World Applied Sciences Journal 3 (Supple 2): 82-90, 2008
ISSN 1818-4952

Information Access Level Control in Electronic Supply Chain

[1]Seyed Mohammad Hashemian, [2]Majeed Behzadian,
[1]Mehdi Ranjbar-Bourani and [1]Fatemeh Zabihy

[1]Department of Industrial Engineering, Faculty of Graduate Studies,
Islamic Azad University-South Tehran Branch, Tehran, Iran
[2]Department of Industrial Engineering, Shomal university, Amol, Iran

Abstract: Nowadays, companies are in the race for improving their organizational competitiveness in order to compete in the 21st century global market. This market is electronically connected and dynamic in nature. Therefore, companies are trying to improve their agility level with the objective of being flexible and responsive to meet the changing market requirements. We live and work in the Information Age, where information is one of our most valuable assets and where, therefore, intelligent action to safeguard it is as necessary as safeguarding movable physical assets. Electronic supply chain (ESC) allows organizations to improve the efficiency and quality of their business activities. ESC uses information technology to achieve a closer integration and better management of partners' relationships between internal and external parties. Companies are attempting to find ways to improve their flexibility and responsiveness and in turn competitiveness by changing their operations strategy, methods and technologies that include the implementation of information sharing. There are many emerging issues in ESC and one of them is access level control. To implement access level control, interfaces between the system elements of the organizations that are involved in the collaboration are needed. However, access level control policies are often inconsistent from interface to interface and therefore conflict resolution should be considered to resolve multilevel access control policy problems. In ESC, partners must share information between themselves. Therefore, it is necessary existence a framework for sharing information than prevent and access level control. In this paper we try to show general conceptual framework for all ESC.

Key words: Access level control · Electronic supply chain · Information sharing

INTRODUCTION

Previous Approaches: Since the early 1980s *supply chain management* (SCM) has received the attention of practitioners and academics [1]. A *supply chain* is a bidirectional flow of information, products and money between the initial suppliers and final customers through different organizations. SCM is about planning, implementing and controlling this flow. Its goal can be to improve organizational competitiveness [2]. The supply chain, particularly SCM, contains different business functions, such as sales, purchases, demand forecasting and resource management. Supply chain integration is about information sharing within and between companies [3]. Information sharing covers exchange of business documents in business processes. Supply chain integration is an important part of SCM. It aims to ease the flow between all organizations in the supply chain. Companies are increasingly aware of the strategic importance of supply chain integration because it affects operational performance.

Since the late 1960s companies have used information systems to exchange standardized data with their business partners [4]. When the data are processed and communicated electronically, printing and re-keying of the data can be reduced. Therefore, information sharing using information and communication technologies can be faster and less error prone than information sharing by meetings, mails, phone calls, faxes or e-mails and it can save both time and money In electronic commerce (e-commerce), companies utilize information sharing in sales with their customers or in purchases with their suppliers [5]. Business-to-business (B2B) e-commerce is a part of electronic business (e-business), in which

Corresponding Author: Mehdi Ranjbar-Bourani, Department of Industrial Engineering, Faculty of Graduate Studies,
Islamic Azad University-South Tehran Branch, Tehran, Iran

companies use information sharing in all kinds of collaborations with their business partners [5]. There is a large variety of initiatives ranging from simple supply chain integration between organizational units within the same company to complex supply chain integration between different companies in the supply chain network. In addition, companies have invested heavily in information systems, particularly in enterprise resource planning (ERP), SCM and customer relationship management (CRM) systems [6]; [7]. Unfortunately, supply chain integration is not easy.

Organizational units within a company may also face integration problems. Although many differences between business partners are inevitable, standards can bring order by reducing the complexity and uncertainty. Standardization of business documents, business processes and messaging leads to harmonization of meanings for terms, modes of operations and messaging interfaces. An *e*-business framework is a standard for information sharing within and between companies that enables the exchange of standardized data, e.g. in the Electronic Data Interchange (EDI) or Extensible Markup Language (XML) formats [14].

Explorations in Information Security: Participation in activities such as electronic commerce requires that people be able to trust the infrastructures that will deliver these services to them. This is not quite the same as saying that we need more secure infrastructures. We believe that it is important to separate theoretical security (the level of secure communication and computation that is technically feasible) from effective security (the level of control that can practically be achieved in everyday settings). Levels of effective control are almost always lower than those of theoretical control. A number of reasons for this disparity have been identified, including poor implementations of key security algorithms [7], insecure programming techniques [8], insecure protocol design [9][10] and inadequate operating systems support [11][12]. One important source of the disparity, though, is problems around the extent to which users can comprehend and make effective use of security mechanisms. Approaches that attempt to make the provision of access control ‘‘automatic’’ or ‘‘transparent’’ essentially remove security from the domain of the end-user.

However, in situations where only the end-user can determine the appropriate use of information or the necessary levels of security, then this explicit disempowerment becomes problematic. It is broadly recognized that one of the major challenges to the effective deployment of information security systems is getting people to use them correctly. Psychological acceptability is one of the design principles that Saltzer and Schroeder identify. Even beyond the domain of electronic information systems, there are many examples of the fact that overly complex security systems actually reduce effective security. For example, [13], cited by [14], suggests that Russian military disasters of the Second World War were partly due to the fact that Russian soldiers abandoned the official army cipher systems because they were too hard to use and instead reverted to simpler systems that proved easier to crack. Schneier [10] sums up the situation: ‘‘Security measures that aren’t understood by and agreed to by everyone don’t work.’’

Usability of Security Software and Mechanisms: In a series of studies, researchers at University College, London have explored some of the interactions between usability and security [15][16]. They focused on user-visible elements of security systems, such as passwords. Although many information systems professionals regard users as being uninterested in the security of their systems (and, indeed, likely to circumvent it by choosing poor passwords, etc.), Adams and Sasse’s investigations demonstrate that users are certainly motivated to support the security of the system, but often unable to determine the security implications of their actions. The specific problems that they identify with passwords have also led to interesting design alternatives [17].

In some cases, the complexity of making security work is as much a matter of interface design as anything else. Whitten and Tygar [18] present a usability analysis of PGP 5.0, demonstrating the difficulties that users have in completing experimental tasks (in their user study, only 3 out of 12 test subjects successfully completed a standard set of tasks using PGP to encrypt and decrypt email.) The problems that they uncovered were largely problems of interface design and in particular the poor matching between user needs and the structure of the encryption technology provided to meet these needs. Zurko and Simon explore similar concerns in their focus on ‘‘user-centered security’’. Like us, they are concerned that the inscrutability of conventional security mechanisms makes it less likely that users will employ them effectively. The approach they outline focuses on graphical interfaces and query mechanisms to MAP, an authorization engine. While this approach is clearly helpful, it is limited to a particular area of system security and lacks the real-time feedback.

Control over Security: One area at the intersection of usability and security that has received some attention is the role of access control in interactive and collaborative systems. For example, Dewan and Shen [19,20] have explored the use of access control and meta-access control models as a basis for describing and controlling degrees of information access and management in collaborative systems. This is not simply a technical matter, since the structure and behavior of these ''internal'' components can have a significant effect on the forms of interactivity and collaboration they can support [21].

Many collaborative systems involve privacy issues and need to provide users with control over the disclosure of information.This has spurred a number of researchers to explore the development of privacy control systems that are tailored to the needs of end-users. For instance, Dourish [22] describes the relationship between three different security mechanisms for similar multimedia communication systems, each of which reflects assumptions and requirements of the different organizations in which they were developed. Bellotti and Sellen [23] draw on experiences with multimedia and ubiquitous computing environments to identify the source of a number of potential privacy and security problems. Their primary concepts-disembodiment and dissociation-are both visibility problems, related to the disconnection between actors and actions that renders either actors invisible at the site of action, or actions invisible to the actor.

Based on their investigations of privacy problems in on-line transactions, Ackerman and colleagues propose the idea of privacy critics-semi-autonomous agents that monitor on-line action and can inform users about potential privacy threats and available countermeasures[24][25]. Again, this mechanism turns on the ability to render invisible threats visible.

One important related topic is control over the degree of security available. One of our criticisms of traditional security systems has been their ''all or nothing'' approach. However, there has been some work that attempts to characterize degrees of security provision, as embodied by the idea of ''quality of security service'' [26]. This builds on earlier work establishing taxonomy of security service levels. The fundamental insight is that organizations and applications need to trade-off different factors against each other, including security of various forms and degrees, in order to make effective use of available resources [4][27]. While this work is directed towards resource management rather than user control, it begins to unpack the ''security'' black box and characterize degrees and qualities of security.

The Internet revolution has dramatically changed the way individuals, firms and the government communicates and conducts business. For example, the Telecommunications, banking and finance, energy and transportation industries, as well as the military and other essential government services, all depend on the Internet and networked computer systems to conduct most of their day to day operations. However, this widespread interconnectivity has increased the vulnerability of computer systems--and more importantly, of the critical infrastructures they support--to information security breaches. In response to this new vulnerability, organizations have created an arsenal of technical weapons to combat computer security breaches. This arsenal includes firewalls, encryption techniques, access control mechanisms and intrusion detection systems. the security and reliability of the entire Internet is affected by the security measures taken by all users of the Internet [14]. Hence, externalities play an important role in the study of information security.

Networked computer systems are increasingly the site of people's work and activity. Millions of ordinary citizens conduct commercial transactions over the Internet, or manage their finances and pay their bills on-line; companies increasingly use the Internet to connect different offices, or form virtual teams to tackle mission-critical problems through entirely ''virtual'' interaction; e.g. interaction between citizens and local and federal government agencies can increasingly be conducted electronically; and the 2004 national elections in Brazil and (to a much more limited extent) the US saw the introduction of electronic voting, which will no doubt become more widespread.

However, these new opportunities have costs associated with them. Commercial, political and financial transactions involve disclosing sensitive information. The media regularly carry stories about hackers breaking into commercial servers, credit card fraud and identity theft. Many people are nervous about committing personal information to electronic information infrastructures. Even though modern computers are powerful enough to offer strong cryptographic guarantees and high levels of security, these concerns remain.

The need for secure ESC is broadly recognized, but most discussions of the ''problem of security'' focus on the foundational elements of information systems (such as network transmission and information storage) and the mechanisms available to system developers, integrators and managers to ensure secure operation and management of data. Access level control, though, is a broader concern and a problem for the end-users of information systems as much as for their administrators.

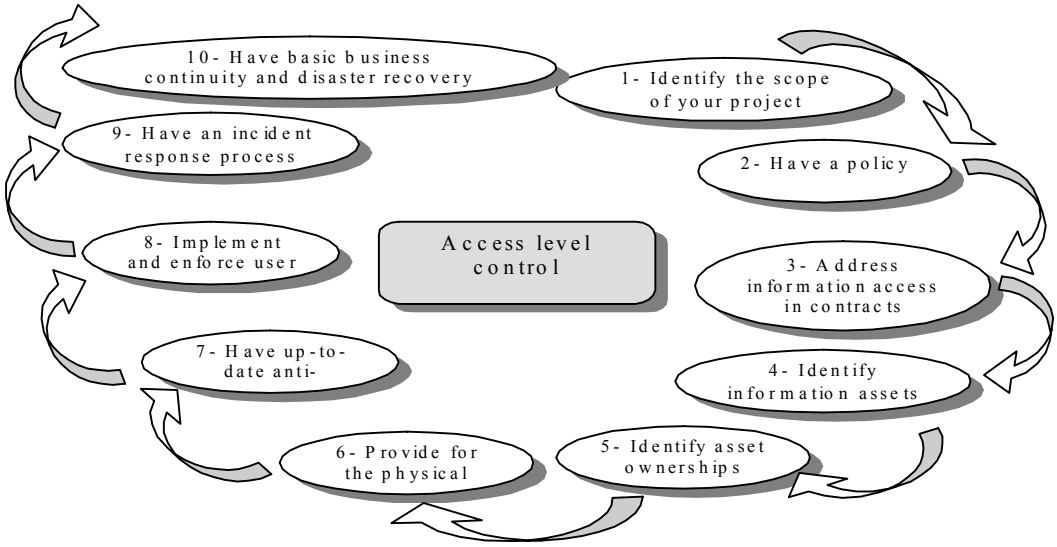

Fig. 1: Steps of access level cotrol

Access Level Control: Access level control, in the vast majority of organizations, is inadequate, unsystematic or, in practical terms, simply non-existent. That's partly because many boards still think of it as computer security and that it's therefore simply an ancillary responsibility of the people who run the computers. It's also partly because many boards have never really thought the information needs (and therefore the information strategy) of their businesses. We live and work in the Information Age, where information is one of our most valuable assets and where, therefore, intelligent action to safeguard it is as necessary as safeguarding movable physical assets.

Information insecurity also exists because organizations don't actually have the knowledge, resources or expertise to tackle it effectively. As a result, small and medium-sized businesses tend to be inaccurate in allocating (sometimes inadequate) resources (manpower, management time and hard cash) to deal with the most important, strategic, business security issues, while tackling individual threats and risks in a haphazard way. Investing in isolated solutions to individual threats leaves so many holes that it's only slightly more useful than not bothering in the first place. Larger organizations tend to operate their security functions in vertically segregated silos with little or no coordination. This structural weakness means that most organizations have significant vulnerabilities that can be exploited deliberately or which simply open them up to disaster. For instance, while the corporate lawyers will tackle all the legal issues (non-disclosure agreements, patents, contracts, etc) they will have little involvement with the information security issues faced on the organizational perimeter, or the way in which cyber law cyber security and e-commerce have to interact for the real benefit of the customer.

The range, scale and complexity of the threats, both internal and external and the increasing difficulty of legal and regulatory compliance, means that boards cannot afford to have loopholes in their information security systems. Therefore, one has to think in terms of access level the whole enterprise, the entire organization, which includes all the possible combinations of physical and cyber assets, all the possible combinations of intranets, extranets and internet interfaces and which might include an extended network of business partners, vendors, customers and others. One has to look at the distribution and supply channels. One has to take into account the present and future information needs of the business and the technology required-today and tomorrow for supporting them.

Access level control is the policy of controlling access to information processing facilities through a combination of access agreements and technological security measures that implement the policy guidelines. These controls therefore restrict the rights of individual users to access information processing facilities. User access rights reflect user access controls: the user has the right to do those things that the controls allow.

Identify the Scope of Your Project: Determining the scope of your information access level control project is harder for larger, complex e-supply chain, than it is for smaller ones. It is, though, essential for any size of chain: you have to decide which information assets you're going to protect before you can decide on appropriate protection. This should be a quick decision for a small or medium-

sized business: everything. That's because there will probably be hard-wired connections between all the information systems and day to-day working relationships within the business that make it either extremely difficult or impractical to try to segregate one part of the business from another. The notion of segregation is at the heart of effective scoping: ultimately, you are going to try to create an impregnable barrier around that part of your business that is within the scope of your project and everything else.

In today's business environment, your defensive barrier has to operate at the individual device level and is highly dependent on user compliance with business procedures. In other words, your scoping decision needs to include all the information devices that people use in their jobs-such as cell phones, wireless laptops, home offices, etc-as well as the more obvious central office systems-accounting, payment processing, production, sales and order management, e-mail, office automation, etc.

In larger, more complex chains, you will also want to ensure that the entity that is within scope has a clearly defined legal and management structure and that there is alignment with the compliance requirements part of the reason for your information security system is to ensure that you are compliant with the myriad of laws and regulations, so it makes sense for that entity that has those compliance obligations, to be fully within the scope of your information security project. There is a range of network mapping software that will automatically map your network for you, some of which have additional management features added in. The network map should integrate with the technology asset list and should be a live document, which is updated as and when the network is changed. It is also one of the most sensitive documents that any organization possesses, so it should be under document control and have a high security classification.

Have a Policy: Every e-supply chain needs a basic statement from its board, which sets out the overall policy for controlling the availability, confidentiality and integrity of the organization's information assets and which reflects senior management's commitment to it. Creating this policy may be an iterative process (particularly in complex organizations dealing with complex information security issues and/or multiple domains) and the final form of access level control policy that is adopted may only emerge after the final risk assessment has been carried out. What we need initially is a policy statement that creates the overall framework for action, or which pulls current information access control activity and requirements into a coherent framework.

An information access control policy answers the four key questions: who, where, what and why? Who is responsible for information security in the organization? To which parts of the organization does the policy apply? What are we required to do? And why are we required to do it?

The policy statement should specifically reference the assets and entity hat have been identified as being within the scope of the project. In addition, the policy should state the organization has the following specific compliance requirements: information systems and assets must be kept physically secure; up-to-date anti-malware and firewall software is required; users are required to conform with company rules on access of information systems and assets; software must be approved by the company and all updates implemented; all staff must comply with the security incident reporting procedure; rules about backup, continuity planning and business continuity plans must be observed; and that the organization will take steps to ensure that its policy is observed.

This policy document should be drawn up, agreed by the board, signed and dated by the Chief executive, issued to every member of staff and posted on notice boards-or, if you use an intranet, here. If you wanted to be precise, you would also make it a controlled document.

Address Information Access in Contracts: All contracts-employment contracts, outsourcing contracts, third-party contracts and customer contracts, need to deal with information access issues. This will take a considerable time-and the input from your corporate lawyers-to prepare and roll out. The two most important areas are employment and outsourcing-approximately half of all information security incidents are caused by INSIDERS, employees or contractors-and so these must be tackled as a priority. Obviously, existing contracts will need to be updated, but it may not be possible to do this immediately. New starters and new outsourcing contracts must be drafted so that they set out clearly the individual or the supplier's information security responsibilities. Once steps have been taken to deal with new contracts, a robust approach must be taken to dealing with the existing ones.

Identify Information Assets: Asset anything that has value to the organization. Information assets are likely to be of the following types:

Information: Databases and data files, other files and copies of plans, *system documentation, original user manuals, original training material,* operational or other

support procedures, continuity plans and other fallback arrangements, archived information, financial and accounting information;

Software: Application software, operating and system software, development tools and utilities, e-learning assets, network tools and utilities;

Physical Assets: Computer equipment (including workstations, notebooks, monitors, modems, scanning machines, printers), communications equipment (routers, cell phones, fax machines, answering machines, voice conferencing units, etc), magnetic media (tapes and disks), other technical equipment (power supplies, air conditioning units), furniture, lighting, other equipment; communications equipment (routers, cellophanes, fax machines, answering machines, voice conferencing units, etc).

Services: 'groups of assets which act together to provide a particular function', such a computing and communications services, general utilities, for example, heating, lighting, power, air conditioning.

Information Classification: The simplest approach is usually one that has only three levels of classification. The first level identifies information that is so confidential that it has to be restricted to the board and specific professional advisers. Information that falls into this category is marked 'Highly Confidential', with the names of the people to whom it is restricted identified on the document. Examples of highly confidential information might include information about potential acquisitions or corporate strategy, or about key organizational personnel, such as the chief executive. The amount of information that falls into this category should be carefully limited; the cost and operational inconvenience of protecting it properly is such that it needs only to be information whose release can significantly damage the organization.

A second level of classification should cover documents that are to be available only to senior or other specified levels of management within the organization. These might be marked 'Confidential Restricted'. Examples might include draft statutory accounts, which might be available to everyone in senior management, or implementation plans for corporate restructuring, which senior managers need to work through prior to their being rolled out.

The Final Level of Classification Is: 'Confidential' and this should cover everything that has value, which should not be allowed to fall into the hands of third parties, but does not fit within either of the other two categories. Every employee should be entitled to access information with this classification.

Identify Asset Ownerships: This requirement is simple to describe, but quite time-consuming to implement. 'Assets', for the purposes of this section, is a key area. You need to create a full inventory of the organization's information assets, looking at each of the categories identified in the definition. The network map and physical asset list that you produced in the initial scoping exercise is the starting point for this exercise. Hopefully, you agreed the network map-derived asset list to the finance department's fixed asset register, to ensure that there were no missing assets on either register. Now you need to extend the list to cover all the categories of information asset. This is an exercise in which it is 'better to be approximately correct than absolutely wrong'.

Each of your information assets should have an identified owner and this person's name should be recorded on the asset list (which must therefore be kept up to date to reflect changes in staffing, job roles, etc). Clearly, the 'owner' is the person, or function, that has responsibility for the asset the 'owner' has no property rights to the asset. This responsibility should be clearly communicated to every owner and written into their access agreements and the acceptable use policy. In terms of desktop computers, laptops, cell phones, etc, the owner will be the person to whom they are assigned and who generally uses them.

It is much more difficult to determine the owners of the intangible information assets. The use of other information assets can, however, be widespread through the esc and which will have been acquired as the result of a strategic or group decision. Examples might include Customer Relation-ship Management (CRM) systems and their client data, workflow systems and the information they contain, accounting systems and financial in-formation.

Many instances of illegal copying arise accidentally; the esc has grown quickly, or systems have been upgraded and the growth in the number of instances of each software package has been uncontrolled. It's simple to put right and cheaper to do so at once. You reduce the number of installed instances of each item of software to the necessary level and you buy additional licenses for whatever the excess number over your existing license base is. Thereafter, you keep a software register, which you update for new computer deployments and you buy the additional licenses you need as and when you need them. You include, in the user agreements, a ban on the installation on corporate computers of unlicensed

software and you have your internal audit team to do regular audits of this. In this section we explain three sector of member of ESC:

External Members: Any organization that takes over and supplies or gets services is likely to be external members. Insofar as the external partners has responsibility for organizational data (a call centre, for instance, or a payroll bureau, both of which may be collecting personal data and both of which may be interacting with organizational information systems), the consequent risks need to be addressed in the contract. In a nutshell, you should want your external partners to maintain information security controls that will at least match those you require of yourself. Appropriate clauses should be drafted by your corporate lawyers and, if they haven't had experience of information security in outsourcing arrangements, find a specialist firm. Your definition of 'outsourcing company' should be expanded to include contractors (for instance, IT contractors), interim managers, consultants, facilities and security staff and cleaners-anyone who is dealing with your information assets, your information systems, or who might have access to them, but who isn't an employee, should be captured by your definition.

Employees: You need to address access control at three stages of employment: recruitment, during employment and at termination. You will need to take the specific advice of your employment lawyers to ensure that your procedures comply with local law, but you want to be sure that you can screen employees for sensitive positions prior to appointing them; that you can require specific compliance behavior from them during employment and that upon termination you can enforce confidentiality clauses and get all information and other assets returned. Your disciplinary policy will also need to be upgraded so that it specifically deals with breaches of access level control policy and guidelines.

Other Third Parties: There are many other third parties that might from time to time need to see-or access-confidential information. You should have a standard agreement drafted by your lawyers, which is available for use at any time. Its information access level control should, to the greatest extent possible, be consistent with those in your employment and outsourcing contracts. You should not reveal confidential information without first having had a copy of the contract signed and returned to you. If you are a private sector firm contracting with the public sector, you need to think through how you want to handle the possible implications of the Freedom of Information Act.

Provide for the Physical Security: There are two aspects to this: desktop systems and central systems. The latter is more important for organizational security than the former and the former can be dealt with through a combination of ensuring that all users are familiar with the guidance of principle 1 of the Internet Highway Code and ensuring that desktop computers in the workplace have been safely set up: on a stable base, with cables controlled with cable tidies so that they can't trip people or get pulled out accidentally (sometimes they pull the computer over as well. Central systems are the heart of the organization's information operation. Traditionally, all the corporate servers on which the organization's applications all run are set up in a central server room. The server room is usually the responsibility of the Head of IT.

Have Up-to-date Anti-malware Software: User training is an essential part of an effective anti-malware posture: users must know how to respond to virus hoaxes, about not opening e-mails from unknown/unexpected sources, etc. The Internet Highway Code provides essential user guidance on this and should be in the hands of all employees. Your policy requirements around anti-virus software (that it must be update that it may never be switched off) should also be written into the user agreement.

Implement and Enforce User Access Controls

User Names: While it is unlikely that any business computer system does not allocate individual user names to employees and others, not all organizations have a clear security policy for how this should be done. At the basic level, user names should be unique, allocated to individuals and subject to a signed user agreement; it should be a disciplinary offence for anyone to use someone else's user name. Using someone else's user name is identity theft and any multi-user systems set up to require only one user name are exposing themselves to untraceable abuse. People who do not need access to specific systems should not be given access to them and deployment of single sign-on systems provides an opportunity to configure user access rights appropriately. The asset list created at the implementation stage of the project can help make decisions about the role and level of employees who should have access to each system. Group IDs and the 'guest' user name should not be available for use: administrators should be issued with standard user names for their everyday work and only use their own administrator name when they have a specific system administrative task to perform. After someone

leaves the organization or their role changes, their user name must be withdrawn or their user rights amended to reflect the new circumstances.

Passwords: Organizations should deploy central system management software that enforces password changes and which requires them to be good quality: seven or more characters long, alpha-numeric, enforced change every 30 days, no reuse of passwords and no use of sequential passwords (for example, rogerson1, rogerson2, etc).

Have an Incident Response Process: You need, therefore, a process for responding to access level control incidents in order to limit business disruption. In essence, the process you need to roll out has two elements: what users should do when something unexpected happens and how these events should be dealt with.

Have Basic Business Continuity and Disaster Recovery Plans: The difference between these two is this: a business continuity plan is essential on a day-to-day basis, a disaster recovery plan is essential for recovering from 'acts of nature'. The two should go hand in hand; in a very real sense, business continuity depends on being able to recover from disasters in a way that is relatively seamless.

CONCLUSION

This focuses our attention on a rather different design challenge; how can we provide ESC with the tools and facilities that they need to understand and dynamically control access as a part of their existing interaction? Rather than providing mechanisms that take security decisions away from ESC, we want to develop open and flexible frameworks that allow them to understand the consequences of their actions and develop new forms of practice.

We provided 10 steps of access level control and tried to attention to all aspect of security in the ESC network.

REFERENCES

1. Cooper, M.C. Cooper, D.M. Lambert and J.D. Pagh, 1997. "Supply chain management: More than a new name for logistics", Intl. J. Logistics Management, 1(8): 1-14.
2. Mukhopadhyay and Kekre, T. Mukhopadhyay and S. Kekre, 2002. "Strategic and operational benefits of electronic integration in B2B procurement processes", Management Sci., 48(10): 1301-1313.
3. Wacker, J.G. Wacker, 2004. "A theory of formal conceptual definitions: Developing theory-building measurement instruments", J. Operations Management, 22(6): 629-650.
4. Henning and R.R. Henning, 2000. Security service level agreements: quantifiable security for the enterprise? Proceedings of the 1999 Workshop on New Security Paradigms. ACM Press, Caledon Hills, Ont., Canada, pp: 54-60.
5. Laudon and Laudon, J.P. Laudon and K.C. Laudon, 2006. Essentials of Business Information Systems, Prentice-Hall, Upper Saddle River, NJ.
6. Falk and M. Falk, 2005. ICT-linked firm reorganisation and productivity gains, Technovation, 25(11): 1229-1250.
7. Kelsey, J. Kelsey, B. Schneier, D. Wagner and C. Hall, 1998. Cryptanalytic attacks on pseudorandom number generators. Proceedings of the Fifth International Workshop on Fast Software Encryption. Springer, Berlin, pp: 168-188.
8. Shankar, U., K. Talwar, J.S. Foster and D. Wagner, 2002. Detecting format string vulnerabilities with type qualifiers. Proceedings of the 10th USENIX Security Symposium (USENIX'02), Washington, DC, pp: 201-220.
9. Kemmerer, R. Kemmerer, C. Meadows and J. Millen, 1994. Three systems for cryptographic protocol analysis. J. Cryptol., 7(2): 79-130.
10. Schneier, B. Schneier and Mudge, 1998. Cryptanalysis of Microsoft's point-to-point tunneling protocol (PPTP). Proceedings of the Fifth ACM Conference on Computer and Communications Security. ACM Press, San Francisco, CA, USA, pp: 132-141.
11. Ames, S. Ames, M. Gasser and R. Schell, 1983. Security Kernel Design and Implementation: An Introduction. IEEE Computer, Silver Spring, MD, pp: 14-22.
12. Bernaschi, M. Bernaschi, E. Gabrielli and L.V. Mancini, 2000. Operating system enhancements to prevent the misuse of system calls. Proceedings of the Seventh ACM Conference on Computer and Communications Security. ACM Press, Athens, Greece, pp: 174-183.

13. Kahn and D. Kahn, 1967. The Codebreakers, The Story of Secret Writing. Macmillan, New York, NY. Spyropoulou, E., Levin, T., Irvine, C., 2000. Calculating costs for quality of security service. Proceedings of the 16th Annual Computer Security Applications Conference. IEEE Computer Society, Silver Spring, MD, pp: 334.
14. Anderson and R. Anderson, 2001. Why cryptosystems fail. Proceedings of the First ACM Conference on COMPUTER and Communications Security. ACM Press, Fairfax, VA, pp: 215-227.
15. Adams, A. Adams and M.A. Sasse, 1999. Users are not the enemy: why users compromise security mechanisms and how to take remedial measures. Communications of the ACM., 42 (12): 40-46.
16. Adams, A. Adams, M.A. Sasse and P. Lunt, 1997. Making passwords secure and usable. Proceedings of HCI on People and Computers XII. Springer, Berlin, pp: 1-19.
17. Dhamija, R. Dhamija and A. Perrig, 2000. Deja Vu: A user study. using images for authentication. Proceedings of the Ninth USENIX Security Symposium, Denver, CO. Greenberg, S.
18. Whitten, A. Whitten and J.D. Tygar, 1999. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. Proceedings of the Ninth USENIX Security Symposium.
19. Dewan, P. Dewan and H. Shen, 1998. Flexible meta access-control for collaborative applications. Proceedings of the 1998 ACM Conference on Computer Supported Cooperative Work. ACM Press, Seattle,WA, USA, pp: 247-256.
20. Shen, H. Shen and P. Dewan, 1992. Access control for collaborative environments. Proceedings of the 1992 ACM Conference on Computer-Supported Cooperative Work. ACM Press, Toronto, Ont., Canada, pp: 51-58.
21. Marwood and D. Marwood, 1994. Real time groupware as a distributed system: concurrency control and its effect on the interface. Proceedings of the 1994 ACM Conference on Computer Supported Cooperative Work. ACM Press, Chapel Hill, NC, USA, pp: 207-217.
22. Dourish and P. Dourish, 1993. Culture and control in a media space. Proceedings of the European Conference on Computer-Supported Cooperative Work ECSCW'93. Kluwer, Dordrecht, pp: 125-137.
23. Bellotti, S. Brostoff and Sasse, 2000. M.A. Are passfaces more usable than passwords? A field trial investigation. In: McDonald, S., Waern, Y., Cockton, G. (Eds.), People and Computers XIV-Usability or Else! Proceedings of HCI 2000. Springer, Berlin, pp: 405-424.
24. Ackerman, M.S. Ackerman and L. Cranor, 1999. Privacy Critics: UI Components to Safeguard Users' Privacy. CHI '99 Extended Abstracts on Human Factors in Computing Systems. ACM Press, Pittsburgh, PA, pp: 258-259.
25. Ackerman, Ackerman, M.S. Cranor, L.F. Reagle and J. Privacy, 1999 in e-commerce: examining user scenarios and privacy preferences. Proceedings of the First ACM Conference on Electronic Commerce. ACM Press, Denver, CO, pp: 1-8.
26. Irvine, C. Irvine and T. Levin, 2000. Quality of security service. Proceedings of the 2000 Workshop on New Security Paradigms. ACM Press, Ballycotton, County Cork, Ireland, pp: 91-99.
27. Thomsen, D. Thomsen and M. Denz, 1997. Incremental assurance for multilevel applications. Proceedings of the 13th Annual Computer Security Applications Conference. IEEE Computer Society, Silver Spring. MD, pp: 81.