Network security essentials-IV

Introduction

Network Security Essentials

15-02-2020 Network security-IV:

Information Systems Controls
Risk Assessment
Case analysis
Degree of Impact and vulnerabilities determine controls
Symentec Report
Security Policy
Access Rules for a Personnel System
Disaster Recovery Planning and Business Continuity Planning
The Role of Auditing
Sample Auditor’s List of Control Weaknesses
Business Continuity Management
Indian Computer Emergency Response Team
Summary of Risk Management
Summary of Development of security policy

Learning objectives

- Information Systems Controls
- Risk Assessment
- Case analysis
- Degree of Impact and vulnerabilities determine controls
- Symentec Report
- Security Policy
- Access Rules for a Personnel System
- Disaster Recovery Planning and Business Continuity Planning
- The Role of Auditing
- Sample Auditor's List of Control Weaknesses
- **Business Continuity Management**
- **Indian Computer Emergency Response Team**
- Summary of Risk Management
- Summary of Development of security policy

- **Real life CASE studies and Discussion on industry situation of cyber security analysis**
- **Further reading materials are also provided including how electricity is under cyber security attack and relevant analysis of threat.**

What Is the Business Value of Security and Control?

- Failed computer systems can lead to significant or total loss of business function
- Firms now are more vulnerable than ever
  - Confidential personal and financial data
  - Trade secrets, new products, strategies
- A security breach may cut into a firm's market value almost immediately
- Inadequate security and controls also bring forth issues of liability

Information Systems Controls

- May be automated or manual
- General controls
  - Govern design, security, and use of computer programs and security of data files in general throughout organization
  - Software controls, hardware controls, computer operations controls, data security controls, system development controls, administrative controls,
- Application controls
  - –Controls unique to each computerized application
  - –Input controls, processing controls, output controls

Types of General Control

TYPE OF GENERAL CONTROL	DESCRIPTION
Software controls	Monitor the use of system software and prevent unauthorized access of software programs, system software, and computer programs.
Hardware controls	Ensure that computer hardware is physically secure, and check for equipment malfunction. Organizations that are critically dependent on their computers also must make provisions for backup or continued operation to maintain constant service.
Computer operations controls	Oversee the work of the computer department to ensure that programmed procedures are consistently and correctly applied to the storage and processing of data. They include controls over the setup of computer processing jobs and backup and recovery procedures for processing that ends abnormally.
Data security controls	Ensure that valuable business data files on either disk or tape are not subject to unauthorized access, change, or destruction while they are in use or in storage.
Implementation controls	Audit the systems development process at various points to ensure that the process is properly controlled and managed.
Administrative controls	Formalize standards, rules, procedures, and control disciplines to ensure that the organization's general and application controls are properly executed and enforced.

Application controls focus on the following objectives:

1. **Completeness of input and update.** All current transactions must reach the computer and be recorded on computer files.

2. **Accuracy of input and update.** Data must be accurately captured by the computer and correctly recorded on computer files.

3. **Validity.** Data must be authorized or otherwise checked with regard to the appropriateness of the transaction. (In other words, the transaction must reflect the right event in the external world. The validity of an address change, for example, refers to whether a transaction actually captured the right address for a specific individual.)

4. **Maintenance.** Data on computer files must continue to remain correct and current.

Risk Assessment

- Determines level of risk to firm if specific activity or process is not properly controlled
    - Types of threat
    - Probability of occurrence during year
    - Potential losses, value of threat
    - Expected annual loss

Online Order Processing Risk Assessment

EXPOSURE	PROBABILITY OF OCCURRENCE	LOSS RANGE (AVERAGE) ($)	EXPECTED ANNUAL LOSS ($)
Power failure	30%	$5,000 - $200,000 ($102,500)	$30,750
Embezzlement	5%	$1,000 - $50,000 ($25,500)	$1275
User error	98%	$200 - $40,000 ($20,100)	$19,698

This table shows the results of a risk assessment of three selected areas of an online order processing system. The likelihood of each exposure occurring over a one-year period is expressed as a percentage. The next column shows the highest and lowest possible loss that could be expected each time the exposure occurred and an “average” loss calculated by adding the highest and lowest figures together and dividing by 2. The expected annual loss for each exposure can be determined by multiplying the “average’ loss by its probability of occurrence.

Degree of Impact and vulnerabilities determine controls

	Severe impact	Significant impact	Minor impact
Severe vulnerabilities	Conduct vulnerability analysis **Must improve controls**	Conduct vulnerability analysis **Must improve controls**	vulnerability analysis unnecessary
Medium vulnerabilities	Conduct vulnerability analysis **Should improve controls**	Conduct vulnerability analysis **Should improve controls**	vulnerability analysis unnecessary
Low vulnerabilities	Conduct vulnerability analysis **Keep controls intact**	Conduct vulnerability analysis **Keep controls intact**	vulnerability analysis unnecessary

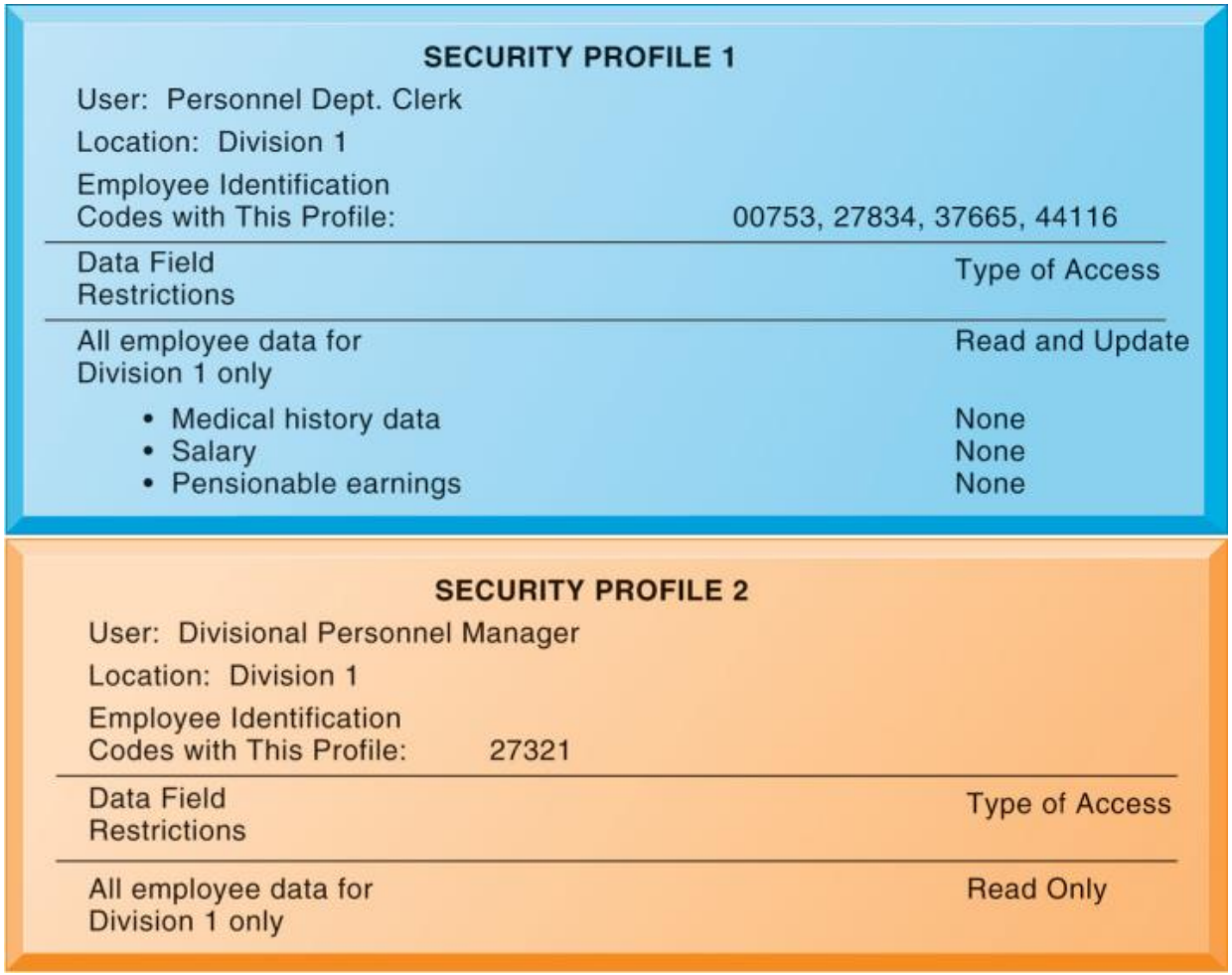
Symentec Report

- Low severity (0-3) – Vulnerabilities that constitute a minor threat. Attackers cannot exploit these vulnerabilities across a network and successful exploitation does not result in a complete compromise of the information stored on or transmitted across the system.
  - Low-severity vulnerabilities include non-critical losses of confidentiality (for example, system configuration exposure) or non-critical losses of integrity (for example, local file corruption).
- Moderate severity (4-7) – Vulnerabilities that result in a partial compromise of the affected system. An attacker may gain elevated privileges but does not gain complete control of the targeted system.
  - Moderately severe vulnerabilities include those for which the impact on systems is high but accessibility to attackers is limited. This includes vulnerabilities that require the attacker to have local access to the system or to be authenticated before the system can be exploited.
- High severity (8-10) – Vulnerabilities that result in a compromise of the entire system if exploited. In almost all cases, successful exploitation can result in a complete loss of confidentiality, integrity, and availability of data stored on or transmitted across the system.
  - High severity vulnerabilities will allow attackers access across a network (that is, remotely) without authentication

Security Policy

- Ranks information risks, identifies acceptable security goals, and identifies mechanisms for achieving these goals
- Drives other policies
  - Acceptable use policy (AUP)
    - Defines acceptable uses of firm's information resources and computing equipment
- Identity management
  - Identifying valid users
  - Controlling access

Access Rules for a Personnel System



SECURITY PROFILE 1

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

Disaster Recovery Planning and Business Continuity Planning

- Disaster recovery planning
  - Devises plans for restoration of disrupted services
- Business continuity planning
  - Focuses on restoring business operations after disaster
- Both types of plans needed to identify firm's most critical systems
  - Business impact analysis to determine impact of an outage
  - Management must determine which systems restored first

Distinguish between disaster recovery planning and business continuity planning.

- Disaster recovery planning devises plans for the restoration of computing and communications services after they have been disrupted by an event such as an earthquake, flood, or terrorist attack.
- Disaster recovery plans focus primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services.
- Business continuity planning focuses on how the company can restore business operations after a disaster strikes.
- The business continuity plan identifies critical business processes and determines action plans for handling mission-critical functions if systems go down.

The Role of Auditing

- Information systems audit
  - Examines firm's overall security environment as well as controls governing individual information systems
- Security audits
  - Review technologies, procedures, documentation, training, and personnel
  - May even simulate disaster to test responses
- List and rank control weaknesses and the probability of occurrence
- Assess financial and organizational impact of each threat

Sample Auditor's List of Control Weaknesses

Function: Loans **Location: Peoria, IL**	**Prepared by: J. Ericson** **Date: June 16, 2016**		**Received by: T. Benson** **Review date: June 28, 2016**	
Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management	
	Yes/ No	Justification	Report date	Management response
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/16	Eliminate accounts without passwords
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/16	Ensure only required directories are shared and that they are protected with strong passwords
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status		

Business Continuity Management

- The activities aimed at ***continuing operations after an IS disruption*** are called **BCM**
- Consists of ***emergency plan*** (safety of employees when disaster strikes alarm/evacuation/fire suppression)
- ***Back up plan***(duplicated hardware, data etc., distributed IS, hot site and cold site back up)
- ***Vital records plan*** (paper, docs, microform, storage media etc. necessary for running firm's business)

Indian Computer Emergency Response Team

- The Indian Computer Emergency Response Team is an office within the Ministry of Electronics and Information Technology. It is the nodal agency to deal with cyber security threats like hacking and phishing. It strengthens security-related defence of the Indian Internet domain.

- https://www.cert-in.org.in/

Summary of Risk Management

- Identify business assets to be protected from risks
- Recognise the risks
- Determine the level of impact on the firm should the risk materialise
- Analyse firm's vulnerabilities

Risk analysis report should consists of

- A description of risk
- Source of risk
- Severity of risk
- Controls that are being applied to risk
- Owner's of the risk
- Recommended action to the risk
- Recommended time frame for addressing the risk

Summary of Development of security policy

Controls

- **Technical control**
- **Access control**
  - User identification(username/password)
  - User authentication (verify right to access by signature/smart card)
  - User authorisation(access level of access)
- **IDS (Intrusion Detection System)**
- **Firewall**
- **Cryptography**
- **Physical control**

- **Formal control(codes of conduct/documentation of policies/procedure/monitoring behaviour etc.)**
- **Informal control(training & educating, mdp etc.)**
- **Industry standard**

- **As per the home assignment communicated before this session followings will be now discussed.**

Interactive Session: Technology: BYOD: A Security Nightmare?

- **Class discussion**
  - **It has been said that a smartphone is a computer in your hand. Discuss the security implications of this statement.**
  - **What kinds of security problems do mobile computing devices pose?**
  - **What management, organizational, and technology issues must be addressed by smartphone security?**
  - **What steps can individuals and businesses take to make their smartphones more secure?**

  - **Please submit this assignment answer with your own answer not more than 2 pages**

Security analysis statistics: Analyze high risk, medium risk, and low risk vulnerabilities by type of computing platform.

SECURITY VULNERABILITIES BY TYPE OF COMPUTING PLATFORM

PLATFORM	NUMBER OF COMPUTERS	HIGH RISK	MEDIUM RISK	LOW RISK	TOTAL VULNERABILITIES
Windows Server (corporate applications)	1	11	37	19	67
Windows Vista Ultimate (high-level administrators)	3	56	242	87	1155
Linux (email and printing services)	1	3	154	98	255
Sun Solaris (UNIX) (e-commerce and web servers)	2	12	299	78	778
Windows Vista Ultimate user desktops and laptops with office productivity tools that can also be linked to the corporate network running corporate applications and intranet	195	14	16	1,237	247,065

Calculate the total number of vulnerabilities for each platform. What is the potential impact of the security problems for each computing platform on the organization?

- **The total number of vulnerabilities for each platform is indicated in the far right column of the table.**
- **Potential impact of the security problems for each computing platform**
  - **High-risk vulnerabilities:** Misuse of passwords allows hackers, crackers, and employees to access specific systems and files and steal data or change application programs; non-authorized users could change applications or enter corrupt or faulty data; unauthorized programs could corrupt data or programs.
  - **Medium-risk vulnerabilities:** Obviously it's not a good thing for users to be able to shut down systems—that should be restricted to high-level administrators; passwords and screen savers could allow viruses, worms, and Trojan horses to enter the system; outdated software versions make it more difficult to keep current software programs up-to-date and provide holes in which unauthorized users could enter a system.
  - **Low-risk vulnerabilities:** Users' lack of knowledge is the single greatest cause of network security breaches. Password systems that are too easy or too difficult compromise system security and could create unintentional vulnerabilities from internal or external threats.

If you only have one information systems specialist in charge of security, which platforms should you address first in trying to eliminate these vulnerabilities? Second? Third? Last? Why? (answer may vary with required justification)

- **First platform to protect: Windows Vista Ultimate (high-level administrators)—administrators usually have access to areas that no other users have. The tasks that administrators perform affect the core operations of a system.**
- **Second platform to protect: Windows Server (corporate applications)—if the corporate applications are down or corrupted, the entire organization will be unable to conduct business**
- **Third platform to protect: Sun Solaris (UNIX) (e-commerce and web servers) — after ensuring that internal operations are safe and secure, the next area to protect focuses on the ability to reach customers and for them to reach the company**
- **Fourth platform to protect: Windows Vista Ultimate user desktops and laptops —this area probably has fewer critical applications, files, and data than the corporate applications area.**
- **Last platform to protect: Linux (email and printing services)—while it may be critical to a few users, it's not likely the organization will suffer huge damage or losses if email and print services are down for a while.**

Identify the types of control problems illustrated by these vulnerabilities and explain the measures that should be taken to solve them.

- **General controls:** Govern the design, security, and use of computer programs and the security of data files in general throughout the organization's information technology infrastructure. General controls apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment.
  - Windows Vista Ultimate (high-level administrators)
  - Sun Solaris (UNIX) (e-commerce and web servers)

Contd… Identify the types of control problems

- **Application controls:** Specific controls unique to each computerized application, such as payroll or order processing. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application. Application controls can be classified as input controls, processing controls, and output controls.
    - Windows Server (corporate applications)
    - Linux (email and printing services)
    - Sun Solaris (UNIX) (e-commerce and web servers)
    - Windows Vista Ultimate user desktops and laptops

Contd… Identify the types of control problems

- **Measures that should be taken to solve them include:**
  - Create a security policy and an acceptable use policy.
  - Use authorization management systems.
  - Create a business continuity plan.
  - Complete an MIS audit that includes a security audit.
  - Apply access controls, firewalls, and antivirus/antispyware to system.
  - Install an intrusion detection management system.
- **Determine if fault-tolerant or high availability computing is necessary**

What does your firm risk by ignoring the security vulnerabilities identified?

- Information systems are vulnerable to technical, organizational, and environmental threats from internal and external sources. Managers at all levels must make system security and reliability their number one priority. They must also impress upon all employees how important security is throughout the system. There are several ways the business value of security and control can be measured:
- The Rupees/dollars a company spends to secure system.
- The amount of money spent to recover from system fraud and abuse.
- The lost revenue from system downtime.
- The amount of money spent on legal claims against a company if it experiences security breaches.
- The damage done to a company's reputation.

Cyber security decision making

- Steam is an online games platform that powers leading massively multiplayer online games. The Steam platform serves more than 15 million users. The games can accommodate millions of players at once and are played simultaneously by people all over the world.
- **Prepare a security analysis for this Internet-based business.**
- **What kinds of threats should it anticipate?**
- **What would be their impact on the business?**
- **What steps can it take to prevent damage to its websites and continuing operations?**

Further Reading materials

- https://www.livemint.com/industry/energy/how-cyber-attacks-are-increasing-in-india-s-power-sector-1568107532851.html
- https://security.uci.edu/security-plan/plan-controls.html
- https://security.uci.edu/security-plan/plan-control4.html
- https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-sgs-ov-controls.html
- https://economictimes.indiatimes.com/tech/internet/why-cybersecurity-should-be-indias-foremost-priority/articleshow/71843562.cms?from=mdr
- https://www.thesslstore.com/blog/cyber-risk-assessment/
- https://www.ibm.com/services/business-continuity/plan
- **The enhanced security control model for critical infrastructures with the blocking prioritization process to cyber threats in power system**
- **CYBER SECURITY IN POWER SYSTEM**

Answer the followings based on your understanding and insightfulness

Security isn’t simply a technology issue, it’s a business issue. Discuss.

If you were developing a business continuity plan for your company, where would you start? What aspects of the business would the plan address?

Suppose your business had an e-commerce Web site where it sold goods and accepted credit card payments. Discuss the major security threats to this Web site and their potential impact. What can be done to minimize these threats?

Thank you