

Management of IT Infrastructure Security by Establishing Separate Functional Area with Spiral Security Model

Abhijit Vitthal Sathe

*Modern Institute of Business Management, Shivajinagar,
Pune 411 005 abhijit_sathe@hotmail.com*

Abstract:

IT infrastructure and IT enabled services are used by management people in their organization for achieving leadership and excellent growth in their business. They try to automate as many activities of their business as they can and so they become more dependent on IT infrastructure. Hence, security and control of IT infrastructure inherently becomes a top priority and remains a big challenge for management.

We store large amount of data in electric form and access it using multi-tier client/server computing environment which becomes more vulnerable when we use Internet and Wireless Networks. The architecture of a Web-based application typically includes a Web Client, a server, corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Activities such as continuous analysis of security mechanisms, redefining of security policies and implementation of new security solutions becomes as important as the business processes of the organization. This paper suggests one additional functional area in the organization's business model and it has to be IT Infrastructure Security.

This paper also suggests a model for security management - Spiral Security Model. This spiral model for IT infrastructure security will be divided into 6 tasks and two regions. The two regions are – New Technology Implementation (NTI) and Existing Security Enhancement (ESE). For both the regions of the Spiral Model same six tasks will be followed: Communication, Planning, Risk Analysis, Engineering, Evaluation and Testing, and Feedback.

Keywords: IT Infrastructure Security as a Functional Area, IT Infrastructure Management Team, IT Infrastructure Manager, Spiral Security Model

1. INTRODUCTION

Computer and Information Technology has become an essential component of organizations today. We started with big and bulky computers with very limited capabilities and today we have hundred to thousand times better computers are available in various forms like desktops, laptops, tablets, iPhones etc.

As the governmental and corporate organizations started adopting and integrating information technologies in their businesses, the growth of Information Technology(IT) has began from smaller local networks of computers connected by bulky cables to today's world of mobile wireless networks and Internet.

Earlier we use to access IT services by reaching to the desktop PCs but now we access these services using any device from anywhere, at any time and from any source. An unpredictable, unprecedented growth in the Information Technology!

This advancement in technology was fascinating but not secure. We have seen various kinds of threats, risks, and attacks on IT infrastructure and our privacy.

Earlier we use to store and retrieve information on single PC which can be easily protected by using simple password mechanism. Then we started building smaller private networks in which information was either present in single PC called as server or it was distributed among multiple PCs. We required mechanism to protect not PCs but the entire network from unauthorized users. But, still it was manageable as access to the network was possible to only employees of the organization. The next era was of an Internet, which is not only used to store and exchange information, but it has provided quite enhanced services like email, exchange of information, e-commerce etc. The services available in the Internet have increased enormously and accordingly security problems also increased exponentially. Not only viruses, but Trojans, worms, hacking, identity threats, privacy violation, data protection, non repudiation and so on created lot of trouble in providing sophisticated services. Today we are using mobility aware services using various devices like cell phones, laptops, PDAs, iPhones, tablets etc. Organizations are using services like M-commerce which provides more flexibility and service satisfaction to their users. Mobile devices has dominated PCs and wired networks today. Of course, now we have to deal with more serious security threats than what we had in the wired network.

As we started using more sophisticated and enhanced services available in Information Technology, we are facing still higher and more severe security threats.

2. FUNCTIONAL BUSINESS PROCESSES OF ORGANIZATIONS

For efficiency and better performance, organizations divide their activities into many functional areas. Every business can be seen as a collection of business processes as follows:

Functional Area	Business Process
Manufacturing and Production	Assembling the product Checking the quality Producing bills of materials
Sales and Marketing	Identifying customers Making the customers aware of the products Selling the product
Finance and Accounting	Paying creditors Creating Financial statements Managing cash accounts
Human Recourses	Hiring Employees Evaluating employees job performance Enrolling employees in benefits plans

Information technology can be used to automate all these business processes and it is becoming the key driving force for the organization to boost their performance. So, it is essential for management people of the organization to take all necessary steps in making IT infrastructure secure.

3. SECURITY THREATS TO IT INFRASTRUCTURE OF ORGANIZATIONS

IT infrastructure and IT enabled services are used by management people in their organization for achieving leadership and excellent growth in their business. They try to automate as many activities of their business as they can and so they become more dependent on IT infrastructure. Hence, security and control of IT infrastructure inherently becomes a top

priority and remains a big challenge for management. Security refers to the policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems. Controls are methods, policies, and organizational procedures that ensure the safety of the organization's assets; the accuracy and reliability of its records; and operational adherence to management standards.

We store large amount of data in electric form and access it using multi-tier client/server computing environment which becomes more vulnerable when we use Internet and Wireless Networks. The architecture of a Web-based application typically includes a Web Client, a server, corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Not only this, payment systems of banks, credit cards and even cloud computing services add to further complexity in implementing and managing security. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.

Security threats to the organization's infrastructure are multidimensional as follows:

Types of Attacks	Description
Computer Viruses	Malware - a malicious software program executes automatically without user knowledge and it is highly destructive – destroying files and programs, clogging of computer memory, reformatting of computer hard drive etc.
Worms	Malware – destroys files and may disrupt operations of computer These programs copy themselves from one computer to another.
Trojan Horse	Malware - Not a virus but it can often introduce different malicious programs into machine.
Spyware	Malware – automatically gets installed from infected emails or web sites and they monitor web surfing and provides

	advertisements clicking on which will redirect to other malicious websites indirectly.
Keyloggers	A kind of spyware records every keystroke made on a computer to steal serial numbers for softwares, to capture passwords of email accounts and credit card information while user is doing transaction online.
Hackers (Crackers)	A community that is spread all over the worlds and trying to gain unauthorized access to computer systems. They can identify weaknesses in the system of the organization to steal vital information.
Spoofing	Hackers attempting to hide their true identities masquerade as someone else. Example: redirecting customer to fake website to steal sensitive information of the customer
Sniffing	Capturing packets moving over the network – stealing proprietary information is the intention.
Denial-of-Service (DOS) Attacks	Flooding network server or web server with many thousands of false requests so that the server will go out of resources to crash the network. The main intention is to avoid access to legitimate users possibly cause a big loss to the organization.
Distributed Denial-of-Service (DDOS) Attacks	DoS attack implemented from various places in the network using many connected machines as a source (botnet).
Identity Theft	A computer crime in which personal information about some user is obtained and misused.

Pharming	Attacker sets up fake websites - Usually the purpose is to get critical personal information of customer
Phishing	Replacing DNS - IP address mapping with another IP address

4. FRAMEWORK FOR SECURITY AND CONTROL

As we adopt new technology we become vulnerable to new innovative, unknown security threats. Suppose if we have made our IT infrastructure secure we cannot afford to assume it will remain secure permanently. It requires continuous observation and analysis to identify loopholes in the security environment that we have setup. It is obvious for the organization to update themselves with new technologies and innovative solutions as and when they are introduced in IT world. These new technologies will have new even higher level security threats. It means activities such as continuous analysis of security mechanisms, redefining of security policies and implementation of new security solutions becomes as important as the business processes of the organization. It becomes essential for the organizations to form a separate security management team which will keep on analyzing and redefining security policies. This management team will keep updating organizations IT infrastructure with proactive and reactive steps all the time.

In other words organization will have one additional functional area in its business model and it has to be IT Infrastructure Security.

Activities of IT Infrastructure Security Management Team

Following will be the activities of IT infrastructure Security Management Team:

- Security Auditing
- Defining Security policies
- Identifying new threats and defining solutions to deal with them
- Identifying security issues in adopting to new technology

- Members must keep themselves updated with new threats and possible solutions to deal with them
- Dealing with Cybercrimes and Intellectual Rights.

5. SPIRAL MODEL FOR IT INFRASTRUCTURE SECURITY

There are various solutions available to deal with different security threats.

Application Layer	Firewalls, Gateways, Secure DNS, PGP, Public-Private Key Infrastructure, Digital Signatures, 3D-Secure, Backup Systems, RAID etc
Transport Layer	TLS/SSL
Network Layer	IPSec, Firewall, VLANs etc.

But all these methods not necessarily will provide permanent security solution. We require continuous assessment and update our security mechanisms accordingly. It is required to implement strategy to keep IT infrastructure secure. The strategy suggested here is based on spiral model of software development.

This spiral model for IT infrastructure security will be divided into 6 tasks and two regions. The two regions are – New Technology Implementation (NTI) and Existing Security Enhancement (ESE).

New Technology Implementation (NTI) Region

The IT Infrastructure Security Team will analyze, identify probable threats and accordingly they will define and plan appropriate solution so that new technology can be adopted conveniently.

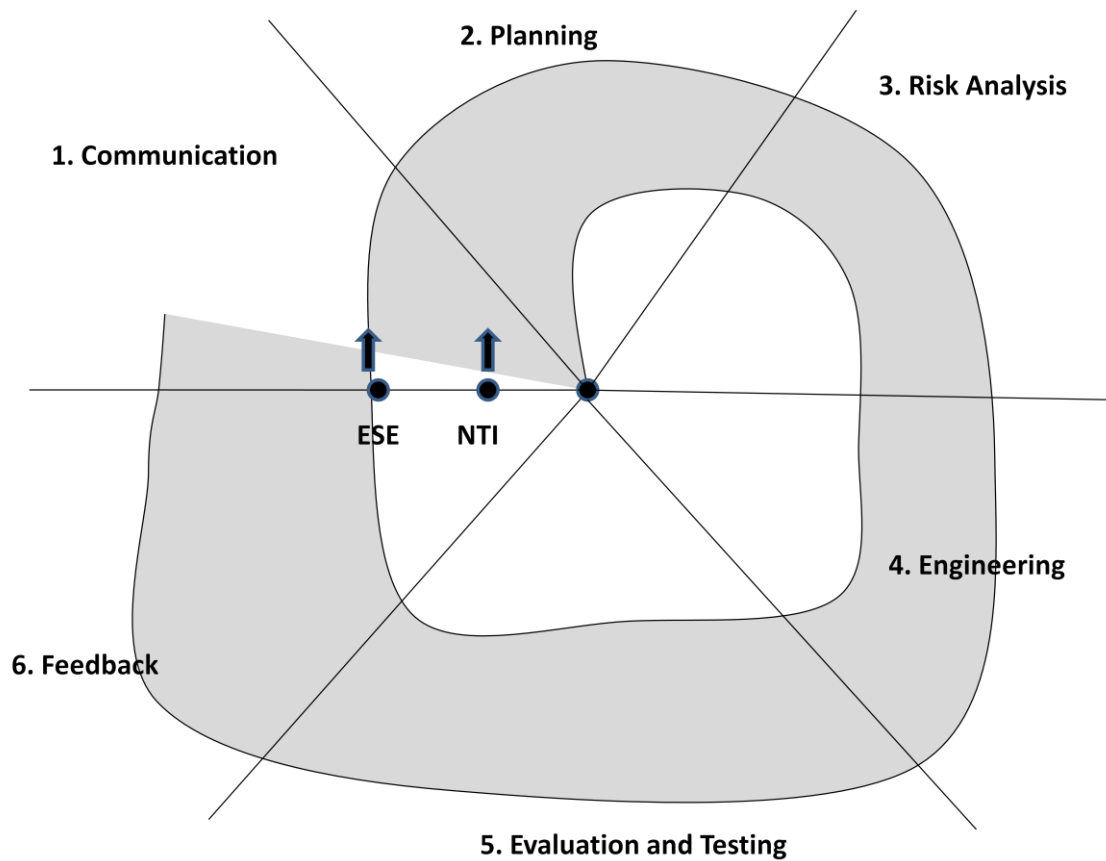
For example – if Sales and marketing unit of company decides to accept orders through mobile devices then IT security team will identify probable security issues and solutions to avoid those issues will be implemented by following all six tasks of spiral model.

Existing Security Enhancement (ESE)

If IT Security team in the organization identifies any threat or if they detect any attack, they will again follow all six tasks of spiral model to implement preventive solution. In this situation, probably security loophole can be identified by regular security auditing process by the team.

For both the regions of the Spiral Model same following six tasks will be followed:

1. **Communication:** IT Security Management Team and management people dealing with other business processes in the organization must have a communication and detailed discussion while defining policies for security of IT infrastructure. Policies defined by mutual agreement and by considering all business processes will be more effective. Once policies are clearly defined and known and agreed by all, they can be implemented with proper planning.
2. **Planning** – IT Security Management Team in the organization must consider guidelines, suggestions and policies defined in communication phase while designing a new security model.
3. **Risk Analysis** – The new security model defined in earlier phase must not affect the organization negatively. Hence, the model need to be analyzed for different parameters like effect on business process and customer, cost of implementation of security, available alternative solutions etc.
4. **Engineering** – This phase can be used for actual implementation of security model for IT infrastructure. This phase may require tasks such as purchasing of hardware/software, designing of new software etc.
5. **Evaluation and Testing** – This phase can be used to evaluate and test newly established security model to check whether it satisfies the criteria set during communication phase. If it does, then the organization will keep on using it and IT security management team will keep on reviewing and updating security model as per the feedback received from customers and employees in the organization.
6. **Feedback** from customers and employees to identify difficulties and loopholes in using the system after implementation of security solution. If modification are required, the whole process starts again from first phase with Existing System Enhancement (ESE) strategy.



New Technology Implementation (NTI)



Existing System Enhancement (ESE)



6. CONCLUSION

This paper recommends continuous assessment, evaluation and enhancement of IT Infrastructure security in the organization by forming a separate functional area called as IT Security Management. This functional area will be responsible for the implementation of various security aspects of the business processes. It will coordinate with other functional areas (such as Manufacturing and Production, Sales and Marketing, Finance and Accounting, and Human Resource) to deal with security problems.

This paper also suggests a security implementation model called as spiral security model which will help organization to continuously assess and enhance security of IT infrastructure. The model that has been suggested here is independent of the implementation of security in software. The security mechanisms implemented within software are usually restricted in their scope and may not help in providing secure environment for overall infrastructure of the organization. This model can be applied for overall security of IT infrastructure which involves networks, servers, individual machines, mobile devices and web services of the organization.

7. REFERENCES

1. Ken Laudon, Jane Laudon, Rajnish Dass, Management Information System, 11th Ed, Pearson, 2010.
2. Rojer S. Pressman, Software Engineering, A Practitioner's Approach, Fourth Edition, 1997.
3. Sophos Security Threat Report 2013.na.1.13
4. Amazon Web Services: Overview of Security Processes, aws.amazon.com/security, June 2013.
5. Office 365 Security, www.microsoft.com, 2013.
6. Strategic Anti-Malware Monitoring with Nessus, PVS, and LCE, White Paper, www.tenable.com, June 2013.
7. SANS 2013 Critical Security Controls Survey: Moving from Awareness to Action, White Paper, www.sans.org, June 2013.
