The Emerald Research Register for this journal is available at
www.emeraldinsight.com/researchregister

The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

E-enterprise security management life cycle

Stephen C. Shih
Department of Information Management Systems, College of Applied Sciences and Arts, Southern Illinois University, Carbondale, Illinois, USA, and
H. Joseph Wen
Department of Accounting and Management Information Systems, Harrison College of Business, Southeast Missouri State University, Cape Girardeau, Missouri, USA

Abstract

Purpose – One of the purposes of this paper is to discuss special security concerns and new challenges at front-end e-business and back-end supply chain operations. An e-enterprise security management life cycle (eSMLC) is then proposed to ensure the unification and congruity of e-enterprise security management.

Design/methodology/approach – To demonstrate the practicality of the eSMLC, a case study is presented to depict the application and implementation of the methodology at a leading US heating, ventilating, and air-conditioning manufacturing company.

Findings – The case study substantiates that the eSMLC methodology can be employed as a unified mechanism to provide central, cohesive control and global visibility. It helps security professionals in the company develop practical steps and sustainable solutions for tackling the unique security challenges arising in an open, unbounded e-enterprise environment.

Practical implications – Implementing eSMLC can help the security specialists focus on different critical security management jobs in a sequential but interrelated and logical manner. Through the use of eSMLC, in-depth understanding of the potential environmental risks can be properly acquired. The methodology also helps managers perform a proactive analysis of the consequences of security breaches in relation to risks.

Originality/value – The proposed eSMLC methodology provides a viable foundation for building a secure and manageable computing environment using a recommended set of solutions, processes, procedures, and technologies. eSMLC methodology renders a unified, structured framework which helps develop an actual security plan and solutions and/or improve currently used security standards, practices, and configurations in response to special security requirements and long-term e-business needs.

Keywords Electronic commerce, Data security, Supply chain management

Paper type Case study

Introduction

According to the statistical study on web defacement (Computer Economics, 2002), just in the year 2001 alone, it is estimated that the worldwide impact of malicious virus code was $13.2 billion. Among those, the largest contributors are SirCam at $1.15 billion, Code Red at $2.62 billion, and NIMDA at $635 million. On September 18, 2001 alone, there were more than 86,000 internet hosts (about 42.97 percent of those hosts resided in the USA) being compromised and used as a vehicle to promulgate the NIMDA worm (SANS, 2001). Anther eye-catching incident of web security attacks is exemplified by

Information Management & Computer Security
Vol. 13 No. 2, 2005
pp. 121-134

0968-5227
DOI 10.1108/09685220510589307

the exploitation of the vulnerability in Microsoft's IIS web server product (CERT, 2002). Over 250,000 web sites were compromised by the "Code Red" worm, in the course of a nine-hour period. As a more recent example, on August 16, 2003, an infamously mass e-mail worm, named Sobig.F, launched a ferocious invasion around the world attempting to download files from the internet and potentially leave computers vulnerable to further attack. Sobig.F is recognized as a new strain of one of the most virulent e-mail viruses that can spread quickly worldwide. In particular, it attacks Windows users via e-mail and file-sharing networks. In addition, this formidable virus deposits a Trojan horse to create a hacker back door for turning victims' computers into senders of spam e-mail. As to the damages caused by Sobig.F, we have seen a pretty frightening statistic. Only ten days after the outbreak, it was estimated that more than 500,000 computers running the latest version of Microsoft Windows were infected. During the month of August, 2003, North American companies alone suffered an estimated $1.3 billion in damage, not including wasted productivity, from fighting off the Sobog.F worm. The estimates do not account for numerous small businesses which have been hurt by this vicious virus.

Widespread security threats may totally devastate an organization's bottom line. Any compromise of the organization's assets, either in terms of loss, tampering, or sabotage of the systems, can be extremely destructive and costly. For instance, in a bi-annual report (UKDTI, 2002) on information security breaches in the UK, Price Waterhouse Coopers found some astonishing facts: the average cost of a serious security incident was £30,000 (approximately US $50,000) and several of those surveyed had single incident costs which were greater than £500,000 (about US$825,000). Omni Consulting Group, of Davis California (INL, 2001) surveyed 3,000 companies and the results showed that security gaps cost the companies between 5.7 and 7 percent of their annual revenue. According to another study (ZDNet, 2001) released by the American Society for Industrial Security and consulting firm PricewaterhouseCoopers, *Fortune* 1,000 companies lost more than $45 billion from security breaches of proprietary information in 1999. The majority of those hacking incidents hit tech companies, with nearly 67 individual attacks and the average theft ringing up about $15 million in losses. Headlines of such reported security incidents just go on and on.

Security concerns of front-end e-enterprise operations

Doing business on the web or performing online trading is still in its infancy (Clarke, 1997). The potential of using the web as a business-to-business (B2B) or business-to-consumer (B2C) commercial medium has been widely explored. However, a critical assessment of its B2B or B2C e-commerce challenges and issues has just started to receive attention. The new economy of ubiquitous e-commerce usually introduces new risks (Clarke, 2001). In particular, one of the factors that contributes to the rise in e-business-related security incidents is the "trusted" business partnership. Business partners in a B2B partner chain can have access to highly confidential back-end resources and information. Consequently, the security challenge migrates from securing of network to protecting the virtual network. The complexities of these B2B partnerships and relationships are often very onerous and intricate.

As more organizations are migrating to an e-business model, it is realized that the single most important initiative is security for web or e-commerce operations. Securing

e-business operations is now the number one priority on the list. According to a survey on e-business-related security issues (IS, 2000), it is revealed that the frequency of security attacks, incidents and breaches is far higher for companies that conduct e-commerce (so called EC organizations) than for those that do not (non EC organizations). For instance, EC organizations are more than twice as likely to get hit with web server-related hacks and 35 percent more likely to be the target of denial-of-service attacks. Other e-business-related security statistics show that 23 percent of survey respondents indicated that they were suffering from unauthorized access or misuse within the last 12 months. Further, other statistics demonstrate the seriousness of increasing security problems on the web: 90 percent of those web sites attacked reported vandalism in 2001 (as opposed to 64 percent in 2000), 78 percent reported denial-of-service in 2001 (only 60 percent in 2000), and 13 percent reported theft of business transactions in 2001 (compared to 8 percent in 2000).

Security concerns of back-end supply chain operations

The large number of business applications and databases being deployed for intranets and extranets in a supply chain continues to grow rapidly. However, with the same distributed nature as that of an internet-based system, an intranet- or extranet-driven supply chain network is always a conspicuous target of security attacks. Doing business via a web-enabled supply chain network can open the possibilities to some significant security threats. For instance, financial transactions may be interrupted or misdirected by the hackers or crackers. Collaborative supply chain information may introduce the opportunity of revealing sensitive intellectual property to competitors. Logistics information can be illegally used to disrupt normal transportation operations. Attackers can break into an organization's or its partner's supply chain infrastructure and may disrupt or totally paralyze its business operations and functions.

In the wake of the September 11 terrorist attacks, supply chain security has taken on a whole new meaning among information systems, security, and logistics professionals. Thwarting cargo theft and securing computer systems against hackers were long the security focuses prior to the 9-11 incident. Supply chain security has now involved attacks via global supply chain networks. The companies are now forced to reassess their security management model, infrastructure and policies that were already in place and to evaluate if they should be strengthened or redesigned. Information systems and logistics experts have to work together to confront this reality immediately. The US Customs Initiative on Supply Chain Security or Customs Trade Partnership Against Terrorism (C-TPAT) has already been implemented. Eventually the scheme will cover the entire supply chain of the importers that includes manufacturers, suppliers, suppliers' vendors, contractors and sub-contractors, warehouse providers, as well as air, sea and land carriers (C-TPAT, 2002). C-TPAT provides guidelines on security recommendations for manufacturers, importers, brokers, air carriers, land carriers and sea carriers. For manufacturers and importers, for example, these recommendations cover physical security, access controls, procedural security, personnel security manifest procedures, conveyance security and education and training awareness.

The stakes can be extraordinarily high from serious security attacks on the supply chain network. Accordingly, when companies are reaching out to each other via the web-based supply chain network, the security should be properly controlled and

managed beyond just perimeter protection. It is also recommended that companies should add on the C-TPAT recommendations as soon as possible so that they can start documenting processes for future compliance assessments. In particular, to protect the communications among business partners effectively, companies need to secure information as it flows between organizations and allow authorized users to access selected applications, specific transactions, and appropriate data sources. Simply stated, security for the supply chain must provide encryption to ensure data integrity and protection end-to-end across wired and wireless links; mutual authentication to prove the parties are who they claim to be; and precise access controls to enable authorized access to specific resources and create an audit trail.

The recent proliferation of wireless communications has elevated the security stakes further. This phenomenon has made its way firmly into the supply chain applications, such as wireless logistics and warehousing implementations, wireless financial transactions, and sales force automation using personal digital assistants (PDAs) and other mobile devices. The inherent strengths of wireless access in a supply chain are also the source of its biggest vulnerabilities. Mobility is a clear benefit that wireless communications brings to supply chain communications. However, it can result in great network exposure and rogue access. Unlike hard-wired systems, unauthorized listeners can easily compromise or tamper with data transmitted over wireless media without having to gain physical access to the network infrastructure. All things considered, this means that the requirements for a complete supply chain security solution must also include the protection of users and resources, whether wired or wireless, as funds are electronically transferred, on-line trades are made, and sensitive business information is shared between collaborative partners.

Business assumptions and security management practices

It is realized that there have been dramatic changes in the nature of security problems, in both technical and business contexts (Lipson and Fisher, 1999). Many business assumptions underlying conventional security solutions and practices may no longer be valid. If the depth and breath of these compounding changes are not recognized, an effective solution to modern security problems for web-based, distributed organizational systems cannot be realized. Traditionally, security concerns have been focused exclusively on privacy or confidentiality of critical organizational data. Nevertheless, the commercial viability of modern businesses depends on their ability to create and deliver their products/services in a continuous and timely manner. As a result, the issue for continuity or availability of mission-critical services and operations among the company, suppliers, third-party infrastructure providers and customers has led to a whole new field of security needs.

The traditional business assumptions may have been appropriate when organizational systems were closed and isolated islands with high degree of controlled interfaces to the other systems. In this electronic age, more and more organizational systems are open and distributed. Lack of central administrative control and management and absence of global visibility are the characteristics of the internet-based and distributed systems. Therefore, without a unified mechanism for providing central, cohesive control and global visibility, these open, unbounded systems will not be compatible with the assumptions underlying the present security requirements.

Most security solutions and technologies derive from a fortress model (Lipson and Fisher, 1999). In such a model, there is a clear distinction between the trusted insiders and other potential system users and intruders. However, in the highly distributed, internet-based enterprise systems, there is little distinction between the insiders and outsiders. Everyone connects to the internet in a supply chain is virtually considered an insider, whether or not they are known to a particular system.

E-enterprise security management life cycle

For developing a truly unified e-enterprise security management life cycle (eSMLC), an emerging discipline, survivability (Lipson and Fisher, 1999), is adopted to coalesce web security with risk management for protecting highly distributed enterprise systems and critical organizational assets from being compromised and affecting the availability of vital operations. Survivability has been defined as the capability of a system to fulfill its critical mission, in a timely manner, in the presence of attacks, failures, or accidents (Ellison *et al.*, 1999). The eSMLC is considered as an emergent property (Cottrel, 1977; Fisher and Lipson, 1999; Hinton, 1997) which portrays a notion that an end-to-end security control cannot be achieved at the level of atomic model components since each component corresponds to a single point of failure for its own survival. In other words, the creation of a reliable security control and management model from atomic components may be less reliable than the composite model. As a result, a holistic approach is embraced to ensure the unification and congruity of the new security management model. Additionally, an engineering approach (Burstein, 1999; Avison and Fitzgerald, 1991), along with other guidelines (Galliers, 1992; Iivari *et al.*, 1998; Nunamaker *et al.*, 1991), is adopted to perform the tasks undertaken in the development of the e-enterprise security management model. In sum, the entire research work is made up of five major tasks:

(1) Establishment of a baseline model.

(2) Development of a visual security scenario simulation model and decision support system.

(3) Development of a security information systems architecture.

(4) Demonstration and validation.

(5) Implementation and deployment.

These major tasks, with associated milestones and phases, are shown in Figure 1.

Task 1 – baseline model establishment

In the first task, emphasis is placed on the development of a baseline model to ensure that the identified security concerns and issues are properly addressed. Specifically, this task is composed of three important steps: field research; security requirements definition and baseline development; and emerging security solutions evaluation.

Field research. As an indispensable requirement, necessary inputs should first be gathered and analyzed for constructing a solid baseline model via field research. Throughout the entire lifecycle, a security steering committee should be formed to perform project management and progress monitoring, give advice and guidance, and conduct feasibility analyses at appropriate checking points. In addition, all the data

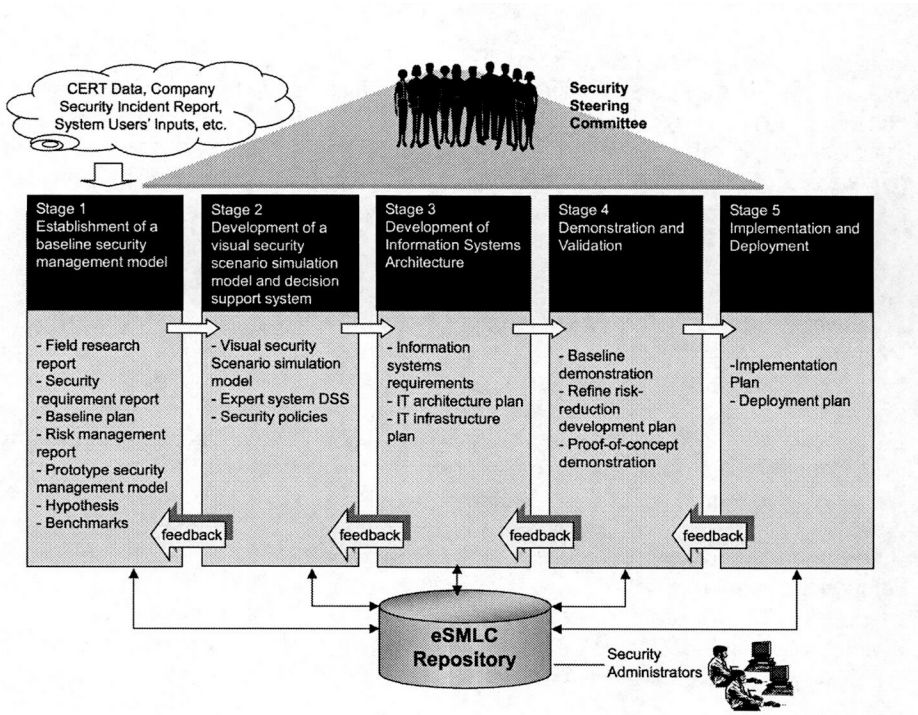

Figure 1.
E-enterprise security management life cycle

and information pertinent to security management activities should be properly stored in the repository and managed by the security administrators.

Security requirements definition and baseline establishment. As an important groundwork for building a baseline model, the first effort is to conduct investigation of the current security models and practices as well as their supply chain coordination and e-business operations. Identified security risks should be further assessed in performing web-based supply chain and e-business operations via the collaborative innovation (CI) process (Amidon, 2002). The CI process has been developed at United Technologies Research Center as an integrated collection of best-practice design methods, enhanced and simplified to support integrated product development (IPD) teams during conceptual design (Zeidner and Wood, 2000). In sum, the primary objectives of this effort include:

- creating an explicit baseline of the intended enterprise-level security model;
- generating alternatives to the baseline, evaluating the value each alternative can offer, and selecting the highest-valued candidate for development;
- analyzing the potential obstacles inherent in each alternative and identifying a development plan that will reduce these risks as rapidly as possible by segregating risk-reduction tasks; and
- ensuring that key decision points, technical risks, and modeling and prototyping goals are thoroughly understood.

The CI requirements definition effort will result in a set of alternative security management solutions, value for each solution, risks associated with elements of each

solution, and in turn a detailed risk reduction plan for each solution. As a key milestone under Task 1, a detailed functional requirements document for the proposed security model along with a baseline statement is developed. This document consists of the formulation of essential model functions, assessment of dependencies among various model components, evaluation of alternative solution models, and estimation of value and risk associated with each alternative solution model. As a supplementary effort, part of this task is to evaluate the effectiveness of many real-life security management practices and supply chain security standards in practice. A number of prototype models are developed to perform the benchmarking of these business practices and evaluate the hypotheses.

Evaluation of emerging security solutions and technologies. Another important step of this task is to evaluate a number of state-of-the-art security solutions and technologies. Along the line, a plan of integrating the state-of-the-art security solutions into the entire security model is also developed. As a general guideline, the security solutions should be developed around an open industry standard and be highly scalable, fully manageable, and extremely resilient.

Task 2 – development and experimentation of security scenario simulation models

To ensure a concrete understanding and proper assessment of the developed model, a test-bed environment is created to drive the "what-if" scenario analyses and incident response testing for e-business and supply chain coordinative operations in the presence of intentional and unintentional security threats against predefined security measures and objectives. A security scenario simulation model and an expert system (ES)-based decision support system are constructed to reflect the generic natures of the underlying security problems. First, critical security equipment, personnel, network and system access points, security procedures and logistics associated with the facility are thoroughly reviewed. Second, a series of scenarios are developed to test the security requirements of different segmental entities (computers, local networks, private networks, public networks, etc.) to help isolate and identify the security issues, possible attacks, data vulnerability, and associated security requirements. Third, attainable solutions are identified to address specific requirements (specified assurance levels, security services, etc.) for each entity in various B2B or B2C interaction scenarios and supply chain cooperative operations. Finally, milestones are evaluated to convert current security models and policies of the investigated companies into a unified security control and management model.

Task 3 – development of security information system architecture

As an integral component, Task 3 involves identifying information systems (IS) requirements and developing an IS architecture to support maximum availability, scalability, manageability and performance of the proposed model. As a general guideline, several IS architectural capabilities are required to ensure a secure e-business computing and communications environment. First, a common infrastructure is necessary for allowing diverse e-enterprise applications to share a common authentication, authorization and administration infrastructure as well as providing flexibility in deploying a single security infrastructure. Second, only a single point of entry and single sign on is allowed to web 4 content, applications, and databases. Third, the information system architecture should support synchronous and asynchronous

communications among system and network components. Fourth, the architecture should be open in order to support multiple computer languages, database applications, and operating systems. Fifth, the architecture should be platform independent for delivering consistent security capabilities across a range of platforms. Finally, an efficient and flexible way of transporting data and messages should be available between web applications in a heterogeneous and homogeneous environment.

A holistic approach is adopted to balance all the high-performance system requirements for sustaining an end-to-end security solution to the rigorous requirements of the web-based operations. The inherent complexity of high fidelity web-based enterprise security modeling is also addressed through the use of hierarchical models (Riesenhuber and Dayan, 1997) and revision management method. In these hierarchical models, some components are aggregates of large numbers of similar components. Other sub-models may be defined as a heterogeneous collection of interacting processes representing a natural decomposition of the overall domain. Still others may be provided as "black boxes" whose contents may not be examined or modified. These black-box components will be incorporated into the model via "wrappers" code that provides standardized interfaces. An open standard, such as Common Object Request Broker Architecture (CORBA) (Zahavi, 2000), is used to integrate these components as easily as possible.

Furthermore, the complexity and size of useful models require that they are executed via parallel processing, which can be achieved in an existing networked computing environment. To insure robust execution in this environment, a virtual processor paradigm (Grossberg, 1997) is used for allowing model elements assigned to one processor to be transferred or restarted on another processor. Each model component can be assigned to one of these virtual processors and communication can be managed via a software bus localized within the domain of the parent model.

Task 4 – demonstration and validation

A baseline demonstration and a proof-of-concept demonstration are conducted focusing on the feasibility analysis of the developed model. Several key components of the model, including risk assessment, survivability analysis, and security policy enforcement, are also demonstrated and validated in this effort. This demonstration and validation task represents a key decision point for determining whether the top line security goals can be reached. Specifically, the method of validating the developed model and results are depicted in the following paragraphs.

Method of validating the security model and research results. Systematic validation and analysis of the research results is an essential step of a successful modeling. To ensure the validity of the developed security model, a validating process is performed to examine if the model correctly represents the underlying aspects of the e-enterprise environment within the real-life context. Two important perspectives of model validity are addressed in the validating process. First, the model is assessed to verify whether it is built in line with the requirements and performance criteria established during the requirements definition stage – and, further, examine if it is a viable representation of the real-life system. Second, the model is validated to determine that it is traceable to system user requirements and fully addresses the system users' intent.

To conduct a successful modeling validation process, validation criteria are first specified to facilitate fully understanding of a successful implementation. The

modeling assumptions are assessed to test various parameters identified in the model. Statistical tests (e.g. goodness-of-fit tests) are performed on all inputs and internal processes. In addition, a continuity test (COT, 2002) is conducted to investigate how changes in the model parameters impinge on the model output. Furthermore, a test of degeneracy (Kleijnen, 1974) is performed to examine how the removal of a certain portion of the model affects the behavior of the systems.

Case study – web e-service security management

This section presents a case study illustrating the application of eSMLC methodology to a unified, end-to-end security management for the e-service operations at HVAC Inc., a leading US company in manufacturing heating, ventilating, and air conditioning products. The scope of this case study is confined to the implementation of eSMLC to the company's service operations in its North America region. The implementation was driven by a security management steeling team made up of e-service system users in the Division of Global Services as well as security engineers in the research center.

Company background

With its headquarters in the East Coast of USA, the company of investigation has over 45,000 employees in over 150 countries. The company manufactures air conditioning and heating products for homes, commercial offices as well as makes industrial heating and cooling systems for business office and school buildings. In addition, it is one of the leading US manufacturers that offers commercial refrigeration and transport refrigeration systems, including truck, trailer and container refrigeration equipment as well as transport air conditioning systems for the bus, rail, and marine industries. In total, the company generates approximately $8.9 billion in annual revenue.

As to its supply and service chain infrastructure, the company has a worldwide network of hundreds of distributors and thousands of dealers who sell, install, and service its products in over 150 countries. In addition, the company designs and manufactures its HVAC products in 20 engineering centers and over 100 plants spread across six continents.

Company's e-business initiatives

Recently, one of the major e-business initiatives of the company was to deploy the web-enabled "e-service" (electronic service) system (see Figure 2) to improve productivity and customer services, specifically for its 90 field service offices in the USA and Canada. The e-service systems have provided a powerful enabler to track customers, jobsites, equipment, parts, tools, and service contracts. With the system, office supervisors can effectively perform the assignment of maintenance tasks at a real-time mode and to track the progress of those tasks via the company's intranet. With tight integration of its SAP enterprise resource planning system, the system allows supervisors to track and manage necessary parts, components, tools, and transportation vehicles on a real-time basis via the web.

The e-service systems have dramatically improved efficiency of the company's B2B e-commerce operations. Customers, dealers, and suppliers are able to deal with the company through both private and semi-private exchanges via the company's web-based supply and customer management networks. Its supply management network is a worldwide federation of over 600 stores that constitute the world's largest

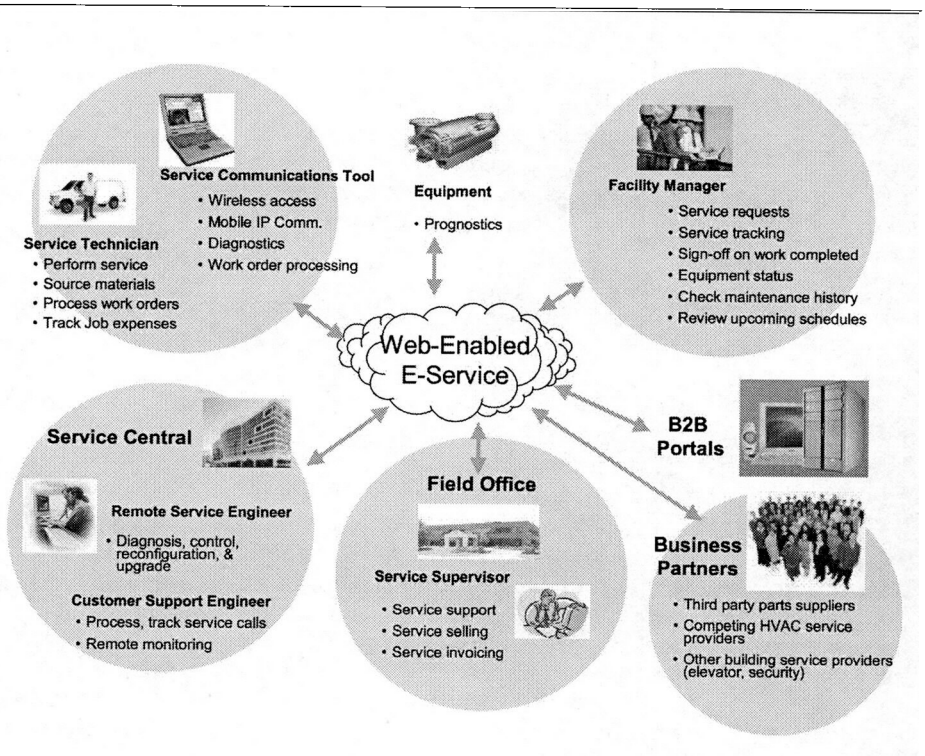

Figure 2.
E-service system

heating, ventilating, air conditioning and refrigeration supplies organization. This B2B site is the true "one-stop online store" for parts and supplies in the industry. Under the centralized management of the company's component replacement center, suppliers, dealers, and customers can gain access to an electronic information catalog of over 100,000 parts.

In B2B e-commerce, wireless connectivity has been recognized by the company to have great potential to revolutionize the HVAC businesses fundamentally – just like the internet. Recent data show that the availability of wireless solutions for mobilizing web-enabled e-commerce applications and the growing number of mobile users (mostly field service technicians) in the company have been triggering wide exploitation of wireless web. With the marriage of internet and telecommunications technologies, both HVAC employees and its business partners are able to access the web from a greater variety of devices, including personal computers and mobile devices such as PDAs, cellular telephones and enhanced pagers. Along the line, a full-scale deployment of mobilized web-driven applications and services is becoming one of the spotlights in the company.

Security concerns in the company's e-service B2B interactions

The company is competing globally to provide access to its critical enterprise information to boost productivity and operational efficiency and to deliver services quickly and satisfactorily – all at the lowest possible cost. The ability to communicate and collaborate with partners, suppliers, customers, and employees anytime and anywhere is now a requirement at the center stage. As a result, deploying the e-service

system is the heart of the company's e-business initiatives for effective B2B e-commerce. While implementing and deploying the system, various concerns have surfaced confronting the system's end-users, including the field service managers and the company's business partners. Among all the concerns raging about the e-service system, security ranks the highest according to a survey conducted with a sample of the company's service offices in North America. The survey revealed that a majority of the office managers were very concerned about security issues in the developing and deploying e-business environment due to many reported incidents in the past.

The advent and acceptance of wireless computing and internet technologies have changed the way the company's information is stored, accessed, and shared. With the e-service system, the company is able to implement a more open and distributed information sharing model for the purpose of leveraging the power of collaboration and network connectivity as well as enabling closer relations and communications with its customers and partners. The company has increasingly opened its networks to business partners and customers via the e-service system. E-business technology is indeed opening up tremendous competitive advantages and opportunities for the company. Unfortunately, this also makes the company far more vulnerable than ever before to security attacks. After working to connect the company's systems more tightly with those of its business partners via the web, the company now realizes that the dangers of attacks by intruders has become increasingly significant, and the scale of potential damage also rises in magnitude. Mobile workers in particular can be vulnerable, as hackers set off attacks through wireless communications channels against the company's and its business partners' networks.

The need for a unified security management method

Security has become an essential part of planning, implementing, and managing the e-service system. Nevertheless, the security issue that HVAC faces is multi-faceted. First, with wide deployment of distributed client/server and web-enabled networks, the company finds it much more difficult and laborious to effectively safeguard its critical networks, applications, and data. Second, the need to connect and collaborate with its partners, suppliers, customers, and employees anytime and anywhere has dramatically increased the complexity of managing network and systems security. Third, field service technicians not only work from branch offices, but also from the service sites, or from the road. Managing access policies for remote connectivity requires great flexibility to apply proper security policies to different types of connectivity. Finally, security in B2B e-commerce environments involves not only the computer where data start off, but also multiple points throughout various networks through which the data pass. In the meshes of supply chain networks, a security implementation is only as secure as its weakest link. Consequently, it is vital to identify and safeguard each point where security has a potential of being breached. In other words, identifying the points of vulnerability is one of the keys to securing the company's network infrastructure and critical enterprise resources in an open and distributed computing environment.

Results

To take advantage of the benefits from implementing the e-service system, HVAC needs a secure IT infrastructure that can minimize security risks and further decrease the costs of security management and operations. More than ever, the company needs

to leverage state-of-the-art security solutions that will reduce risks while enabling flexibility and adaptability to ensure a proper balance for the corporate security strategy and policy. Addressing this need, eSMLC methodology is adopted to help the company identify its security exposures as well as provide the right kind of security tools and controls, especially for a secured e-business environment. Figure 3 summarizes four major tasks in developing security baseline, simulation models, and systems validation and demonstration in three implementation horizons.

All the reports and documents generated in the four major tasks are stored in the eSMLC repository. The eSMLC repository contains a collection of good security management practices and principles as well as simulation models, which can be used as comprehensive technical guidance and detailed operational procedures for identifying risks at all levels of the e-service IT infrastructure. The merit of envisioning the entire e-enterprise network as a set of architectural building blocks is that it can assist in identifying and isolating each entity in order to focus on implementing different security measures within it.

Conclusions

Implementing eSMLC has served to help the security specialists zero in on different critical security management jobs in a sequential but interrelated and logical manner.

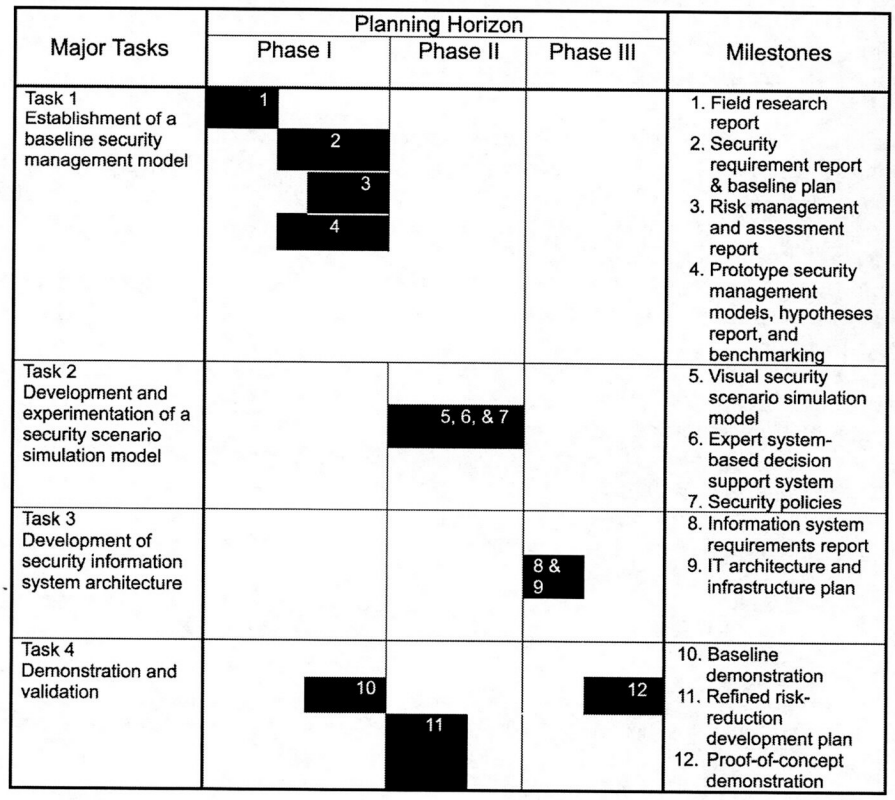

Figure 3.
Tasks, phases, and milestones for eSMLC implementation

Through the use of eSMLC, in-depth understanding of the potential environmental risks can be properly acquired. The methodology helps managers perform a proactive analysis of the consequences of security breaches in relation to risks. Incorporating security measures into all aspects of the e-enterprise network, a set of meticulously planned security management strategies can then be developed based on the analysis.

The eSMLC methodology provides a viable foundation for building a secure and manageable computing environment using a recommended set of solutions, processes, procedures, and technologies. Nevertheless, the aim of the eSMLC is not to provide a recipe book with predetermined steps on security management practices for all possible scenarios. On the contrary, it renders a unified, structured framework which helps develop an actual security plan and solutions and/or improve currently used security standards, practices, and configurations in response to special security requirements and long-term e-business needs.

References

Amidon, D.M. (2002), "Collaborative innovation and the knowledge economy: toward the 'world trade of ideas'", available at: www.entovation.com/info/future.htm

Avison, D.E. and Fitzgerald, G. (1991), "Information systems practice education and research", *Journal of Information Systems*, Vol. 1 No. 1, pp. 5-17.

Burstein, F. (1999), "The systems development or engineering approach to research in information systems: an action research perspective", *Proceedings of the 10th Australasian Conference on Information Systems*, pp. 122-34.

CERT (2002), available at: www.cert.org/stats/cert_stats.html

Clarke, R. (1997), "Electronic commerce definitions", available at: www.anu.edu.au/people/Roger.Clarke/EC/ECDefns.html

Clarke, R. (2001), "Introduction to information security", available at: www.anu.edu.au/people/Roger.Clarke/EC/IntroSecy.html

Computer Economics (2002), available at: www.computereconomics.com/cei/press/pr92101.htm

COT (2002), "Continuity testing", available at: www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/cot_123.pdf

Cottrel, A. (1977), "Emergent properties of complex systems", in Duncan, R. (Ed.), *The Encyclopedia of Ignorance – Everything You Ever Wanted to Know about the Unknown*, Pergamon Press, Oxford, pp. 129-35.

C-TPAT (2002), available at: www.customs.treas.gov

Ellison, R.J., Fisher, R.C., Linger, H.F., Lispon, H.F., Longstaff, T.A. and Mead, N.R. (1999), "Survivable systems: an emerging discipline", *Proceedings of the 11th Canadian Information Technology Security Symposium (CITSS)*, Ottawa, May 10-14.

Fisher, D.A. and Lipson, H.F. (1999), "Emergent algorithms – a new method for enhancing survivability in unbounded systems", *Proceedings of the 32nd Annual Hawaii International Conference on System Sciences*, Maui, HI, January 5-8, HICSS-32, IEEE Computer Society, Los Alamitos, CA.

Galliers, R. (1992), "Choosing information systems research approaches", in Galliers, R. (Ed.), *Information Systems Research: Issues, Methods and Practical Guidelines*, Blackwell Scientific Publications, Oxford, pp. 144-62.

Grossberg, S. (1997), "Nonlinear neural networks: principles, mechanisms, and systems", *Prog. Neurobiol.*, Vol. 51, pp. 167-94.

Hinton, H.M. (1997), "Under-specification, composition and emergent properties", *Proceedings of the 1997 New Security Paradigms Workshop*, Langdale, September 23-26, Association for Computing Machinery, New York, NY.

Iivari, J., Hirschheim, R. and Klein, H. (1998), "A paradigmatic analysis contrasting information systems development approaches and methodologies", *Information Systems Research*, Vol. 9 No. 2, pp. 164-93.

INL (2001), Independent Newspapers Ltd, available at: www.stuff.co.nz/inl/index/0,1008,665885a1897,FF.html.

IS (2000), "2000 industry survey – security-focused", *Information Security Magazine*, September, pp. 40-68.

Kleijnen, J. (1974), *Statistical Techniques in Simulation – Part I*, Marcel Dekker, New York, NY.

Lipson, H.F. and Fisher, D.A. (1999), "Survivability – a new technical and business perspective on security", *Proceedings of the 1999 New Security Paradigms Workshop*, Caledon Hills.

Nunamaker, J., Chen, M. and Purdin, T. (1991), "Systems development in information systems research", *Journal of Management Information Systems*, Vol. 7 No. 3, pp. 89-106.

Riesenhuber, M. and Dayan, P. (1997), "Neural models for part-whole hierarchies", in Mozer, M., Jordan, M. and Petsche, T. (Eds), *Advances in Neural Information Processing Systems*, Vol. 9, MIT Press, Cambridge, MA, pp. 17-23.

SANS (2001), available at: www.incidents.org/react/nimda.pdf

UKDTI (2002), UK Dept of Trade and Industry, available at: www.security-survey.gov.uk/View2002SurveyResults.htm

Zahavi, R. (2000), *Enterprise Application Integration with CORBA – Component and Web-based Solutions*, John Wiley & Sons, New York, NY.

ZDNet (2001), available at: www.zdnet.com/zdnn/stories/news/0,4586,2677878,00.html

Zeidner, L. and Wood, R. (2000), "The collaborative innovation (CI) process", paper presented at the Altshuller Institute TRIZCON2000, available at: www.triz-journal.com/archives/2000/06/a/