DESIGN AND ANALYSIS OF STRATEGIC BUSINESS INFORMATION SECURITY CONTROL MODEL

MR. RAHUL MOHARE*; DR. U A LANJEWAR**; MR. KRUNAL PAREKH***

*Faculty-MBA Department,
Datta Meghe Institute of Management Studies,
RTM Nagpur University,
Atrey Layout, Nagpur.
**Professor,
MCA Department,
VMV-JMT-JJP Science Collge,
RTM Nagpur University,
Wardhaman Nagar, Nagpur.
***Faculty-MBA Department,
Datta Meghe Institute of Management Studies,
RTM Nagpur University,
Atrey Layout, Nagpur.

ABSTRACT

Information is one of the most important assets of any institution. Protection of information assets is necessary to establish and maintain trust between the institution and its customers, maintain compliance with the law, and protect the reputation of the institution. Timely and reliable information is necessary to process transactions and support any institution and customer decisions. Any institution’s earnings and capital can be adversely affected if information becomes known to unauthorized parties, is altered, or is not available when it is needed.

In this paper we have introduced a information security control model by virtue of which any institution can determine their data security in best possible way, the aspects we have explored are Access, physical & Environment protection, encryption, malicious code prevention, personal and data security and many more.

1. INTRODUCTION

Information security is the process by which an organization protects and secures its data, systems and facilities that process and maintains information which is important to its operations. Security is an ongoing process, whereby the condition of any institution’s controls is just one indicator of its overall security posture. Other indicators include the ability of the institution to continually assess its position and react appropriately in the face of rapidly changing threats, technologies, and business conditions. Information security enables any institution or organisation to meet its business objectives by implementing business systems with due consideration of information technology (IT)- related risks to the organization, business and trading partners, technology service providers, and customers. Organizations meet this goal by striving to accomplish the following objectives.
Availability—the ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems.

Integrity of Data or Systems—System and data integrity relate to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.

Confidentiality of Data or Systems—Confidentiality covers the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use.

Accountability—Clear accountability involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.

Assurance—Assurance addresses the processes, policies, and controls used to develop confidence that technical and operational security measures work as intended. Assurance levels are part of the system design and include availability, integrity, confidentiality, and accountability. Assurance highlights the notion that secure systems provide the intended functionality while preventing undesired actions.

2. BUSINESS INFORMATION SECURITY CONTROL MODEL

The primary objective of information security is to protect the confidentiality, integrity, and availability of the institution’s information assets; here we are introducing a Business Information Security Control Model which will explore many aspects related to the controlling of Information Security.
3. ACCESS CONTROL

The goal of access control is to allow access by authorized individuals and devices and to disallow access to all others. Authorized individuals may be employees, technology service provider (TSP) employees, vendors, contractors, customers, or visitors. Access should be authorized and provided only to individuals whose identity is established.

Authorized devices are used, whose placement on the network is approved in accordance with institution policy. An effective control mechanism includes numerous controls to safeguard and limits access to key information system assets at all layers in the network.
Management and information system administrators should critically evaluate information system access privileges and establish access controls to prevent unnecessary access. Access rights should be based upon the needs of the applicable user to carry out legal and approved activities on the any institution’s information systems. Policies, procedures, and criteria need to be established for both the granting of appropriate access rights and for the purpose of establishing those legitimate activities.

Formal access rights administration for users consists of four processes:

- An enrollment process to add new users to the system;
- An authorization process to add, delete, or modify authorized user access to operating systems, applications, directories, files, and specific types of information;
- An authentication process to identify the user during subsequent activities; and
- A monitoring process to supervise and manage the access rights granted to each user.

Authorization for privileged access should be tightly controlled. Privileged access refers to the ability to override system or application controls. Good practices for controlling privileged access include:

- Identifying each privilege associated with each system component,
- Implementing a process to allocate privileges and allocating those privileges either on a need-to-use or an event-by-event basis,
- Documenting the granting and administrative limits on privileges,
- Assigning privileges to a unique user ID apart from the one used for normal business use,
- Logging and auditing the use of privileged access,
- Reviewing privileged access rights at appropriate intervals and regularly reviewing privilege access allocations, and
- Prohibiting shared privileged access by multiple users.

4. PHYSICAL AND ENVIRONMENTAL PROTECTION

The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. Conceptually, those physical security risks are mitigated through zone-oriented implementations. For instance, data centers may be in the highest security zone, and branches may be in a much lower security zone. Different security zones can exist within the same structure. Routers and servers in a branch, for instance, may be protected to a greater degree than customer service terminals. Computers and
telecommunications equipment within an operations center will have a higher security zone than I/O operations. The requirements for each zone should be determined through the risk assessment. The Zones that need highest security are

**DATA CENTER SECURITY**

When selecting a site for the most important information systems components, one major objective is to limit the risk of exposure from internal and external sources. The selection process should include a review of the surrounding area to determine if it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Detection devices, where applicable, should be utilized to prevent theft and safeguard the equipment. They should provide continuous coverage. Detection devices have two purposes—to alarm when a response is necessary and to support subsequent forensics. The alarm capability is useful only when a response will occur.

**PHYSICAL SECURITY IN DISTRIBUTED IT ENVIRONMENTS**

Hardware and software located in a user department are often less secure than that located in a computer room. Distributed hardware and software environments (e.g., local area networks or LANs) that offer a full range of applications for small institutions as well as larger organizations are commonly housed throughout the organization, without special environmental controls or raised flooring. Because of their portability and location in distributed environments, personal computers (PCs) often are prime targets for theft and misuse. The location of PCs and the sensitivity of the data and systems they access determine the extent of physical security required. Physical security for distributed IT, particularly LANs that are usually PC-based, is slightly different than for mainframe platforms. Physical protection for networks as well as PCs includes power protection, physical locks, and secure work areas enforced by security guards and authentication technologies such as magnetic badge readers. Physical access to the network components (i.e., files, applications, communications, etc.) should be limited to those who require access to perform their jobs. Network workstations or PCs should be password protected and monitored for workstation activity.

5. **ENCRYPTION**

Encryption is used to secure communications and data storage, particularly authentication of credentials and the transmission of sensitive information. It can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols. Encryption can be used as a preventive control, a detective control, or both. As a prevention control, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to allow discovery of unauthorized changes to data and to assign responsibility for data among authorized parties. When prevention and detection are joined, encryption is a key control in ensuring confidentiality, data integrity, and accountability. Encryption may also be used to protect data in storage. Encryption cannot guarantee data security. Even if encryption is properly implemented, for example, a security breach at one of the endpoints of the communication can be used to steal the data or allow an intruder to masquerade as a legitimate system user.
6. MALICIOUS CODE PREVENTION

Malicious code is any program that acts in unexpected and potentially damaging ways. Common types of malicious code are viruses, worms, Trojan horses, monitoring programs such as spyware, and cross-site scripts. The functions of each one is mutually exclusive; however, developers combined functions to create more powerful malicious code.

Malicious code can

- Replicate itself within a computer and transmit itself between computers.
- Change, delete, or insert data, transmit data outside the institution, and insert backdoors into institution systems.
- Attack institutions at either the server or the client level.
- Attack routers, switches, and other parts of the institution infrastructure. Malicious code can also monitor users in many ways, such as logging keystrokes and transmitting screenshots to the attacker. Typically malicious code is mobile, using e-mail, Instant Messenger, and other peer-to-peer (P2P) applications.

The code also can be hidden in programs that are downloaded from the Internet or brought into the institution on diskette. At times, the malicious code can be created on the institution’s systems either by intruders or by authorized users.

7. SYSTEMS DEVELOPMENT, ACQUISITION, AND MAINTENANCE

Any institutions obtain software through self-development, contracted development, the purchase of pre-written code, or variations of those development and acquisition approaches. The security issues associated with the approaches involve the security controls built into the code and the dependability of the code that is placed into the institution’s environment. The security features of the code can be assessed regardless of the means of development. The trustworthiness of the code, however, is ascertained differently depending on the availability of information necessary to perform an assessment.

Test data consisting of institution data or customer data frequently is used in development tests or certifications. Appropriate risk improvement techniques should be employed to protect that data from unauthorized disclosure. Any institutions that introduce trustworthy systems into their environment should ensure that the systems retain the same trustworthiness over time. Essential control elements are the development of appropriately hardened systems, usage of standard builds, the appropriate updating of builds and deployed systems through patch management, and the controlled introduction of changes into the institution’s environment.

When deploying off-the-shelf software, management should harden the resulting system. Hardening includes the following actions:
Determining the purpose of the system and minimum software and hardware requirements;

- Documenting the minimum hardware, software, and services to be included on the system;

- Installing the minimum hardware, software, and services necessary to meet the requirements using a documented installation procedure;

- Installing necessary patches;

- Installing the most secure and up-to-date versions of applications;

- Configuring privilege and access controls by first denying all, then granting back the minimum necessary to each user;

- Configuring security settings as appropriate, enabling allowed activity, and disallowing other activity;

- Creating cryptographic hashes of key files;

- Archiving the configuration and checksums in secure storage prior to system deployment;

- Testing the system to ensure a secure configuration;

- Using secure replication procedures for additional, identically configured systems, making configuration changes on a case-by-case basis;

- Changing all default passwords; and

8. PERSONNEL SECURITY

Application owners grant legitimate users system access necessary to perform their duties; security personnel enforce access rights in accordance with institution standards. Because of their internal access levels and intimate knowledge of any institution’s process, authorized users pose a potential threat to systems and data. Employees or contractors can exploit their legitimate computer access for malicious, counterfeit, or economic reasons. Additionally, the degree of internal access granted to some users increases the risk of accidental damage or loss of information and systems. Risk exposures from internal users include

- Altering data,

- Deleting production and back-up data,

- Disrupting and Destroying systems,

- Misusing systems for personal gain or to damage the institution,
Holding data hostage, and

Stealing strategic or customer data for corporate espionage or fraud schemes.

9. DATA SECURITY

The primary objective of information security is to protect the confidentiality, integrity, and availability of the institution’s information assets. All of the controls discussed so far contribute to the achievement of that objective. However, not all data in an institution require the same protections as other data, and not all data remain within the institution’s physical perimeter.

Data Security policies include

- Contractual requirements that incorporate necessary risk-based controls,
- Restrictions on the carriers used and procedures to verify the identity of couriers,
- Requirements for appropriate packaging to protect the media from damage,
- Use of encryption for transmission or transport of sensitive information,
- Tracking of shipments to provide early indications of loss or damage,
- Security reviews or independent security reports of receiving companies, and
- Use of nondisclosure agreements between couriers and third parties.

10. SERVICE PROVIDER OVERSIGHT

Many institutions outsource some aspect of their operations. Although outsourcing arrangements often provide a cost-effective means to support the institution’s technology needs, the ultimate responsibility and risk rests with the institution. Any institutions are required to ensure service providers have implemented adequate security controls to safeguard customer information. The guidelines require institutions to

- Exercise appropriate due diligence in selecting service providers,
- Require service providers by contract to implement appropriate security controls to comply with the guidelines, and
- Monitor service providers to confirm that they are maintaining those controls when indicated by the institution’s risk assessment.

Any institutions should implement these same precautions in all TSP relationships based on the level of access to systems or data for safety and soundness reasons, in addition to the privacy
requirements. Any institutes institutions should evaluate the following security considerations when selecting a service provider:

- Service provider references and experience,
- Security expertise of TSP personnel,
- Background checks on TSP personnel,
- Contract assurances regarding security responsibilities and controls,
- Nondisclosure agreements covering the institution’s systems and data
- Ability to conduct audit coverage of security controls or obtain adequate reports of security testing from independent third parties, and

11. BUSINESS CONTINUITY CONSIDERATIONS

Events that trigger the implementation of a business continuity plan may have significant security implications. Depending on the event, some or all of the elements of the security environment may change. Different people may be involved in operations, at different physical locations, using similar but different machines and software which may communicate over different communications lines. Different tradeoffs may exist between availability, integrity, confidentiality, and accountability, with a different appetite for risk on the part of management. Business continuity plans should be reviewed as an integral part of the security process. Risk assessments should consider the changing risks that appear in business continuity scenarios and the different security posture that may be established. Strategies should consider the different risk environment and the degree of risk mitigation necessary to protect the institution in the event the continuity plans must be implemented. The implementation should consider the training of appropriate personnel in their security roles, and the implementation and updating of technologies and plans for back-up sites and communications networks. These security considerations should be integrated with the testing of business continuity plan implementations.

12. INSURANCE

Any institutions use insurance coverage as an effective method to transfer risks from themselves to insurance carriers. Coverage is increasingly available to cover risks from security breaches or denial of service attacks. Several insurance companies offer commerce insurance packages that can reimburse any institutions for losses from fraud, privacy breaches, system downtime, or incident response. When evaluating the need for insurance to cover information security threats, any institutions should understand the following points:

- Insurance is not a substitute for an effective security program.
- Traditional loyalty bond coverage may not protect from losses related to security intrusions.
Availability, cost, and covered risks vary by insurance company.

Availability of new insurance products creates a more dynamic environment for these factors.

Insurance cannot adequately cover the reputation and compliance risk related to customer relationships and privacy.

Insurance companies typically require companies to certify that certain security practices are in place.

Insurance coverage is rapidly evolving to meet the growing number of security-related threats. Coverage varies by insurance company, but currently available insurance products may include coverage for the following risks:

- Denial-of-service attacks;
- Loss of income;
- Computer extortion associated with threats of attack or disclosure of data;
- Theft of confidential information;
- Privacy violations;
- Litigation (breach of contract);
- Destruction or manipulation of data (including viruses);
- Fraudulent electronic signatures on loan agreements;
- Fraudulent instructions through e-mail;
- Third-party risk from companies responsible for security of any institute institutions systems or information;
- Insiders who exceed system authorization; and
- Incident response costs related to the use of negotiators, public relations consultants, security and computer forensic consultants, programmers, replacement systems, etc.

13. CONCLUSION

Although there are still practical modeling issues that need to be refined and configured before this model can be used in practice, it does provide a benchmark framework that will, when fully developed, determine the cost efficiency, and to a lesser extent, the cost effectiveness, of an
Information Security environment. Certain areas need to be researched and defined in greater detail, and aspects such as the impact of service levels and best practice implementation must still be qualified – their impact on efficiency and expenditure also needs to be determined and quantified. Further development of this framework will focus on ensuring that the benchmark model is practical, comprehensive and fair, and that it can be implemented by and used within organisations to assess their Business Information Security environments, regardless of industry or geography.

14. BIBLIOGRAPHY


