INFORMATION SECURITY GOVERNANCE: WHAT, HOW & WHY OF IS SECURITY

N.NAGARAJAN, CIA, CISA, CISM, CFE
OFFICE OF THE COMPTROLLER AND
AUDITOR GENERAL OF INDIA

Abstract: IT has become an integral part of everyday business and private life. Although new technologies give unprecedented functionality they introduce new risks and an IT environment is harder to control. Increased dependency on IT means a greater impact when things go wrong and a security breach will have a major impact. Everyone is 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, 10/08/2006*

b. BPO scams can happen anywhere in the world: UK *Economic Times, 16/09/2006*

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, 30/09/2006*

What does this indicate, why does this happen and what does it affect?

All these questions lead to an answer about information security. Widespread use of the internet, handheld and portable computer devices, mobile and wireless technologies have made access to data and information easy, accessible and affordable. On the other hand these developments cause 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, reputational and other damages.

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

What is the impact?

Loss of business for commercial organisations, loss of privacy and lawsuits if the organisation is in a country that has strict privacy laws and the most important one that directly affects organisations like ours is loss of confidence. Most Supreme Audit Institutions deal with sensitive, confidential and classified information during the course of audit and all along we have been able to safeguard the trust put upon us from leakage of information provided to us. Can we afford to forego this faith that organisations have in us? The simple answer is NO. We cannot afford to forego this trust at any cost. Now many of our auditees have computerised to a large extent and the necessity to safeguard has also grown beyond the level of imagination and we have to gear up to deal with the growing threat.

IT governance

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

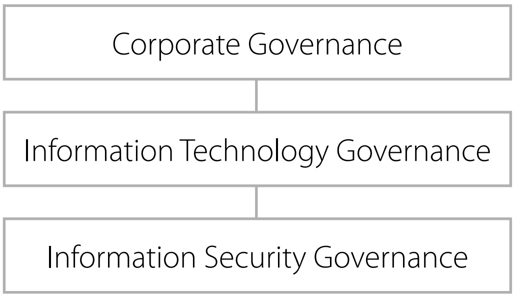
- widespread use of technology
- interconnectivity of the system
- elimination of distance, time and space as constraints
- unevenness of technological changes
- devolution of management and control
- attractiveness of conducting unconventional electronic attacks against organisations
- external factors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

All these result 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 fit into overall Corporate Governance

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



Corporate Governance

Information Technology Governance

Information Security Governance

Information and information systems have become an essential aspect of any business. They have graduated from facilitator and information provider to that of effective decision making ability and help in improving efficiency. The growing dependence of most organisations on their information systems have provided problems such as theft of data, attacks using malicious code, denial of service etc, and 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, seen as a negative factor creating value through non-occurrence. 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. Risks as well as careless mistakes can result in serious financial, reputational and other damage. In order to safeguard the organisation from loss of reputation, the 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 information security as examples of hacking, data theft and other attacks occur more frequently than ever. Executive management has been given the responsibility of ensuring an organisation provides users with a secure information systems environment. Furthermore the organisations need to protect themselves against the risks inherent in the use of information systems while simultaneously recognising 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 controls 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 maximises 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. Although controls should be built into the system this rarely happens, maybe 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 any time.

Principles of Information Security

Organisations have diverse needs and will vary their approaches to information security governance. The Corporate Governance Task force has identified a core set of principles to help guide their efforts. By reviewing these principles internally, organisations can develop a programme that is best tailored to their needs[2] .

- CEOs should conduct an annual information security evaluation, and review evaluation results with staff and report on performance.
- Organisations should conduct periodic risk assessment of information assets as part of risk management programme.
- Organisations should implement policies and procedures based on risk assessments to secure information assets.
- Organisations should have a security management structure.
- Organisations should plan and initiate action to provide adequate information security for networks, facilities, systems and information and test regularly.
- Organisations should provide information security awareness, training and education to personnel.
- Organisations should create and execute a plan for remedial action to address any information security deficiencies.
- Organisation should develop and implement incident response procedures.
- 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,
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

IS Security Governance should provide strategic alignment, value delivery, risk management and performance measurement.

Strategic alignment

- Security requirement driven by enterprise requirements
- Security solutions fit for enterprise processes
- Investment in information security aligned with enterprise strategy and agreed risk profile

Value delivery

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

Risk Management

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

Performance measurement

- Defined set of metrics
- Independence assurance

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

If all the three are not aligned well there will be a huge disconnect and the organisations not aligned well will not get value from their IT functions and ultimately may not achieve the objectives of the organisation. It will not make any business sense if not aligned. Only those organisations aligned will reap the benefit. One must understand that this is not just an IT issue, it is a business issue, and senior management especially must understand that any mis-coordination may result in loss of business advantage.

Risks of Information Security

- Physical damage (fire, water and natural disasters)
- Human error (accidental / intentional)
- Equipment malfunction (failure of systems and peripheral devices)
- Inside and external attack (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

Risk analysis is a 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 programme objectives with the company's business objectives and requirements. All these are required to be properly aligned for the success of the organisation.

Vulnerabilities that lie in web based activities

- Incorrect configuration of firewalls
- Web servers not hardened and open to attack on operating system and applications
- Middle tiers that do not give right combination and detailed security
- Back end servers that accept requests from any source
- Not running intrusion detection to watch for suspicious activities
- Routers that send packets instead of routing them properly

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

Layered approach to protect large systems

- Understand the environment that needs to be protected
- Make sure software patches and devices are checked and tested
- Have an intrusion detection system established in vulnerable segments of networks
- Make scheduled security scans to seek new vulnerabilities
- Maintain up to date knowledge of security compromises
- Keep intrusion detection and anti virus signatures up to date

IT auditors

The IT Auditor should understand how systems process business information, the IT risks associated with it, underlying technologies and how IT is being managed. One can understand the flow of transactions, but cannot really understand how to control the system unless one knows how the system is put together and how it works.

The IT Auditor should understand how systems work, what the risks are and how controls work against the risks in an IT environment, what the roles are of controls such as access control and security in the process, and how system development, system maintenance, and system change 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 upstream and downstream and should be able to think strategically and analyse problems critically.

It is not always necessary to purchase the latest security software, but it is necessary to be aware of where the risks can evolve and take steps to prevent them.

Six simple steps to added security[3]

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

Conclusion

There is no such thing as total security, IT environments 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 amounts of time and expense. For example, raising awareness, recognising the risks that can occur and taking sensible precautions can be achieved with little effort.

The 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]

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, LLPnn

4 Dr. Paul Dorey, director, digital business security, BP Plc.