

DRAFT

Information Security Governance: What, How and Why of IS Security

(N.Nagarajan, (CIA, CISA, CISM, CFE), O/o. CAG of India)

Abstract: IT has become an integral part of everyday business and private life, though new technologies give unprecedented functionality it introduces new risks and environment harder to control. Increased dependency on IT means higher impact when things go wrong. A security breach will have a major impact. All are concerned about the privacy of their information and business losses and hence information security has become a part of IT Governance and corporate governance

Introduction

- a. Credit card information of 40 million customers stolen: Times of India, 10/08/06
- b. BPO scams can happen anywhere in the world: UK Economic Times, 16/09/06
- c. European companies to splurge on BPO services “Spend on financial services’ Back office, procurement& customer care to rise to \$ 35 billion by 2011, Economic Times, 30/09/06 etc.,

What does this indicate, Why does this happen and How does it affect

All these questions lead to an answer about information security. Widespread use of internet, handheld and portable computer devices, mobile and wireless technologies have made access to data and information easy and accessible and affordable. On the other hand these developments causes new opportunities for information technology related problems to occur, such as theft of data, malicious attacks using viruses, hacking, denial of service. These risks as well as potential for careless mistakes can result in serious financial, reputation and other damages.

Security relates to protection of valuable assets, in our case it is information recorded, processed, stored, and transmitted. The information must be protected from harm from threats leading to loss, non availability, alteration and wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional changes. ¹The objective of information security is protecting the interest of those relying on information and systems from the harm resulting from failure of availability, confidentiality and integrity. The security objective can be considered as achieved when the information is disclosed to only those who have the right to know (confidentiality), information is protected against unauthorized changes (integrity), information systems are available and usable (availability), and transactions are not disputed (Nonrepudiation and authenticity). Thus, Information Security is a key aspect of information technology governance.

DRAFT

What is the impact

Loss of business for commercial organizations, loss of privacy and lawsuits if the organization is in a country that has strict privacy laws and the most important one that shall directly affect organizations like ours is loss of confidence. Most Supreme Audit Institutions deals with sensitive, confidential and classified information during the course of audit and all along we have been able to safeguard the faith imposed on us from leakage of information provided to us. Can we afford to forego this faith the organization have in us. Answer is simple NO. We can't afford to forego this faith at any cost. Now many of our auditee organizations have computerized to a large extent and the necessity to safeguard also grown beyond the level of imagination and we have to gear up to compensate the growing threat.

Information Security Gap

Information Systems can generate many direct and indirect benefits and as many direct and indirect risks. These risks have led to the gap between the need to protect systems and the degree of protection applied. The gap is caused by

- widespread use of technology
- interconnectivity of the system
- elimination of distance, time and space as constraints
- unevenness of technological changes
- devolution of management and control
- attractiveness of conducting unconventional electronic attacks against organizations
- external factors such as legislative, legal and regulatory requirements

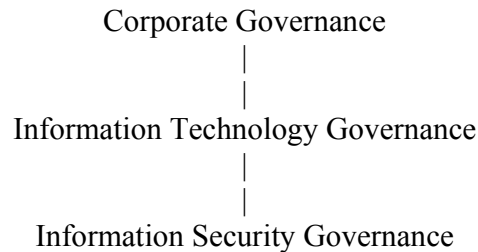
all these results in new risks that could have significant impact on critical business operations such as

- Increasing requirements for availability and robustness
- Growing potential for misuse and abuse of information systems affecting privacy and ethical values
- External dangers from hackers, leading to denial of service and virus attacks, extortion and leakage of corporate information

How does IS Security Governance Fits in to overall Corporate Governance

IS security is a complex subject, to protect environment one must understand the environment, fixes to be applied, difference between vendor applications and hardware variations and how attacks are preferred

DRAFT



In the present day scenario information and information systems has become an essential aspect of any business. It has graduated from facilitator and information provider to that of effective decision making ability and help in improving efficiency. Growing dependence of most organizations on their information systems have provided problems such as theft of data, attacks using malicious code, denial of service etc, new opportunities for IT related issues coupled with risks have made IT Governance an increasingly critical facet of overall governance. Information security is not just a technology problem, it is a business issue, it was seen as a negative factor creating value through nonoccurrence. However as a result of global networking and extending the enterprise beyond its traditional boundaries, it is emerging as a value creator and opportunity builder in its own right by building trust among stakeholders. The risks as well as careless mistakes can result in serious financial, reputational and other damages. In order to safeguard the organization from loss and reputation, confidentiality, integrity and availability of data needs to be protected and thus information security has emerged as key aspect of IT Governance.

Stakeholders are becoming more and more concerned about the information security as news of hacking, data theft and other attacks happen more frequently than ever dreamt of. Executive management has been showered with the responsibility of ensuring an organization provides users with secure information systems environment. Furthermore the organizations need to protect themselves against the risks inherent in the use of information systems while simultaneously recognizing the benefits that can accrue from having secure information systems. Thus as dependence on information system increases, the criticality of information security brings with it the need for effective information security governance

An information security program is a risk mitigation method like other control and governance. IT governance itself is emerging as an integral part of corporate governance with the goal of ascertaining that IT is aligned with business, enables the achievement of business goals and maximizes benefits, IT resources are used responsibly and IT related risks are managed appropriately

Of all the IT Governance issues it is imperative that IS Security governance plays a major role. Though the controls are to be inbuilt in the system to safeguard. It rarely happens

DRAFT

may be because of the fact that the field as such is growing at a phenomenal speed and it is impossible to comprehend all the security issues in the beginning and provide for security, because the breach may happen from any side, anywhere and at anytime.

Principles of Information Security

Organisations have diverse needs and will vary their approaches to information security governance, Corporate Governance Task force has identified core set of principles to help guide their efforts. By reviewing these principles internally, organizations can develop a program that is best tailored to their needs².

1. CEO's have an annual information security evaluation conducted, review evaluation results with staff and report on performance
2. Organisations should conduct periodic risk assessment of information assets as part of risk management program
3. Organisations should implement policies and procedures based on risk assessment to secure information assets
4. Organisations should have a security management structure
5. Organisations should plan and initiate action to provide adequate information security for networks, facilities, systems and information and test regularly
6. Organisations should provide information security awareness, training and education to personnel
7. Organisation should create and execute a plan for remedial action to address any information security deficiencies
8. Organisation should develop and implement incident response procedures
9. Organisations should use security best practices guidelines, to measure information security performance

Six major activities involved in Information Security are

1. Policy development, 2. Specification of roles and responsibilities, 3. design –developing a security control framework, 4. implementing a solution, 5. monitoring and finally awareness, 6. training and education.

The speed with which risks emerge and the rate of change require a different and continuous approach. It implies continuous monitoring and testing of infrastructure and environment for vulnerabilities and required response in terms of security fixes through security management functions.

What should IS Security Governance deliver

Should provide strategic alignment, value delivery, risk management and performance measurement

1. Strategic alignment

- Security requirement driven by enterprise requirements

DRAFT

- Security solutions fit for enterprise processes
- Investment in information security aligned with enterprise strategy and agreed upon risk profile

2. Value delivery

- A standard set of security practices (baseline security following best practices)
- Properly prioritized and distributed effort to areas with great impact and business benefit
- Institutionalized and commoditised solutions
- Complete solutions covering organization and process as well as technology
- A continuous improvement culture

3. Risk Management

- Agreed upon risk profile
- Understanding of risk exposure
- Awareness of risk management priorities

4. Performance measurement

- Defined set of metrics
- Measurement process with feedback on progress made
- Independence assurance

If IS Security is not aligned with IT governance and Corporate Governance

If all the three are not aligned well there shall exist a huge disconnect and the organizations not aligned well will not get the value from their IT functions and ultimately may result in not achieving the objective set forth by the organization. It shall not make any business sense if not aligned. Only those organizations aligned shall reap the benefit. One must understand that this is not just the IT issue it is business issue, one must especially the senior management must understand that any mis coordination may result in loss of business advantages

Risks of Information Security

Physical damage (fire, water and natural disasters)

Human error (accidental / intentional)

Equipment mal functions (failure of systems and peripheral devices)

Inside and outside attacks (hacking, cracking and other attacks)

Misuse of data (sharing trade secrets, espionage, fraud and theft)

Application error (computational errors, input errors, buffer overflows)

Risk analysis

DRAFT

Method of identifying risks, assessing the possible damage that could be caused to justify security safeguards. It is used to ensure that security is cost effective, relevant, timely and responsive to threats. Risk analysis helps to integrate security program objectives with company's business objectives and requirements. All these are required to be properly aligned for the success of the organization

Vulnerabilities that lie in web based activities

- Incorrect configuration at firewall
- Web servers not hardened and are open to attacks to operating system and applications
- Middle tier that do not give right combination and detailed security
- Back end servers that accept request from any source
- Not running intrusion detection to watch suspicious activities
- Routers that send packets instead of routing them properly

Since, programming are done mainly to provide functionality to the users of the system the security related issues are not given adequate importance it needs. And, hence most of the exploited vulnerabilities are with in the code of operating system and application.

Layered approach to protect large systems

- Understand the environment that needs to be protected
- To check unforeseen situations
 - Have the software patches and devices checked and tested
 - Have an intrusion detection system established in vulnerable segments of network
 - Have scheduled security scans to seek new vulnerabilities
 - Have up to date knowledge of security compromises
 - Keep intrusion detection and anti virus signatures up to date

In order to get the full benefit IT auditor should know

Auditor should understand how system process business information, IT risks associated with it, underlying technologies and how IT is being managed (e.g) SAP one can understand the flow of transaction, but, cannot really understand how to control unless one know how the system is put together and how it works

Auditor should understand how system works, what are the risks and how controls works against the risks in an IT environment, what are the roles of controls such as access control and security in the process. How does the system development, system maintenance, system updates affect the reliability of the process

IT Auditors have to be more business focused. They have to combine technical skills with soft skills such as understanding the business, communicating, presenting ideas both

DRAFT

upstream and downstream and should be able to think strategically and analyse problems critically

Always not necessary to purchase the newest security software, but necessary to be aware of where the risks can evolve and take steps to prevent it

Six simple steps to added security³

- Change the default password
- Change service set identifier (SSID)
- Specify authorized media access control addresses
- Limit devices connected at one time
- Enable an encryption solution
- Disable devices during non business hours

Conclusion

There is no such thing as 100 percent security, IT environment keep changing, new security risks can occur at any time. The amount of effort applied to implementing a safe and secure working environment should be based on how much of an impact a security problem could cause to the business

However, implementing good security does not necessarily mean investing large amount of time and expense. For example raising awareness, recognizing the risks that can occur and taking sensible precautions can be achieved with little effort

Amount of protection required depends on how likely a security risk may occur and how big an impact it would have if it occurs. Protection is achieved through a combination of technical and non technical safeguards. For large enterprises protection will be a major task with a layered series of safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics and firewalls.

In the ever-changing technological environment, security that is state of the art today may be obsolete tomorrow. Therefore security protection must keep pace with these changes.

“Information security provides the management processes, technology and assurance to allow business management to ensure business transactions can be trusted; ensure IT services are usable and can resist and recover from failures due to error, attacks or disaster; and ensure critical confidential information is withheld from those who should not have access to it”⁴

DRAFT

References:

1. COBIT SECURITY BASELINE, An Information Security Survival Kit.
2. Information Security Governance, (corporate Governance Task Force Report) a call to action
3. Bryce H. Peterson, HBPM, Network+ Senior Associate, KPMG, LLP
4. Dr. Paul Dorey, director, digital business security, BP Plc.