outsourced, the company still has the responsibility to protect its assets and its infrastructure. The client has to retain a sufficient level of competency to fulfil this responsibility (and train its people if necessary) and must sure that contractual and service level agreement language supports this.

Shared Environment

The MSSPs generally use the same shared operational environment to provide the services to its many clients, which can constitute a big risk because different clients might access the critical data of each others if the environment is not properly secured. This shared processing environment (such as a general purpose server) among multiple clients could make the organization's sensitive data unsecured.

Implementation

The implementation of a managed security services relationship in an organization may include movement of people, and computer infrastructure (like complex processes, hardware, software etc) and other different type of assets from the client to the provider or from one provider to another. These transitions could introduce risks for the company. The implementation might also require the introduction of new interfaces, new approaches, and important changes.

Control of infrastructures

The control of the infrastructure goes to hand of outsider or security provider so, granting control of infrastructures and applications to an outside provider have great deal toward a significant risk for CIO's and MIS directors.

Unreliability:

The company needs data at real time to make decisions and a little down falling can cause a great harm on the performance of the company as well as to compete with others. If the provider of the security services fails to provide the reliable data then it is possible to delay in the company decision so, as a result the company can lose their great number of customers, so the IT staff will be held responsible for this. This is basic reason that most of companies are hesitant to hire the security services from outside. Nowadays the MSP model is used by most of the companies (customers) to retain control of their networks and data centres to maintain and improve the overall security of their firms, so many corporation can save their critical information.

Legal Issues

Outsourcing with MSS doesn't mean that the organization will be completely free from liability in security incidents, especially when both parties are involved. Hence, there is need to consider legal issues, so it is important that an organization and an MSSP evaluate and discuss legal issues that could arise at any time in an organization during a security incident. Parties must understand the legal frameworks of each others.

Part IV: Future Steps

Introduction

Once Ericsson decides to outsource from Symantec, the following five phases should be done by Ericsson in order to outsource: The Request for Proposal (RFP) phase, the Evaluation of MSS Proposal, the Contract Phase, Service Level Agreement (SLA) and finally the Transition phase. In this way, the outsourcing process will be managed and implemented in a smooth way. We will introduce the four phases respectively in more detail in the following sections.

Request for Proposal

Request for Proposal (RFP) is a proposal of Ericsson's requirements that need to be submitted between Ericsson and Symantec as Managed Security Service Provider (MSSP). In the RFP, all Ericsson requirements need to be listed to ensure full information security. The MSSP should be asked to propose alternatives in case some of the requirement cannot be fulfilled.

Ericsson requirements:

Site availability
Server's accessibility
Software Integrity
Data confidentiality
Content filtering – spam, viruses, web contents...
Virus protection
VPN
Comprehensive reports of the MSS status
Reports of all vulnerabilities in the system
Monitoring the system
Security policies, procedures and regulations

Implementation of MSS must be applied regarding the Ericsson's security policies. Implementing Symantec's MSS, Ericsson needs to **reduce risk** (providing constant surveillance of attacks, malicious code and vulnerabilities), **minimize business impact** (helping to reduce the effect of system downtime, productivity loss and information loss), **improve security posture and compliance** (providing 24x7 advanced monitoring and applying best practice device management to improve security), and **reduce cost**.

Evaluating an MSS Proposal

When the RFP is sent to the provider the provider is in the position to answer the client's requests and prove that is the right one for the job. The provider shall prove that he has adequate resources and experience so as to ensure a high quality and continuous level of service.

More detailed, the client will be informed about the provider's strategy, reputation, experience, financial condition, skilled personnel and information concerning tiered services concerning delivery service, tiered provider's access to the client and liability issues. An evaluation is carried out to judge the level of trust that the client can have to the provider, their responsiveness and quality of service. Ericsson will therefore be fully informed concerning the provider's practices and policies and will be able to evaluate the proposal.

The points that the provider should answer in detail are:

- Confidentiality issues concerning clients private data
- Qualitative or quantitative aspect of the evaluation
- Providers strategies, reputation, experiences and financial overview

- Presentation of tiered providers if any, presentation of their interaction with the client and liability issues
- Contract termination conditions
- Providers communication methods with the client, how the cooperation will work
- Assessment of provider's responsiveness and quality of service, proving the level of trust the client can have and subsequent improvements to clients business.
- Discussion on the evaluation management plan, people assigned to the project, management issues and responsibility issues.

While conducting the evaluation the client should be careful for

- Request an evaluation form a third party or check current reviews.
- The provider should be requested to present references from other clients
- Conduct on site visits to understand and monitor the process
- Service delivery issues and delays.

All these issues should be discussed and documented during the evaluation period. In detail the following documents will be produced

- A Signed Request for Proposal focusing on contractual services
- An Executive Summary
- A Corporate Overview
- The Technical Approach of the implementation and
- The Cost Proposal

An evaluation of the MSS proposal will result in more information concerning Symantec's MSS and the decision if its MSS solution is suitable for Ericsson. It will also prove the adequacy of Symantec and if they can handle Ericsson's systems. Furthermore, the evaluation will prove if the MSSP has high quality support and knowledge to meet the requirements which are mentioned in the RFP. This evaluation is required because it will show whether or not the provider has enough resources and the required experience to ensure high quality services. In the SLA (Service Level Agreement) that follows next, the minimal requirements that Symantec needs to implement will be introduced.

Contract Phase

Whenever two organizations decide to cooperate in a business deal a contract agreement should be signed. This agreement should be based on some common ground found during a discussion. For the cooperation to be successful both parties should have an understanding of their rights, obligations and other responsibilities. By this way disputes are minimized. First the client point of contract (identified in the RFP) and the provider point of contract (identified in the proposal) should be identified which will in result serve as the primary interface between the two organizations. Nothing should be left vague and open to different interpretations. Because this is not a "typical procurement" contract and security is more like a complex process than a product or service, it is of decisive importance that Ericsson security experts should be present and active during all phases of negotiations. When the contract phase is concluded the implementation phase is ready to begin.

Service Level Agreement

The Service Level Agreement (SLA) is an agreement between the client (Ericsson) and the MSS provider (Symantec). The SLA specifies the performance standard and service quality that Symantec needs to provide to Ericsson.

Its purpose is to:

- clarify the working practices for provisioning of performance and maintenance
- set measurement points for services provided by Symantec
- set actions that Symantec will require from participants in order to meet the agreed levels of service

The SLA will be reviewed once per year and then will be discussed about the extension of the agreement. Factors that will be considered at the revision are stability of managed system, system performance, validity of performance measures.

Requested Services

Services that Symantec need to provide to Ericsson:

- **Firewall Service** – monitoring and management of firewalls. Symantec needs to provide continuous real-time analysis of data, VPN modification/configuration, rule changes, and to be liable for firewalls configurations.
- **Intrusion Detection Service** – monitoring of network and management of IDS system. Symantec needs to provide continuous real-time analysis of data and to be liable for management of IDS configuration.
- **Vulnerability Assessment Service** – scanning and testing of Ericsson's network and its servers (mail server, DNS server ...) for vulnerabilities. Symantec needs to inform Ericsson when the scanning and testing will be held. Symantec MUST have an approval for each vulnerability assessment by Ericsson. After each assessment, Symantec must provide reports to Ericsson.
- **Virus Protection Service** – protection against viruses, spam and unwanted web contents. The protection must be 24/7. Symantec need to provide daily updates and keep Virus Protection System up-to-date.

Service Level Management

Symantec will provide monitoring and management of implemented MSS. Symantec need to document how monitoring and management of MSS will be done, and how the effectiveness of implemented MSS will be measured and tracked. All reports generated by implemented services and reports of performance and effectiveness of Ericsson's system, should be provided to Ericsson. If Symantec needs to implement a new service or change a present one, Symantec needs to inform Ericsson and get approval for the implementation/changes. Ericsson will consider all Symantec's requests, and based on Ericsson's information security and policies, Ericsson will approve or will not approve the implementation of the new service or changes of present service. All reports received from Symantec will be considered in an annual review and based on that reports, effectiveness and efficiency of MSS will be assessed. The extension of the agreement will depend on the results given on annual review. If Symantec has any disputes, disagree with Ericsson's decisions or have any problem with the implementation of MSS, Symantec and Ericsson need to arrange meetings and find another way to solve problems.

Roles and Responsibilities

Ericsson will take responsibilities for the network infrastructure (cables, servers, hubs, and other hardware), software, employee’s mistakes (stealing information, erasing data …), and other non-Symantec related issues. Symantec will take responsibilities for monitoring and managing firewalls, intrusion detection/protection system management, virus protection service, content filtering service, remote access, and vulnerability assessment. Symantec also will be responsible for further systems updates/upgrades. Symantec will not have responsibilities for managing and monitoring of inaccessible parts of the network. For Vulnerability Assessment and other non-continuous real-time actions specified above in the document, Symantec needs to have Ericsson's approval for conducting actions. Also, Symantec needs to specify date and time when the actions will be taken.

Transition

When you decide to outsource, you have to transfer the current function of your in-house work to your providers. If Ericsson decides to outsource MSS to Symantec, it has to transfer its current security system infrastructure, hardware, software, company documents, even people to Symantec. Transition is a very important step in implementing an outsourcing process. If you ask any IT manager the keys to successful outsourcing, they are sure to mention at one point the importance of a smooth transition. The transition phase is designed to take the organization from its current business situation to where it wants to be. It involves people (human resource), process, hardware, software, and other assets of the organization from the client to the provider. For instance, sometimes outsource requires that the existing staff of the organization be transferred to the new vendor, but those staff who has been transferred may hold the intangible knowledge of their previous organization, so these people should be well looked after. Not only transitioning staff is a specialist skill, but also the transitions of other things. An outsource transition can bring to an organization impacts to all of its stakeholders, such as employees, users and support groups. The transition phase is also referred as the implementation phase. In order to gain a successful transition, we will talk about what have to be done in implementation activities and what are involved in an implementation plan.

Implementation Activities

Ericsson should define the requirement that the RFP (Request for Proposal) contains. Both Ericsson and Symantec should agree on the RFP (Request for Proposal) and SLA (Service Level Agreement). Ericsson and Symantec have to attend planning and resource allocation together. Symantec should take responsibility to technical infrastructure procurement and installation, system modifications, interface development. Ericsson may support Symantec with the conversion of client data from a previous service provider or from in-house systems, but authority and confidentiality should be ensured. Persons in Ericsson should be trained in order to get used to the new system. System testing and secure communications mechanisms should be done by Symantec. Before full transition occurs, a specified, continuous period of live service operation is required. Ericsson should also do a client acceptance test in order to make sure that its clients are satisfied with the new security system. And the specified documentation work should to be done for both parties.

Implementation Plan

In outsourcing MSS, the implementation plan describes "*how to effectively move from the execution of the MSS contract to full production use of the provider's managed services.*" It is challenging and high-risk. If an implementation plan is not well managed may cause overall break down in the organization, client inconvenience, client dissatisfaction and unexpected operational support costs and so on. The main spirit in implementation phase is "*to having plans and processes in place to handle the transition reduces rework and decreases the likelihood of client dissatisfaction and provider inability to perform services as expected*". We can see that defining a detailed, well managed implementation plan can help with gaining a successful outsourcing contract implementation to large extent. So in our case, both Ericsson and Symantec have to participate in creating the implementation plan. Each of them should indicate a point of contact with overall responsibility and authority for implementation activities of themselves. And during the implementation, both parties have to meet, preferably, once a week, to discuss and indicate the other party what is going on, the process, problems and so on.

The Implementation Plan should contain the following information

- Transition of people, process, hardware, software, and other assets should be done; both Ericsson and Symantec have to attend.
- Risk analyses, constraints
- Implementation process is described by both parties. It includes how managed security service systems are built and tested and whether this occurs in both a non-production and production environment; The anticipated client downtime for service installation (hours, days, how are scheduled, how impact is minimized) and if this can be scheduled at the client's convenience ;The existence of a trial period during which Symantec offers on-site or immediate on-call support ; Presence of back-doors into MSS systems and the use of modems for remote access administrative purposes; whether they are disconnected or disabled when not in use

- The detailed tasks of Symantec that specified in the contract
- When can Symantec make the whole system installed and got into use, trial period and so on?
- Time schedule of process
- Required resources (people, hardware, software, software licenses, other)
- Both parties assigned their responsibilities
- Transition of personnel, assets, software licenses, client data
- Service-level acceptance requirement (refer to Service Level Agreement)
- Ongoing review, reporting, and change management process definitions
- Satisfaction of business attributes, service attributes, and security practices including process definitions and how satisfaction is demonstrated
- Approaches for obtaining buy-in from client and provider stakeholders
- Contingency plans in the event that the contract is not fully implemented

Ericsson and Symantec should negotiate a timeframe for successful implementation. If the implementation has not been successfully completed in the discussed timeframe, Ericsson and Symantec can agree to extend the time or Ericsson can terminate the contract without any additional cost to Symantec. Both parties shall evaluate the implementation plan, process, status; agree on significant exceptions and document them. During implementing, Ericsson and Symantec try to find open issues, decide resolution and management responsibility to communicate and solve the issues, and they can decide a time for the resolution.

Concluding Remarks

We presented and discussed the steps that Ericsson should follow in order to evaluate Symantec's proposal. Furthermore the process that should be followed in the case that Ericsson accepts Symantec's offer has been introduced. When the final decision will be made the information presented here will be used as a brief guideline. Further information will be required to create the whole picture and lead to a fruitful cooperation.

Part V: Executive Summary

Today's IT world is no longer a peaceful environment like it used to be years ago. All companies are now continuously face to face with security issues; and 'securing' becomes a bigger challenge every day, especially for companies like Ericsson which are leaders in their business areas and have a complex structure.

Ericsson's core business segments are Systems, which includes mobile networks, fixed networks and professional services (managed services, consulting, system integration,…), Phones, which is joint with Sony (Sony-Ericsson) and other operations that constitute about 6% of the net sales. The Systems segment is by far the most valuable business of Ericsson and the mobile networks area constitute 80% of the sales within this segment. These core business segments, as well as Ericsson's own infrastructure, are completely dependant on the proper functioning of IT systems.

A large number of threats exist in the IT/IS environment. Malicious software like viruses, trojan horses, worms and many others are created and circulate on the Internet. Outsiders, including experienced hackers and script kiddies, are attacking systems every minute. On the other hand, insiders are probably the most dangerous ones, having already access and thus being difficult to detect. Ericsson has suffered from these in the past. Other threats could be exemplified as unauthorized physical access, lack in security awareness, power outrages, equipment failures and natural disasters. All of these are threats against the confidentiality, integrity and availability of Ericsson's IT systems. Since Ericsson is an industry providing services and solutions strongly connected with information technology, threats against IT/IS have direct impact on Ericsson's core business areas and its shareholder value.

With the increasing complexity and dynamism of IT systems, security becomes a difficult target that requires a high amount of resources and knowledge. Managed Security Services (MSS) steps in at this stage as a different systematic approach that we can briefly define as 'outsourcing security' to a Managed Security Services Provider (MSSP). The MSSP, typically a company whose main business area is IT security, will 'share' the risks of the company, help the company manage them with its deep knowledge, resources and experience in the field.

Building an MSS partnership is often a good choice to reduce or transfer information security risks. However, there are drawbacks and business risks as well as benefits involved in such cooperation, and both have to be taken into consideration before making the decision.

One of the main advantages of MSS is the extensive knowledge and professional experience of the MSSP. This security awareness, together with high technology equipments, specialized facilities and security experts, provides 7/24 management, monitoring and support. Moreover, MSSPs are aware of legal issues and are compliant with legislations and prosecution cases. Maybe one of the most important benefits is the reduction of the security-related costs, as the company will not have to recruit, hire and train many security personnel and manage all the systems. By outsourcing with MSS, the company will be able to focus on its strategic business goals, letting the provider focus on security.

On the other side, MSS has its risks and drawbacks, mainly because of the partnership dependence that will be created. However, Ericsson can minimize this dependence by including some of its internal staff for decision-making and active participation in the MSS process. One other risk comes from the shared environment used by the provider, so the security of this channel should be guaranteed. Also, the implementation process of MSS might be difficult and might require new approaches and changes in the system. This, however, is not a big issue if everything is clarified and agreed upon the contract.

MSS services differ from provider to provider. However, we can list some of the typical services as: constant monitoring, management and log analysis of security equipments like firewalls and intrusion detection systems, responding to emergencies, anti-virus and content filtering, data archiving and restoration, on-site consulting,… As we said, MSSPs have different characteristics, and offer different services, so the choice of the provider is not a trivial one. Hence, Ericsson has to consider different MSSPs and answer the following important questions beforehand for each of them:
Can we rely on the MSSP for the good of our business?
Does the MSSP have the necessary experience and competence level?

Does the MSSP offer all the services that we need?
Will we have enough support once we are a MSSP customer?
Is the MSSP compliant with international standards?

Symantec is one of the leaders in the IT security business, and one of the biggest MSS providers in the market. It provides both monitoring and management of security tools, and performs real-time threat analysis, keeping the customer constantly aware and allowing them to maintain complete insight into the critical business information. Symantec's MSS covers well the general services offered by MSS providers, and its reputation in the IT world makes it a trustworthy company to build partnership with. Hence, we believe that outsourcing MSS to Symantec is a good choice for Ericsson.

Implementing MSS is a critical and difficult process that requires a lot of preparation from Ericsson. First of all, we need to perform a business risk analysis to identify the most critical assets and define our needs and requirements, our 'expectations' from Symantec. These requirements will be stated in the Request for Proposal (RFP) and sent to Symantec, which will send us back their MSS Proposal. At this stage, an evaluation of the proposal will be performed by Ericsson to decide if Symantec's MSS is suitable for our needs. Once the suitability is confirmed, the Contract phase is conducted to establish the interface between the two parties. This will be followed by the establishment of the Service Level Agreement (SLA), specifying the limits of the MSS partnership: the performance standard and service quality that needs to be provided to Ericsson. Finally, the Transition phase will consist of transferring in-house systems to Symantec, and is the key step to a successful outsourcing. It is important that Ericsson representatives be present and active during all these steps to eliminate ambiguities and future problems that may arise from them, and to make the whole process successful.

During the previous parts of this report we had the chance to thoroughly investigate how IT interacts with our business interests and why security is of essence. Furthermore we presented MSS in detail and investigated its various aspects. To this we can add the crisis we faced during the last years and which were related to IT Security (spy and hacker case). It is obvious that we have to evolve in this domain. We strongly believe that outsourcing Managed Security Services would be beneficial for our corporation. The diversity and continuous evolution of IT security has as a result the need for continuous training of the IT staff and acquirement of specialized technological solutions. Today the cost for creating and retaining a specialized IT security team is very high. Furthermore if we take into account the size of our company (50000 staff in various locations around the globe) and the need for constant unhindered electronic communication (e-mail, Instant Messaging, VOIP telephony etc.) it becomes obvious that the cost for such an improvement is significant.

Having an outsider handle this critical area will save great amounts of money which we will be able to invest on other critical sections of our business. Outsourcing has time and again proven helpful to our business and is a current and future trend in corporate management. Our knowledge on outsourcing guarantees that we can construct an agreement beneficial to our interests. It should also be mentioned that Symantec is a leader in the area and has proven time and again that it can handle organizations like ours with great success. The most important thing in a cooperation like this is trust and Symantec has proven to be trustworthy. The solutions provided by Symantec are utilized by major financial organizations all over the world. Most of the key players today seem to trust Symantec. Of course we should not blindly place our trust to Symantec. If we need to measure "trust" we can study Symantec's certifications or hire a consultant to prepare a report on Symantec and her relationship with her clients. By cooperating with the leader in this business area we are guaranteed to receive the best services. The technology utilized for our security will be the most evolved and reliable in the industry. We will also benefit greatly in the domain of industry benchmarks and regulations (for example SOX) and manage to compete evenly with other leading corporations on business deals requiring such certification without investing a great deal of money. Furthermore the factor of time is important. If we engaged ourselves today in a complete evaluation of our IT security we would have to dedicate at least a couple of years in the process. By engaging ourselves in a deal with an MSSP we greatly save time by acquiring ready solutions to various problems. Time in business is always of essence in order to remain in the game and compete evenly with others. It is of great significance that this decision should have the backing of the whole corporation in order to succeed because only then can the required changes to our organization be made without interference. The backing and help of the directors of the company is of great importance. To conclude we would like to mention that since outsourcing MSS is a solution that can greatly --positively-influence our business, a solution that we should adopt for our benefits, there is no better entity to cooperate with than Symantec.

References

1) *“Ericsson outsourcing deal threatens 11,000 jobs worldwide”*, S. James , http://www.wsws.org/articles/2001/feb2001/eric-f01.shtml, 2006-4-10
2) *“Sweden’s Ericsson posts historic losses”*, S. James, http://www.wsws.org/articles/2002/feb2002/eric-f06.shtml, 2006-4-10
3) “*Ericsson Anual Report 2005”*, Ericsson, http://www.ericsson.com/ericsson/investors/financial_reports/2005/annual05/summary_downloads/ar2005_en.pdf, 2006-4-10
4) *“Ericsson Fourth Quarter Report 2006”*, Ericsson, http://www.ericsson.com/ericsson/investors/financial_reports/2005/12month05-en.pdf, 2006-4-10
5) *“Enterprise Security Assessments”*, Verisign, http://www.verisign.com/products-services/security-services/security-consulting/services/security-assessment/index.html, 2006-4-103)
http://www.verisign.com/products-services/security-services/security-consulting/services/security-assessment/index.html
6) “*Hungarian man charged with hacking Sony Ericsson site*”, J. Bostrom, http://www.infoworld.com/article/05/03/08/HNsonyhack_1.html, 2006-4-10
7) “*Managing Information Security Risks*”, C. Alberts, A.Dorofee, Addison-Wesley, 2002
8) *“Symantec™ Managed Integrated Security Appliance Services”*, Symantec, http://enterprisesecurity.symantec.com/Content/displaypdf.cfm?pdfid=668, 2006-4-10
9) *“Corporate News Archive”*, Symantec, http://www.symantec.com/about/news/release/corporate.jsp, 2006-4-10
10) “*Outsourcing Managed Security Services*”, J. Allena, D Gabbard, C. May, http://www.cert.org/security-improvement/modules/omss/index.html, 2006-4-10
11) *“Benefits of Engaging an MSS Provider”*, FarPost, http://www.farpost.com/it/benefits-mss-provider.php, 2006-4-10
12) “*Securing Critical Information Assets: A Business Case for Managed Security Services”*, CGI Group, http://www.cgi.com/cgi/pdf/cgi_whpr_50_mss_e.pdf, 2006-4-10
13) *“How to outsource Part 3 : A Smooth Transition”*, Syntelligence Volume 2 Number 9 http://www.syntelinc.com/syntelligence/index.aspx?id=208, 2006-4-10
14) *“Outsourcing protection: the search for the right MSSP”*, ENA, http://www.networksasia.net/ena/article/articleDetail.jsp?id=185137, 2006-4-10
15) *“Technology Overview - Symantec Managed Security Services*”, Symantec, http://www.symantec.com/about/news/resources/press_kits/securityintelligence/media/MSS-TechOV.pdf, 2006-4-10
16) *“Managed Security Services”*, Symantec, https://www.enterprisesecurity.symantec.com/content/displaypdf.cfm?ssspdfid=50&EID=0, 2006-4-10
17) *“Establishing Service Level Agreements”*, Karten Associates, http://www.nkarten.com/sla.html, 2006-4-10
18) *“Real-Time Managed Security Services”*, Symantec, http://enterprisesecurity.symantec.com/SecurityServices/content.cfm?articleid=1520, 2006-4-10