Security Policy

Unit: 5

Cyber Security

ANC0301

(B Tech III[rd] Sem)

Sujeet Singh Bhadouria
Assistant Professor
(CSE)
NIET, Gr. Noida

Faculty Profile

FACULTY PROFILE
Name of Faculty: Sujeet Singh Bhadouria

Designation & Department: Assistant Professor, CSE

Qualification: Ph.D (Pre-Submission) M.Tech

Experience: 10 Years of teaching experience

Area of Interest: Computer Network

Reviewer: IET Communications ISSN 1751-8644 (SCI & SCOPUS INDEX)
Research Publications:
International Journal 09
Paper Presentation 06
International Patent 01 (Granted)
National Patent 04

Evaluation Scheme

Sl. No.	Subject Codes	Subject Name	Periods			Evaluation Scheme				End Semester		Total	Credit
			L	T	P	CT	TA	TOTAL	PS	TE	PE		
WEEKS COMPULSORY INDUCTION PROGRAM													
1	AAS0301A	Engineering Mathematics-III	3	1	0	30	20	50		100		150	4
2	ACSE0306	Discrete Structures	3	0	0	30	20	50		100		150	3
3	ACSE0304	Digital Logic & Circuit Design	3	0	0	30	20	50		100		150	3
4	ACSE0301	Data Structures	3	1	0	30	20	50		100		150	4
5	ACSE0302	Object Oriented Techniques using Java	3	0	0	30	20	50		100		150	3
6	ACSE0305	Computer Organization & Architecture	3	0	0	30	20	50		100		150	3
7	ACSE0354	Digital Logic & Circuit Design Lab	0	0	2				25		25	50	1
8	ACSE0351	Data Structures Lab	0	0	2				25		25	50	1
9	ACSE0352	Object Oriented Techniques using Java Lab	0	0	2				25		25	50	1
10	ACSE0359	Internship Assessment-I	0	0	2				50			50	1
11	ANC0301/ ANC0302	Cyber Security*/ Environmental Science*(Non Credit)	2	0	0	30	20	50		50		100	0
12		MOOCs** (For B.Tech. Hons. Degree)											
		GRAND TOTAL										**1100**	**24**

Syllabus

Introduction:

Introduction to Information Systems: Types of Information Systems, Development of Information Systems, Need for Information Security, Threats to Information Systems, Information Assurance, Guidelines for Secure Password and WI-FI Security and social media and Windows Security, Security Risk Analysis and Risk Management.

Application Layer Security:

Data Security Considerations-Backups, Archival Storage and Disposal of Data, Security Technology-Firewall, Intrusion Detection, Access Control, Security Threats -Viruses, Worms, Trojan Horse, Bombs, Trapdoors, Spoofs, E-mail Viruses, Macro Viruses, Malicious Software, Network and Denial of Services Attack, Security, Threats to E-Commerce: Electronic Payment System, e- Cash, Issues with Credit/Debit Cards.

Syllabus

Secure System Development:

Application Development Security, Architecture & Design, Security Issues in Hardware: Data Storage and Downloadable Devices, Mobile Protection, Security Threats involving in social media, Physical Security of IT Assets, Access Control, CCTV and Intrusion Detection Systems, Backup Security Measures.

Cryptography and Network Security:

- Public key cryptography: RSA Public Key Crypto with implementation in Python, Digital Signature Hash Functions, Public Key Distribution.
- Symmetric key cryptography: DES (Data Encryption Standard), AES (Advanced Encryption Standard), Secure hash algorithm (SHA-1).
- Real World Protocols: Basic Terminologies, VPN, Email Security Certificates, Transport Layer Security, TLS, IP security, DNS Security.

Syllabus

Security Policy:

- Policy design Task, WWW Policies, Email based Policies, Policy Revaluation Process-Corporate Policies-Sample Security Policies, Publishing and Notification Requirement of the updated and new Policies.
- Recent trends in security.

Applications

There are many cyber security real-life examples where financial organizations like banks and social organizations, weather channels etc. have faced cyber-attacks and have lost valuable information and resources. To fix these problems, you'll need comprehensive cyber security awareness.

According to KPMG, the annual compensation for cyber security heads ranges from 2 Cr to 4 Cr annually. The industry also reports a satisfaction level of 68%, making it a mentally and financially satisfying career for most.

Course Objective

Students will learn about :

- Security of Information system and Risk factors.
- Examine security threats and vulnerability in various scenarios.
- Understand concept of cryptography and encryption technique to protect the data from cyber-attack
- Provide protection for software and hardware.

Course Outcome

- After successful completion of this course student will be able to -

COURSE OUTCOME NO.	COURSE OUTCOMES	Bloom's Knowledge Level (KL)
CO1	Analyze the cyber security needs of an organization.	K4
CO2	Identify and examine software vulnerabilities and security solutions.	K1, K3
CO3	Comprehend IT Assets security (hardware and Software) and performance indicators.	K2
CO4	Measure the performance and encoding strategies of security systems.	K3, K5
CO5	Understand and apply cyber security methods and policies to enhance current scenario security.	K2, K3

Program Outcomes

1. Engineering knowledge
2. Problem analysis
3. Design/development of solutions
4. Conduct investigations of complex problems
5. Modern tool usage
6. The engineer and society
7. Environment and sustainability

Program Outcomes…(cont.)

8. Ethics
9. Individual and team work
10. Communication
11. Project management and finance
12. Life-long learning

CO-PO Mapping

CO-PO Mapping

PO No. → CO No. ↓	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	2	1	2	-	-	-	1	2	1	2	2
CO2	2	2	2	2	2	1	-	1	2	1	2	2
CO3	2	2	1	2	2	-	-	1	2	1	2	2
CO4	2	2	1	2	2	1	-	1	2	1	2	2
CO5	2	2	1	2	2	-	-	1	2	1	2	2

*3= High *2= Medium *1=Low

Program Specific Outcomes

Program Specific Outcomes (PSOs) are what the students should be able to do at the time of graduation. The PSOs are program specific. PSOs are written by the department offering the program.

On successful completion of B. Tech. (CSE) Program, the Information and Technology engineering graduates will be able to:

PSO1 : Work as a software developer, database administrator, tester or networking engineer for providing solutions to the real world and industrial problems.

PSO2 : Apply core subjects of information technology related to data structure and algorithm, software engineering, web technology, operating system, database and networking to solve complex IT problems

PSO3 : Practice multi-disciplinary and modern computing techniques by lifelong learning to establish innovative career

PSO4 : Work in a team or individual to manage projects with ethical concern to be a successful employee
or employer in IT industry.

PSO Mapping

Program Specific Outcomes and Course Outcomes Mapping

CO	PSO1	PSO2	PSO3	PSO4
CO1	2	2	-	2
CO2	2	2	1	2
CO3	2	2	-	2
CO4	2	2	-	2
CO5	2	2	-	2

*3= High *2= Medium *1=Low

Program Educational Objectives

- The Program Educational Objectives (PEOs) of an engineering degree program are the statements that describe the expected achievements of graduates in their career, and what the graduates are expected to perform and achieve during the first few years after graduation.

PEO1: To have an excellent scientific and engineering breadth so as to comprehend, analyze, design and solve real-life problems using state-of-the-art technology.

PEO2: To lead a successful career in industries or to pursue higher studies or to understand entrepreneurial endeavors.

PEO3: To effectively bridge the gap between industry and academics through effective communication skill, professional attitude and a desire to learn.

Result Analysis

Faculty Name	Subject Name	Code	Result
Ms Ruchika Sharma	Cyber Security	ANC0301	100%

Question Paper Template

(SEM:.....SESSIONAL EXAMINATION –I)(2021-2022)

Subject Name: .....

Time: 1.15Hours **Max. Marks:30**

General Instructions:

- All questions are compulsory. Answers should be brief and to the point.
- This Question paper consists of .....pages & ...5.....questions.
- It comprises of three Sections, A, B, and C. You are to attempt all the sections.
- Section A -Question No- 1 is objective type questions carrying 1 mark each, Question No- 2 is very short answer type carrying 2 mark each. You are expected to answer them as directed.
- Section B - Question No-3 is Short answer type questions carrying 5 marks each. You need to attempt any two out of three questions given.
- Section C -Question No. 4 &5are Long answer type (within unit choice) questions carrying 6marks each. You need to attempt any one part a. or b.
- Students are instructed to cross the blank sheets before handing over the answer sheet to the invigilator.
- No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.

		SECTION – A	[8]	
1.	**Attempt all parts**		**(4×1=4)**	**CO**
	a.		**(1)**	
	b.		**(1)**	
	c.		**(1)**	
	d.		**(1)**	
2.	**Attempt all parts**		**(2×2=4)**	**CO**
	a.		**(2)**	
	b.		**(2)**	

Question Paper Template

		SECTION – B		
3.	**Answer any two of the following-**		**[2×5=10]**	**CO**
	a.		**(5)**	
	b.		**(5)**	
	c.		**(5)**	
		SECTION – C		
4	**Answer any one of the following-(Any one can be applicative if applicable)**		**[2×6=12]**	**CO**
	a.	**Question-**	**(6)**	
	b.	**Question-**	**(6)**	
5.	**Answer any one of the following-**			
	a.		**(6)**	
	b.		**(6)**	

Question Paper Template

		SECTION – A		CO
1.	Attempt all parts-		[10×1=10]	
	1-a.	Question-	-1	
	1-b.	Question-	-1	
	1-c.	Question-	-1	
	1-d.	Question-	-1	
	1-e.	Question-	-1	
	1-f.	Question-	-1	
	1-g.	Question-	-1	
	1-h.	Question-	-1	
	1-i.	Question-	-1	
	1-j.	Question-	-1	
2	Attempt all parts-		[5×2=10]	CO
	2-a.	Question-	-2	
	2-b.	Question-	-2	
	2-c.	Question-	-2	
	2-d.	Question-	-2	
	2-e.	Question-	-2	

Question Paper Template

SECTION – B				CO
3	Answer any five of the following-		[5×6=30]	
	3-a.	Question-	-6	
	3-b.	Question-	-6	
	3-c.	Question-	-6	
	3-d.	Question-	-6	
	3-e.	Question-	-6	
	3-f.	Question-	-6	
	3-g.	Question-	-6	

Question Paper Template

SECTION – C				CO
4	Answer any one of the following-		[5×10=50]	
	4-a.	Question-	-10	
	4-b.	Question-	-10	
5	Answer any one of the following-			
	5-a.	Question-	-10	
	5-b.	Question-	-10	
6	Answer any one of the following-			
	6-a.	Question-	-10	
	6-b.	Question-	-10	
7	Answer any one of the following-			
	7-a.	Question-	-10	
	7-b.	Question-	-10	
8	Answer any one of the following-			
	8-a.	Question-	-10	
	8-b.	Question-	-10	

Prerequisite/Recap

- Basics recognition in the domain of Computer Science.
- Concept of network and operating system.
- Commands of programming language.

Introduction

- Modern life depends on online services, so having a better understanding of cyber security threats is vital.
- The course will improve your online safety in the context of the wider world, introducing concepts like malware, trojan virus, network security, cryptography, identity theft, and risk management.

1. https://www.javatpoint.com/cyber-security-introduction
2. https://www.edureka.co/blog/what-is-cybersecurity/
3. http://natoassociation.ca/a-short-introduction-to-cyber-security/

Content (Unit-5)

- Policy design Task
- WWW Policies
- Email based Policies
- Policy Revaluation Process-Corporate Policies-Sample Security Policies
- Publishing and Notification Requirement of the updated and new Policies
- Recent trends in security.

Unit Objective/Outcome

Topic	Objective
Policy design Task, WWW Policies, Email based Policies	Develop and examine an understanding of Secure Policies for WWW Policies, Email Security
Policy Revaluation Process-Corporate Policies-Sample Security Policies	Study of Policy Review Process for Corporate and Sample Security Policies for organization
Publishing and Notification Requirement of the updated and new Policies	Study of Publishing and Notification Requirement
Recent trends in security	Examine security of mobile devices , cloud, Outsourcing, and supply chain management

Topic Mapping with CO

Topic	CO
Policy design Task, WWW Policies, Email based Policies	CO5
Policy Revaluation Process-Corporate Policies-Sample Security Policies	CO5
Publishing and Notification Requirement of the updated and new Policies	CO5
Recent trends in security	CO5

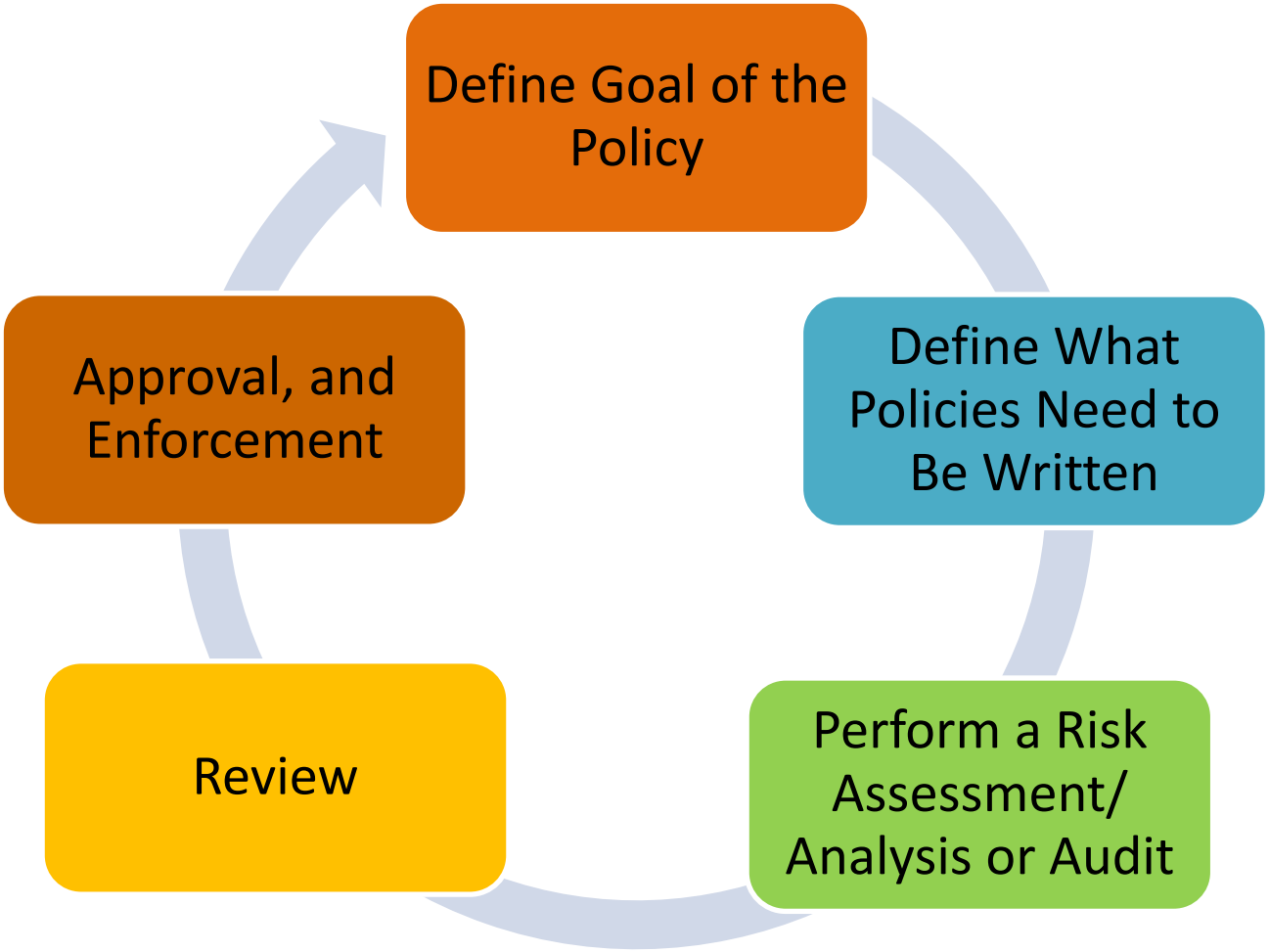
Recap

- In the previous unit we learnt about Public key cryptography and Symmetric key cryptography.
- Also gained knowledge about various Real World Protocols and Basic Terminologies like VPN, Email Security Certificates, Transport Layer Security, TLS, IP security, DNS Security.

Policy Design Task (CO5)

- An information security policy should be part of any organization's overall asset security policy.
- The security policies, standards, and procedures define a security program.
- The information security professionals of an organization are responsible to implement security policies that depict the business and mission requirements of an organization.

Development of Policy (CO5)



Development of Policy

Step-1: Define Goal of the Policy (What and Why)

- Before policy documents can be written, the overall goal of the policies must be determined.
- Example- Is the goal to protect the company and its interactions with its customers? Or will you protect the flow of data for the system?
- In any case, the first step is to determine what is being protected and why it is being protected.

Development of Policy

Step 2 : Define What Policies Need to Be Written

- Rather than trying to write one policy document, write individual documents and call them chapters of your information security policy.
- By doing so, they are easier to understand, easier to distribute, and easier to provide individual training with because each policy will have its own section.
- Smaller sections are also easier to modify and update.
- How many policies should you write?

Development of Policy

Step-3 Perform a Risk Assessment/Analysis or Audit

- The only way to understand your infrastructure is to perform a full risk assessment, risk analysis, or audit on the entire enterprise.
- By doing so, policy writers can obtain a great understanding on the reach of information technology within the organization.

Step-4: Review

- The review process should consider not only the technical aspects of security, but also the legal aspects of it as it relates to the organization.
- Prior to authoring any policies, there should be a clear understanding of the overall review process.

Development of Policy

Step- 5 : Approval, and Enforcement

- The approval process is a simple matter of the management agreeing to the final version of the document. Their approval should come after it is reviewed.

- Finally, after the policy is written, approved, and administrators implement its directive, the policy must be enforced. Policies that are not enforced will be broken at will. It is the same as laws that are not enforced in society.

When Policies Should be Developed?

- Ideally, the best time to define your policies should be before your first security problem.
- Also it is always easier to write policy for a developing infrastructure rather than trying to retrofit it into an existing business environment.
- After a Security Breach
- Demonstrate Quality Control Processes
- Document Compliance with Government

Need for Policy Development

- Identify What Is to Be Protected
- Identify From Whom It Is Being Protected
- Data Security Considerations
- Backups, Archival Storage, and Disposal of Data
- Intellectual Property Rights and Policies

Security Policies

- Organizations are required to develop and maintain specific security policies and procedures. Apart from designing a security policy, its review process is also essential to ensure that the policy is appropriate or adequate.
- Some Examples are-

  The World Wide Web (WWW) policy

  The e-mail security policy

  The corporate policy

  Sample security policy

WWW Policy(CO5)

- **Introduction to Web Security**
- Internet has facilitated most of our operations and services through web sites
- Majority of the on-line users spend their time in referring to the web sites for their everyday work
- These are vulnerable to cyber-attacks
- Cyber-attacks can be executed on web sites, web servers and web applications.

WWW Policy

- **Why Web Security?**
- The purpose of web-security is to prevent the web sites, web servers and web applications from cyber-attacks
- It is defined as the act or practice of protecting websites from
  - Unauthorized access
  - Use
  - Modification
  - Destruction or
  - Disruption
- It plays major role in preventing users against vulnerabilities

WWW Policy

Website Security issues

Website source code	•Caused due to improper development of source code • More possibilities of bugs and security loopholes
Website visitor access	•Highly vulnerable to attacks •Difficult to distinguish genuine user from illegitimate user at times of large number of visitors
Sophistication of Website security attacks	• Many new methods are found by hackers and implemented • Web security software and malware does not differentiate are methods used to handle the issues

Source: Swayam

Web Security Risks(CO5)

- SQL Injection
- Password Breach
- Data Breach
- Remote File Inclusion
- Code Injection
- Cross Site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross Site Request Forgery(CSRF)
- Security Misconfigurations
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Un-validated Redirects and Page Forwards

WWW policy to Avoid Risks

- No offensive or harassing material may be made available through company websites.
- No personal commercial advertising should be made available through company websites.
- The personal material on or accessible from the website should be minimal.
- No company confidential material should be made available
- Users of an organization should not be permitted to install or run Web servers

E-mail System(CO5)

- E-mail is the popular form of sending or exchanging information between two or many parties

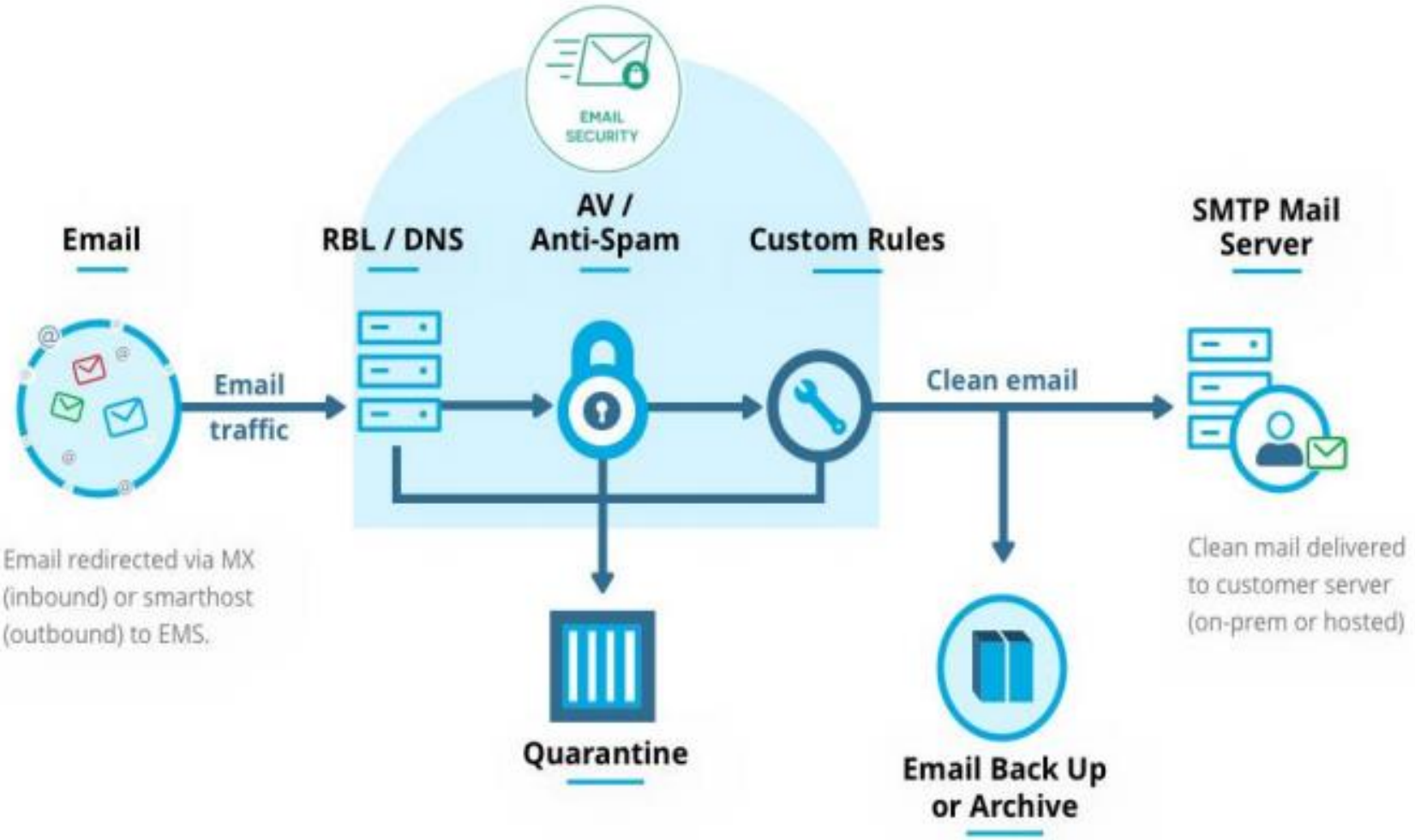
- Despite being popular, malware, spam and phishing attacks are executed

- E-mail also acts the entry point for the enterprise network to gain access to their valuable data

E-mail Security

- It deals with the different techniques to secure the information sent through email
- The e-mail accounts are prevented from unauthorized access, loss, or compromise
- It is important to provide e-mail security as individuals and business organizations expand their extensive communication through email

E-mail Security



Source: Swayam

Need for E-mail Security

- Every organisation must employ e-mail administrators responsible in providing security to the e-mail system
- It is important to provide e-mail security as individuals and business organizations expand their extensive communications through e-mail
- Hence E-mail messages must be secured as they are delivered and received across un-trusted networks

Importance of E-mail Security

- It provides security over external networks security i.e., outside the organization's boundary
- It maintains the CIA of information transferred through e-mail
- It provides implementation of good management system planning by continuous monitoring
- It also maintains the effectiveness of the e-mail system and IT infrastructure

Common Threats to e-mail security

Source: swayam

E-mail Security Policy(CO5)

An organization can include the following "Ten Commandments of E-mail" while developing an e-mail policy:

1. You will [may be replaced may be complicated by readers] demonstrate the same respect that gives to verbal communications.

2. You will check the spelling, the grammar, and read own message thrice before you send it.

3. You will not forward any chain letter.

E-mail Security Policy

4. You will not transmit unsolicited mass e-mail (spam) to anyone.

5. You will not send messages that are hateful, harassing, or threatening unto fellow users.

6. You will not send any message that supports illegal or unethical activities.

7. You will remember that e-mail is the electronic equivalent of a post card and will not be used to transmit sensitive information.

E-mail Security Policy

8. You will not use email broadcasting facilities except for making appropriate announcements.

9. You will keep personal email use to a minimum.

9. You will keep policies and procedures secrete and help administrators protect them from abusers.

Policy Revaluation Process (CO5)

Policy Revaluation Process-Corporate Policies-Sample Security Policies

Corporate Policies (CO5)

Corporate Policies

- Corporate Policy is the formal declaration of the principles and polices according to which a company will operate .These policies and principles are prepared by board of directors of the company or senior management committee .

- Corporate policy comprises:

➢ Company's mission statement

➢ Company's objectives

➢ Principles on the basis of which strategic decisions are made

Sample Security Policy(CO5)

Let's now look at the sample security policy. The template of the sample security policy is as follows:

1. Information security policy
    a) Purpose
    b) Aims and commitments
    c) Responsibilities
    d) Councils
    e) Heads of departments
    f) Users and external parties

Sample Security Policy

2. Risk assessment and the classification of information
    a) Risk assessment of information held
    b) Personal data
3. Protection of information systems and assets
4. Protection of confidential information
    a) Storage
    b) Access
    c) Copying
    d) Disposal
    e) Use of portable devices or media

Sample Security Policy

4. Protection of confidential information
    f) Cryptographic controls
    g) Exchange of information and use of e-mail
    h) Backup
    i) Hard copies

5. Risk identification and analysis
    a) Assets
    b) Threats and risks

Recap

- WWW Policy
- E-mail System
- Corporate policies
- Sample security policy

Policy Revaluation/Review Process(CO5)

6 important steps to be performed while evaluating information security policy:

- Having someone other than the person who wrote the policy review it
- Assessing policy for completeness
- Ensuring that policy statement is clear, concise, and SMART
- Ensuring that policy answers the 5 Ws
- Ensuring consistency with laws, regulations, and other levels of policy
- Checking policy freshness and easy availability to organization members

Policy Review Process

Step-1: Having someone other than the person who wrote the policy review it:

- Someone other than the person who created the policy should review and assess for mistakes.
- The policy reviewer should be aware about the organization fundamentals of information security and detail oriented for best results.
- Moreover, the person should be technically sound to review the policy for technical accuracy.

Policy Review Process

Step-2: Assessing policy for completeness:

- Assessing policy framework for completeness:

  Checks or examines the existence of standards and procedures supporting the policy set.

- Assessing policy elements for completeness:

  Checks or examines if the policy is not flawed due the lack of an element.

Policy Review Process

Step-3: Ensuring that policy statement is clear, concise, and SMART:

- SMART stands for specific, measurable, achievable, realistic, and time bound.
- In this step, the policy reviewer ensures that the policy is clear, and simple language is used to ensure that it can be easily understood by everyone.

Step-4: Ensuring that policy answers the 5 Ws:

- In this step, the reviewer checks whether the appropriate function is defined for the correct person in place.
- The reviewer also ensures when the actions will be accomplished. In other words, the policy should clearly explain the purpose, background, or policy statement.

Policy Review Process

Step-5: Ensuring consistency with laws, regulations, and other levels of policy:

- In this step, the reviewer ensures that the policy is consistent with various laws and regulations; otherwise, the organization will face lawsuits.
- Also, the policy should ensure consistency with the laws and regulations of each country.
- During policy assessment, the policies are checked for consistency with lower and higher levels. Any discrepancy found should be resolved.

Policy Review Process

Step-6: Checking policy freshness and easy availability to organization members:

- In this step, a policy is examined for provisions to keep it updated.
- This is important because an outdated policy can result into damage than good.

Publishing and Notification requirement of the Policies(CO5)

- After the policies have been written, they will not do your organization any good if they sit on the shelf collecting dust. Not only should it be a living document, but it also should be accessible to all users.

- A common way of doing this is to publish the policies on the organization's intranet.

- Policies in this area should cover both the publishing of the policy documents and notification of when published.

Publishing and Notification requirement of the Policies

- This policy also should cover who is responsible for these acts. (Human Resources Department)

- Notify each department and user by providing Printed Copy or Electronic version of the published policy.

Recap

- Corporate Policy
- Sample Security Policy
- Policy Review Process
- Publishing and Notification requirement of the Policies

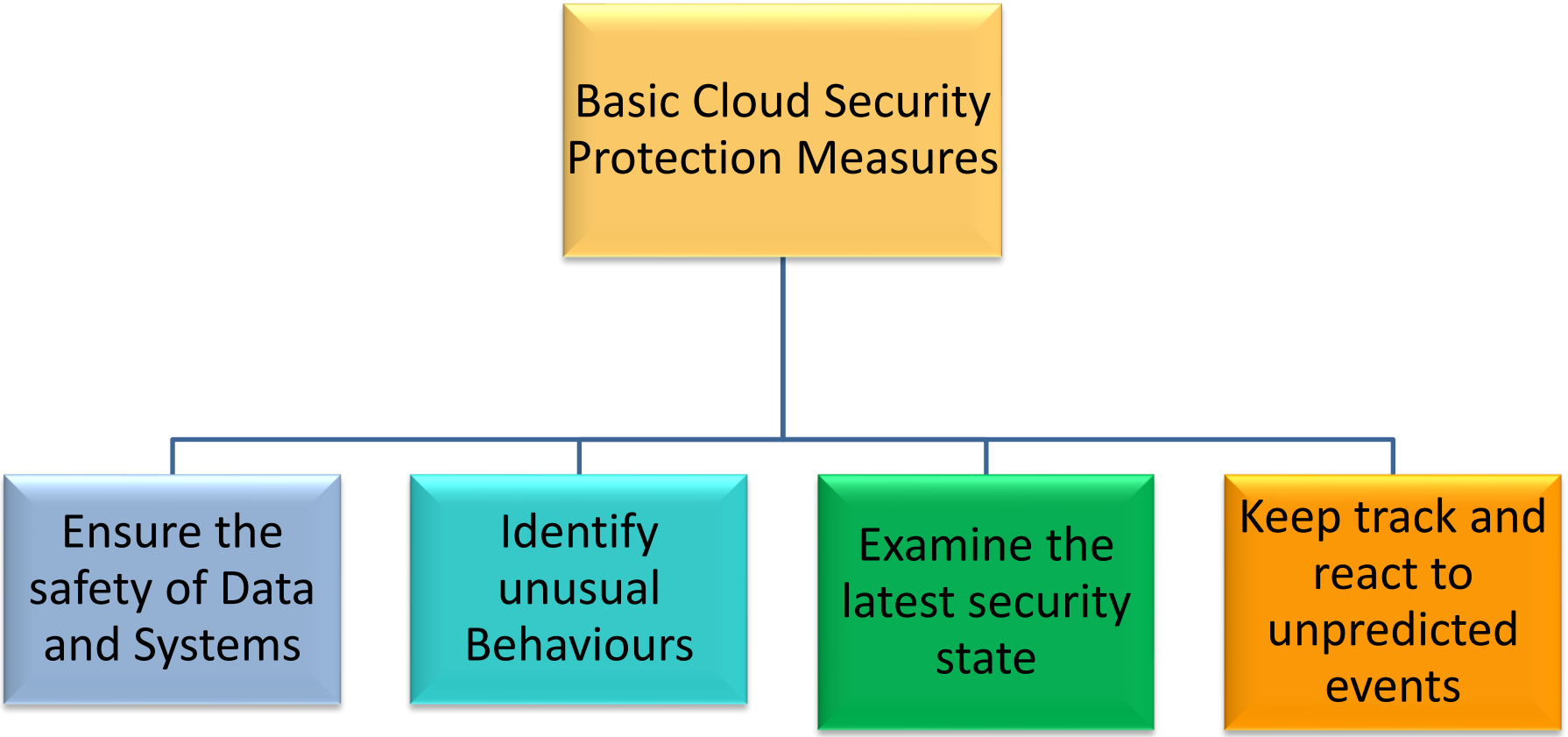
Recent trends in security (CO5)

- Cloud security
- Outsourcing
- SCM

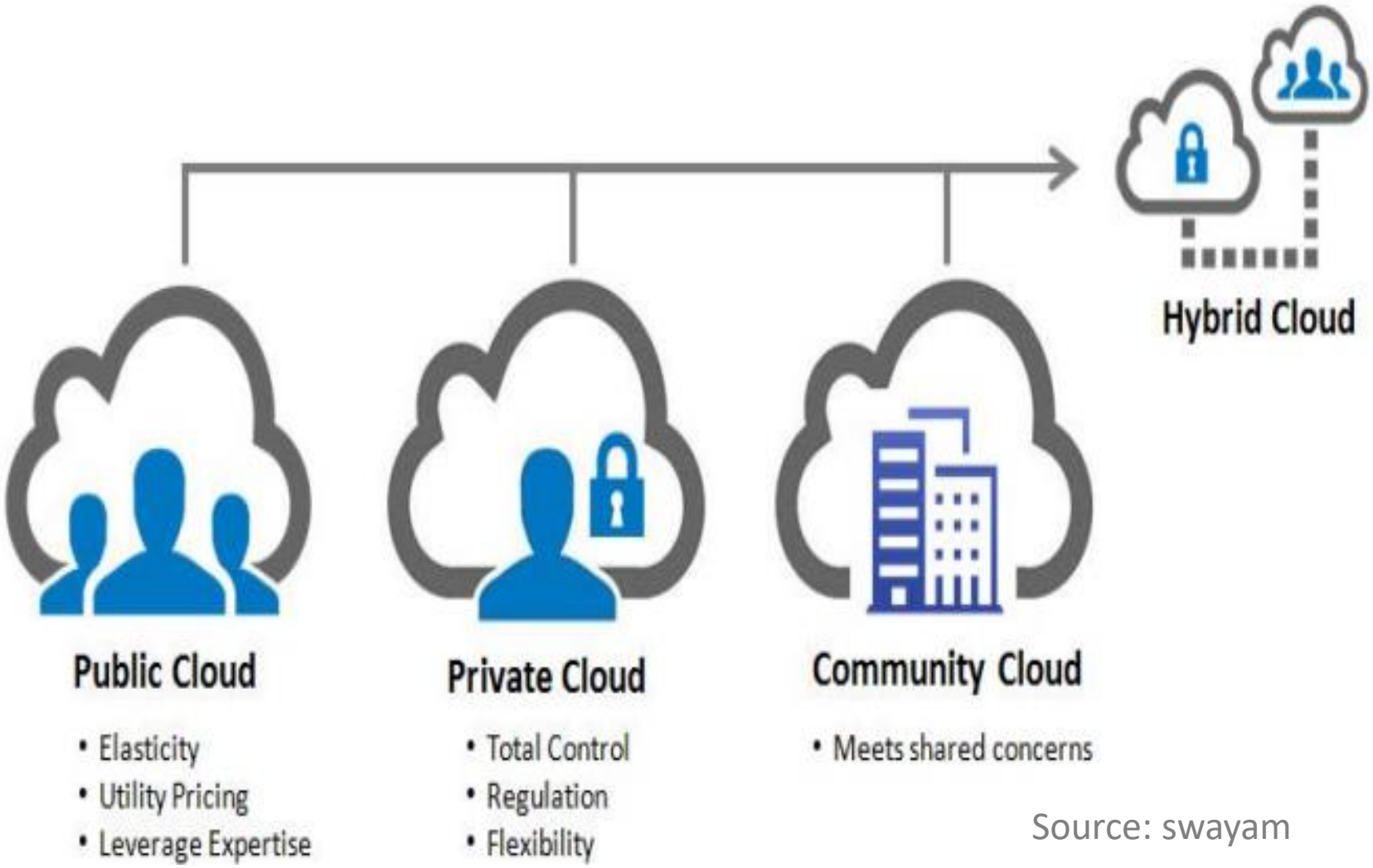
Cloud Security (CO5)

- Cloud computing is one of the promised leading computing technologies
- The emergence of cloud users has increased in IT sectors
- The security in cloud refers to the process of securing data and information present in the cloud
- Cloud computing security processes should address the security controls
- The cloud provider incorporates to maintain the customer's data security, privacy and compliance with necessary regulations

Basic Cloud Security Protection Measures

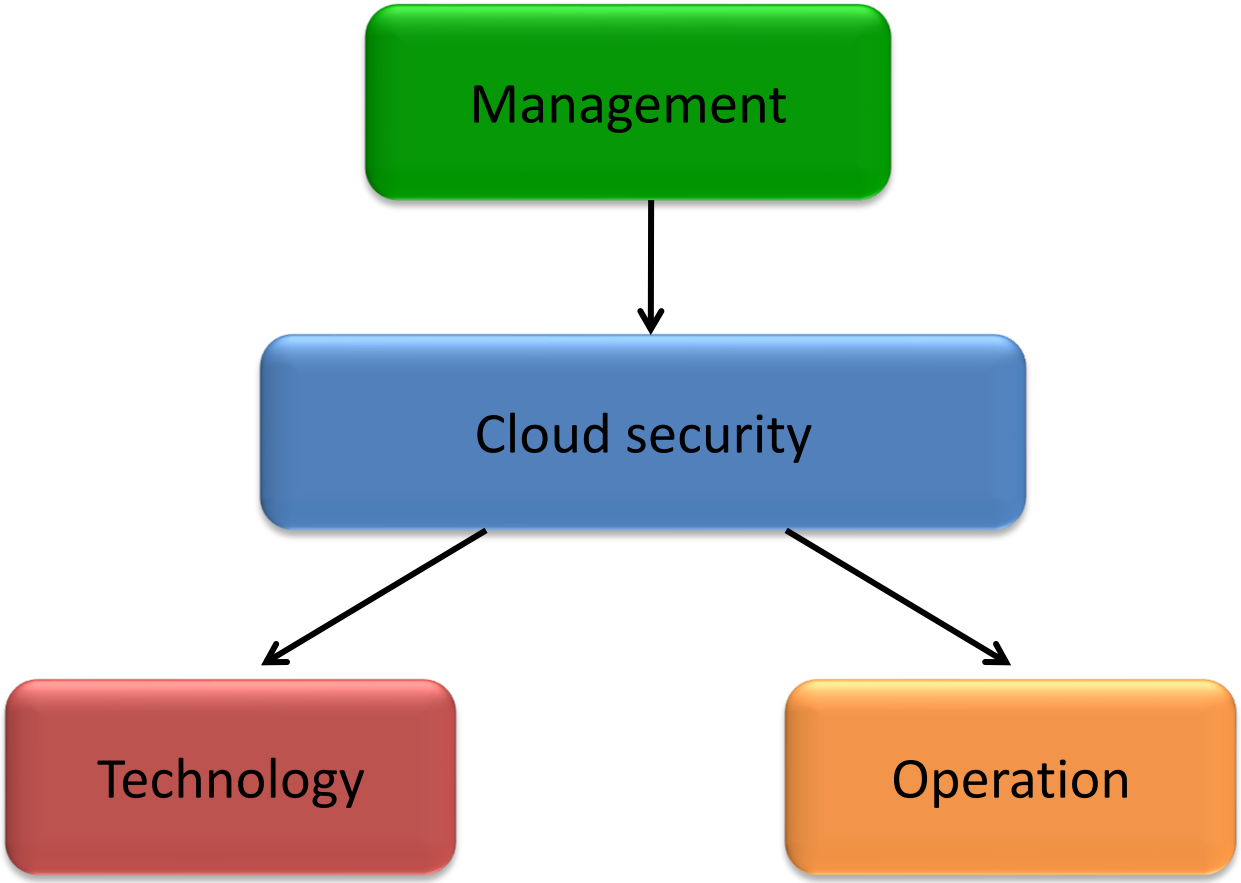


Cloud Deployment Models



Source: swayam

The Key Aspects of Cloud Security



Key Aspects of Cloud Security Management

- Alteration of security policies
- Cloud security strategy
- Cloud security governance
- Cloud security processes
- Security roles & responsibilities
- Cloud security guidelines
- Cloud security assessment
- Service integration
- IT & procurement security requirements
- Cloud security management

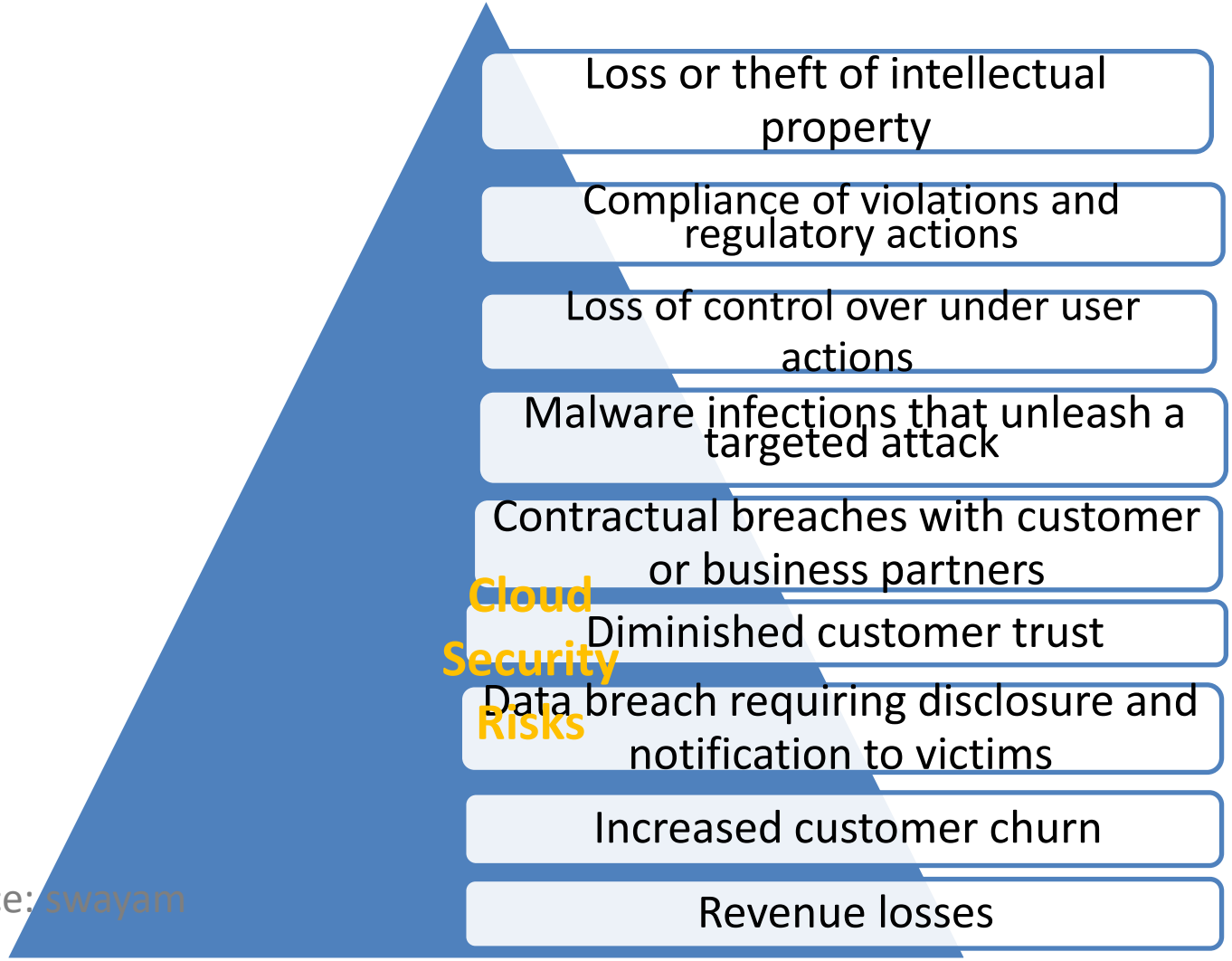
Key Aspects of Cloud Security Operation

- Awareness and training programs on cloud security
- Incident management
- Configuration management
- Contingency planning
- Maintenance
- Media protection
- Environmental protection
- System integrity
- Information integrity
- Personnel security

Key Aspects of Cloud Security Technology

- Access control Technology and software configuration
- System Protection Technology
- Authentication Technology
- Cloud security audits
- Identity and key management
- Physical security protection
- Backup recovery and archive
- Core infrastructure

Risks in Cloud Security



Source: swayam

Tools used in Cloud security

- OpenStack is an open source software used for creating private and public clouds
- Users can create virtual machines and other instances that do different things in the cloud environment
- It allows users to quickly create new VM or instance upon which other cloud components can run providing infrastructure
- This puts OpenStack in the Cloud Infrastructure as a Service category

Outsourcing (CO5)

- Software Outsourcing is the process of selecting a 3rd party service provider of software development services that will manage all the tasks involved in a development project.
- Companies can easily reduce costs with the help of outsourcing software development services.
- It's very difficult for IT firms to stay updated in an environment where new software is rising on a daily basis.

Why Outsource?

- Speed up and scale a development team.
- Streamlining or increasing efficiency for time-consuming functions
- Maximizing use of external resources
- Sharing risks with a partner company
- Reducing and controlling operating costs
- Pros of Software Outsourcing
- Flexibility
- Increase skills and scale a development team
- Enhanced Business Productivity and Cut on Costs
- Focusing On a Project and Core Business Value
- Risk sharing
- Better efficiency
- Overwhelming results
- Time-saving

Outsourcing Risks

Supply Chain Management(SCM)(CO5)

- Cyber security in the supply chain cannot be viewed as an IT problem only.
- Cyber supply chain risks touch sourcing, vendor management, supply chain continuity and quality, transportation security and many other functions across the enterprise and require a coordinated effort to address.
- Develop your defences based on the principle that your systems will be breached
- Cyber security is never just a technology problem, it's a people, processes and knowledge problem
- Security is Security.

SCM Risks

- Third party service providers or vendors – from janitorial services to software engineering -- with physical or virtual access to information systems, software code, or IP.
- Poor information security practices by lower-tier suppliers.
- Compromised software or hardware purchased from suppliers.
- Software security vulnerabilities in supply chain management or supplier systems.
- Counterfeit hardware or hardware with embedded malware.
- Third party data storage or data aggregators.

SCM Best Practices

- Security requirements are included in every RFP and contract.
- Once a vendor is accepted in the formal supply chain, a security team works with them on-site to address any vulnerabilities and security gaps.
- "One strike and you're out" policies with respect to vendor products that are either counterfeit or do not match specification.
- Component purchases are tightly controlled; component purchases from approved vendors are prequalified. Parts purchased from other vendors are unpacked, inspected, and x-rayed before being accepted.

SCM Best Practices

- Secure Software Lifecycle Development Programs and training for all engineers in the life cycle are established.
- Source code is obtained for all purchased software.
- Software and hardware have a security handshake. Secure booting processes look for authentication codes and the system will not boot if codes are not recognized.
- Automation of manufacturing and testing regimes reduces the risk of human intervention.

Daily Quiz

- What are the Threats to e-mail security?
- What are the Threats to Mobile Device Security?
- What are the key aspects to cloud Security?
- What is OpenStack ?
- What is Spam mail?

Weekly Assignment

1. What do you mean by policy? why it is developed and reviewed?
2. Explain is email system andEmail Policy.
3. Describe WWW policy.
4. Briefly explain the role of security in Internet and Web services.
5. Describe corporate policy
6. Discuss security issues in Supply Chain Management(SCM)
7. Classify the risk in cloud security.
8. Describe Common risks in Mobile Devices.
9. Explain steps in Policy Review Process
10. What are the common threats to mobile devices

Faculty Video Links, Youtube & NPTEL Video Links and Online Courses Details

- https://youtu.be/tZJoMjEsf4E
- https://youtu.be/09NW4WeBLrw
- https://www.youtube.com/watch?v=L-cC-JjYos0
- https://www.youtube.com/watch?v=QxEpued61OI
- https://www.youtube.com/watch?v=ahNb6kA0Lms
- https://www.youtube.com/watch?v=ZnxnTLPcdDk
- https://www.youtube.com/watch?v=Og9lf0StwVA

Faculty Video Links, Youtube & NPTEL Video Links and Online Courses Details

- https://www.youtube.com/watch?v=E47ew_IsqaM
- https://www.youtube.com/watch?v=gDtlbGK13xM
- https://www.youtube.com/watch?v=xFzaoJjzXJQ
- https://youtu.be/RQOJgEA5e1k
- https://youtu.be/GKqOWCK71K4
- https://youtu.be/zDDkNq6kpRE

Glossary Questions

Fill the right options:

Community, Confidentiality of Information, mass email, Define Goal of the Policy

1. Risk associated with outsourcing _____
2. One type of cloud deployment model____
3. On commandment of email security policy: You will not transmit _____unsolicited to anyone.
4. Step one of policy development _____

Recap of Unit

- Policy design Task
- WWW Policies
- Email based Policies
- Policy Revaluation Process-Corporate Policies-Sample Security Policies
- Publishing and Notification Requirement of the updated and new Policies
- Recent trends in security

Daily Quiz

1. Figure out the vulnerability that targets scripts embedded in a page executed on the client side.
   a) Web application firewall
   b) Cross Site Scripting
   c) Network
   d) Objects

2. Label the process of setting up of fake access points in high traffic public locations.
   a) Unsecured Wi-Fi
   b) Phishing Attacks
   c) Network Spoofing
   d) Spyware

3. 3. Recognize the cheapest form of Authentication.
   a) Password based Authentication
   b) Encryption
   c) Biometric based Authentication
   d) Smart cards

Daily Quiz

4. Which of the following implies the influence of the attack when security is compromised in a System?
   a) Exploitability
   b) Detectability
   c) Impact
   d) None of the above
5. What causes the loss of CIA triad in mobile devices?
   a) Multiple user logs
   b) Mobile browsing
   c) Bluetooth attacks
   d) Coding issues
6. Choose the model used in implementing and managing security in Cloud.
   a) Information-as-a-Service (IaaS)
   b) Security-as-a-Service (SaaS)
   c) Platform-as-a-Service (PaaS)
   d) Human-as-a-Services(HuaaS)

Daily Quiz

7. Determine the older form of Social Engineering.
   a) Pre-texting
   b) Phishing
   c) Baiting
   d) All the above
8. Point out the technology used for purchasing products securely through mobile devices with an embedded chip.
   a) Bluetooth
   b) Virtual Private Network
   c) Neat Field Chip
   d) Neat Field Communication
9. Select the common security concerns that affect cloud systems
   a) Unauthorized exposure
   b) Cloud type
   c) Data leakage
   d) Service type
10. 11. Establish the primary components of e-mail system.
    a) Network
    b) Mail Clients
    c) Mail Servers
    d) Protocols

Weekly Assignment

1. Collect the various web security risks and the strategies to solve them.
2. Examine and analyze the common threats encountered in email security.
3. Describe the components of mobile device security.
4. Demonstrate the key aspects in maintaining cloud security.
5. What is cloud architecture? How is cloud different from traditional data centers?
6. How can you deploy cloud computing with different models?

MCQ s

1. Analyze the common places where user interactions take place in WebPages.
   a) Form/search field
   b) Code area
   c) Blogs
   d) Empty area

2. Which of the following is the operational domain of CSA?
   a) Scalability
   b) Portability and interoperability
   c) Flexibility
   d) None of the mentioned

MCQ s

- 3. Which of the following ensure interoperability between different mail clients and servers?
  a) Simple Mail Transfer Protocol
  b) Extended Simple Mail Transfer Protocol
  c) Extended Simple Mail Transfer Protocol
  d) Internet Message Protocol

MCQ s

- Which of the following policy helps in avoiding the risk of browsing the Internet accessing sites containing offensive material?

  a) WWW policy b) Email Policy

  c) Corporate policy d) All

- Determine the older form of Social Engineering.

  a) Pre-texting b) Phishing

  c) Baiting d) All

- Which of them is not a major way of stealing email information?

  a) Stealing cookies b) **Reverse Engineering**

  c) Password Phishing c) Social Engineering

MCQ s

- Which of them is not a proper method for email security?
  a) Use Strong password
  b) Use email Encryption
  c) Spam filters and malware scanners
  d) Click on unknown links to explore
- Unsolicited Bulk E-mails (UBI) are called _____
  a) SMS
  b) MMS
  c) Spam emails
  d) Malicious emails
- Lack of access control policy is a _____
  a) Bug
  b) Threat
  c) Vulnerability
  d) Attack

MCQ s

- Data leakage threats do not usually occur from which of the following?
  a) Web and email
  b) Mobile data storage
  c) USB drives and laptops
  d) Television
- Spywares can be used to steal _____ from the attacker's browser.
  a) browsing history b) company details
  c) plug-ins used d) browser details
- Which of the following is not a spot from where attackers seek information?
  a) Domain name b) IP address
  c) System enumeration **d) Document files**

Past Sessional Papers

Printed page: 2 Subject Code:ANC0301

Roll No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute)

Affiliated to Dr. A.P. J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow

Course : B.Tech Branch : CSE.

Semester : III Sessional Examination : Second Year- (2021 - 2022)

Subject Name: Cyber Security

Time: 1.15Hours [SET- A] Max. Marks:30

General Instructions:

- This Question paper consists of .....pages & .....questions.It comprises of three Sections, A, B, and C
- **Section A** -Question No- 1 is objective type questions carrying 1 mark each, Question No- 2 is very short answer type carrying 2 mark each. You are expected to answer them as directed.
- **Section B** - Question No-3 is Short answer type questions carrying 5 marks each. Attempt any two out of three questions given.
- **Section C** -Question No. 4 &5are Long answer type (within unit choice) questions carrying 6marks each. Attempt any one part a or b.

		SECTION – A	[08Marks]	
1.	All questions are compulsory		(4×1=4)	
	a.	1. How many layers are there in OSI model? a. 4 b. 7 c. 3 d. 8	(1)	CO2
	b.	2. Data security considerations are? a. Backups b. Archival storage c. Disposal of data d. All	(1)	CO2
	c.	3. Full form of IDS? a. Invention detection system b. Illusion detection system c. Intrusion detection system d. None	(1)	CO2
	d.	4. Full form of VIRUS? a. Various Information Resource Under Support b. Very Information Resource Under Support c. Vital Information Resource Under Seize d. none	(1)	CO2

Past Sessional Papers

2.	All questions are compulsory		[2×2=4]	
	a.	Differentiate virus and worms?	(2)	CO2
	b.	Define zero day attack?	(2)	CO2
		SECTION – B	[10Marks]	
3.	Answer any two of the following-		[2×5=10]	
	a.	What is a firewall? Mention all types of Firewalls.	(5)	CO2
	b.	What is spoofing ? What are its different types?	(5)	CO2
	c.	What is e-commerce. Name some e -commerce site. How is payment done while the transaction of goods here?	(5)	CO2
		SECTION – C	[12Marks]	
4	Answer any one of the following-		[1×6=6]	
	a.	What is a Trojan horse in Network security and how it got its name?	(6)	CO2
	b.	Explain intrusion detection system?	(6)	CO2
5.	Answer any one of the following-		[1×6=6]	
	a.	Differentiate between Debit card and Credit card?	(6)	CO2
	b.	Explain the advantages and disadvantages of E-cash?	(6)	CO2

Past Sessional Papers

Printed page: 2 Subject Code: ANC0301

Roll No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute)

Affiliated to Dr. A.P. J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow

Course: B.Tech Branch: CSE

Semester: 3rd Sessional Examination: 2nd Sessional Year- (2021 – 2022)

Subject Name: Cyber Security

Time: 1.15Hours [SET- B] Max. Marks: 30

General Instructions:

- This Question paper consists of .....pages & .....questions.It comprises of three Sections, A, B, and C
- Section A -Question No- 1 is objective type questions carrying 1 mark each, Question No- 2 is very short answer type carrying 2 mark each. You are expected to answer them as directed.
- Section B - Question No-3 is Short answer type questions carrying 5 marks each. Attempt any two out of three questions given.
- Section C -Question No. 4 &5are Long answer type (within unit choice) questions carrying 6marks each. Attempt any one part a or b.

		SECTION – A	[08Marks]	
1.		**All questions are compulsory**	(4×1=4)	
	a.	1. How many layers are there in OSI model? a. 4 b. 7 c. 3 d. 8	(1)	CO2
	b.	2. Data security considerations are? a. Backups b. Archival storage c. Disposal of data d. All	(1)	CO2
	c.	3. Full form of IDS? a. Invention detection system b. Illusion detection system c. Intrusion detection system d. None	(1)	CO2
	d.	4. Full form of VIRUS? a. Various Information Resource Under Support b. Very Information Resource Under Support c. Vital Information Resource Under Seize d. none	(1)	CO2

Past Sessional Papers

2.	All questions are compulsory		(2×2=4)	
	a.	Define zero day attack.	(2)	CO2
	b.	Differentiate virus , worms, Trojan horse and logic bombs?	(2)	CO2
		SECTION – B	[10Marks]	
3.	Answer any two of the following-		(2×5=10)	
	a.	What is spoofing? Explain different types of spoofing?	(5)	CO2
	b.	Explain the working of IDS System with the help of the diagram.	(5)	CO2
	c.	Explain virtual private networks in detail?	(5)	CO2
		SECTION – C	[12Marks]	
4	Answer any one of the following-		(1×6=6)	
	a.	What is the data security consideration? Explain in this reference Data backup security, Data archival security and Data disposal consideration.	(6)	CO2
	b.	Discuss Electronic Payment System and its types. Explain the threats to E Commerce.	(6)	CO2
5.	Answer any one of the following-		(1×6=6)	
	a.	What is Firewall and explain the types of Firewall?	(6)	CO2
	b.	Differentiate between Debit card and Credit card?	(6)	CO2

Old Question Papers

Printed Pages:01 | Sub Code: RUC 501

Paper Id: 199503 | Roll No.

B TECH

(SEM V) THEORY EXAMINATION 2018-19

CYBER SECURITY

Time: 3 Hours | ***Total Marks: 70***

Note: **1.** Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. **Attempt *all* questions in brief.** **2 x 7 = 14**

a. Write a short note on the Copyright Act?
b. What do you mean by physical Security for informationSystems?
c. Describe Intellectual Property Issues (IPR).
d. Write short notes on "Patent Law".
e. What do you mean by WWW policy?
f. Give small notes on Corporate Policy.
g. Differentiate between Cyber Security and Information Security.

SECTION B

2. **Attempt any *three* of the following:** **7 x 3 = 21**

a. What are the key differences between Symmetric and Asymmetric encryption?
b. Explain Information Security Governance in detail and process involved in the Risk Management?
c. Explain briefly about Application Development Security with guidelines.
d. Elaborate the term Access Control. What is include in authorization process for (File, Program, Data rights) and explain the all types of controls.
e. What do you understand by security structure (Architecture) and design?

Old Question Papers

SECTION C

3. Attempt any *one* part of the following: 7 x 1 = 7

(a) What do you mean by Intellectual Property? Describe various means using which Intellectual Property may be protected to an extent.

(b) Explain Confidentiality, Integrity and Availability in terms of cyber security.

4. Attempt any *one* part of the following: 7 x 1 = 7

(a) What are the approaches followed in developing Information System (IS)? Explain the difference between security and threats.

(b) What is the need of information Security also explain the term ISMS?

5. Attempt any *one* part of the following: 7 x 1 = 7

(a) Explain the role of Security in Internet and Web Services.

(b) What is Intrusion Detection System? Explain with Block Diagram.

6. Attempt any *one* part of the following: 7 x 1 = 7

(a) Explain in Detail about Secure Information System Development.

(b) Describe the working principle of CCTV.

7. Attempt any *one* part of the following: 7 x 1 = 7

(a) What are the Data Security Considerations? Explain in this reference Data Backup Security.

(b) What is Public Key Cryptography? Define its Advantage and Disadvantage.

Old Question Papers

Printed Pages : 1 **Roll No.** | | | | | | | | | | | **AUC002**

COMMON TO ALL BRANCHES
THEORY EXAMINATION (SEM-IV) 2016-17
CYBER SECURITY

Time : 3 Hours *Max. Marks : 100*

Note : Be precise in your answer.

SECTION – A

1. Attempt all of the following questions: **10 x 2 = 20**

(a) What is CIA (Confidentiality, Integrity and Availability) trade?
(b) What are the threats to information system?
(c) What is System Development Life Cycle (SDLC)?
(d) Define the terms RTGS and NEFT.
(e) What do you mean by virus, worm and IP spoofing?
(f) How cyber security is different from computer security?
(g) State the difference between Risk Management and Risk Assessment.
(h) Explain briefly about disposal of data.
(i) Define IT asset and the security of IT Assets.
(j) What is the need of cyber laws in India?

Old Question Papers

SECTION – B

2. **Attempt any five parts of the following question:** **5 x 10 = 50**

(a) What are biometric? How can a biometric be used for access control? Discuss the criteria for selection of biometrics.

(b) What is Intrusion Detection System (IDS)? Explain its type in detail.

(c) What are the backup security measures? Discuss its type.

(d) What are the basic fundamental principles of information security? Explain.

(e) Write a short note on CCTV and its applications.

(f) What is Electronic cash? How does cash based transaction system differ from credit card based transactions?

(g) What do you mean by Virtual Private Networks? Discuss authentication mechanism used in VPN.

(h) **Write a short note on:**

(i) Database Security **(ii)** Email Security **(iii)** Internet Security

SECTION – C

Attempt any two of the following questions: **2 x 15 = 30**

3. What is Electronic Data Interchange (EDI)? What are the benefits of EDI? How can it be helpful in governance?

4. What is digital signature? What are the requirements of a digital signature system? List the security services provided by digital signature.

5. Explain the following in detail :

(i) Private Key cryptosystem and Public key cryptosystems.

(ii) Firewall.

Expected Questions for University Exam

1. Explain the Recent Trends in security in mobile.
2. Explain the Recent Trends in security in cloud.
3. Explain the need for Information Security Policies.
4. What are the components of cyber security?
5. The most dangerous vulnerabilities in stored mobile data?
6. How to protect email messages?
7. What are the risks associated with public Wi-Fi?
8. What is a security auditing?

Summary

- Policy design Task
- WWW Policies
- Email based Policies
- Policy Revaluation Process-Corporate Policies-Sample Security Policies
- Publishing and Notification Requirement of the updated and new Policies
- Recent trends in security

References

1. Dr. Surya Prakash Tripathi, Ritendra Goyal, Praveen kumar Shukla ,"Introduction to Information Security and Cyber Law" Willey Dreamtech Press.(prefer)
2. http://caaa.in/Image/cyber%20laws%20overview.pdf
3. https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf
4. https://www.tutorialspoint.com/information_security_cyber_law/information_security_cyber_law_tutorial.pdf
5. http://lawcommissionofindia.nic.in/1-50/Report42.pdf
6. http://www.caaa.in/Image/34_Hb_on_IPR.pdf
7. http://www.esi.mil/download.aspx?id=6073
8. https://onlinecourses.swayam2.ac.in/cec20_cs09/unit?unit=244&lesson=253

Thank You