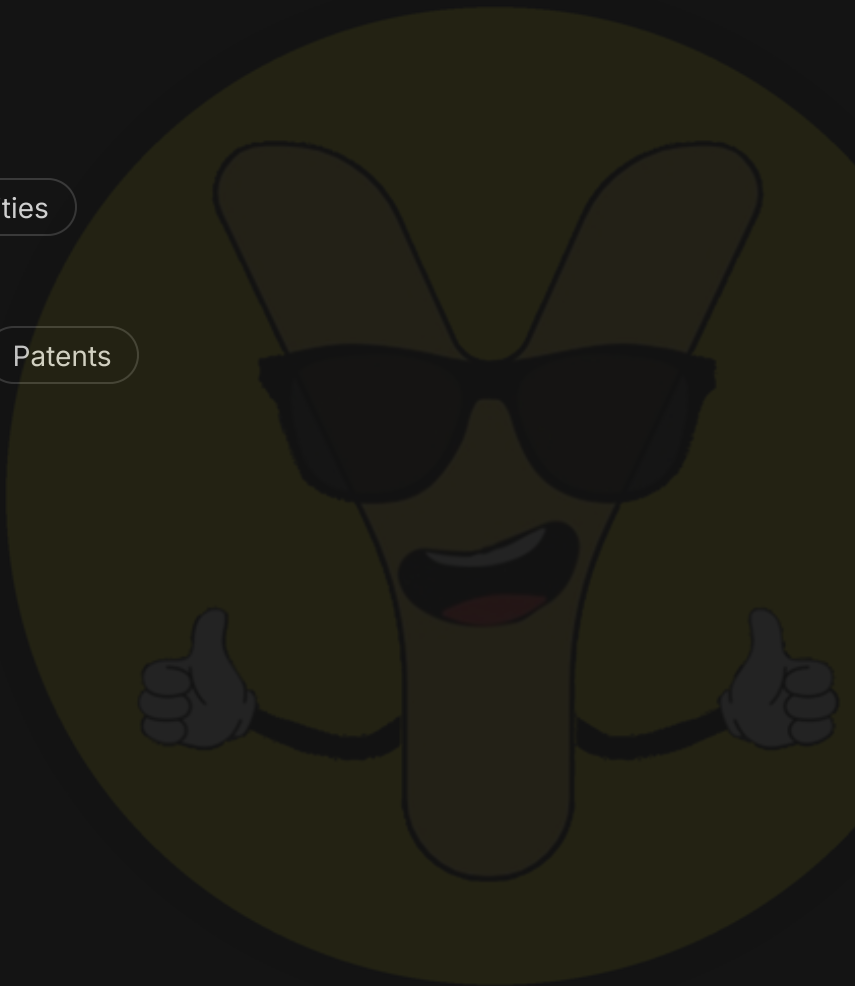
AKTU · 2ND YEAR · BCC301 / BCC401

Cyber Security

Unit 4 — Cyber Security: Organizational Implications

- Cost of Cybercrimes and IPR Issues
- Webservers
- Attacks on Webservers
- Web Application Vulnerabilities
- Cross-Site Scripting (XSS)
- Cyber Security: Organizational Implications
- Cost of Cybercrime
- Understanding Intellectual Property Rights (IPR)
- Internet Intellectual Property
- Copyright Infringement
- Patents
- Trademarks
- Data Theft



DECODED BY

Chirag Jain

Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

Unit 4 Overview: Organizational Implications

This unit covers financial impacts of cyber attacks, web infrastructure security, application vulnerabilities, and intellectual property protection.

- Cost of Cybercrimes and Intellectual Property Rights (IPR)
- Webservers and Attacks on Webservers
- Web Application Vulnerabilities and Cross-Site Scripting (XSS)
- Internet Intellectual Property: Copyright, Patents, Trademarks
- Data Theft and Organizational Risk Mitigation

Cost of Cybercrimes

CYBERCRIME FINANCIAL IMPACT

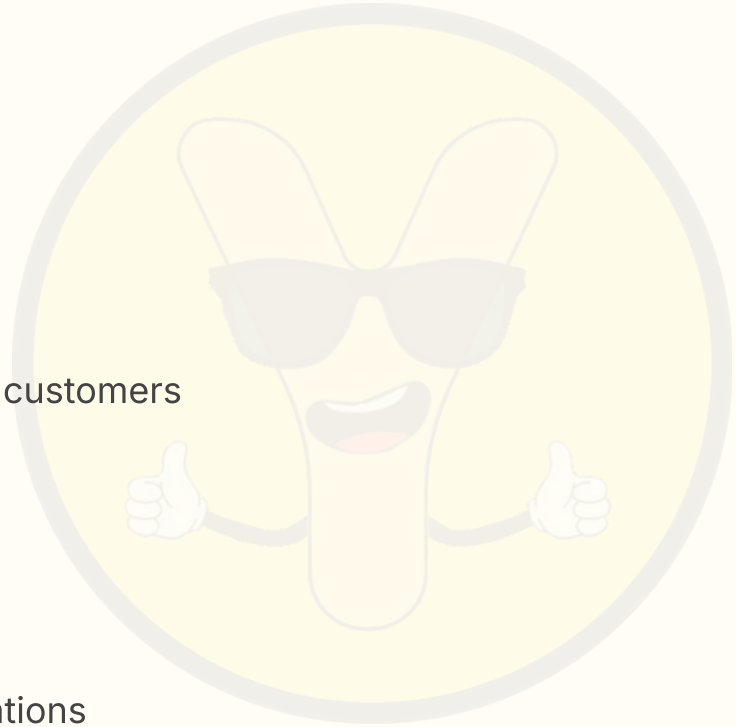
The total economic loss incurred by an organization due to malicious cyber activities, encompassing direct losses, operational disruption, and recovery expenses.

- Calculated via formula: Total Cost = Direct Costs + Indirect Costs + Recovery Costs
- Direct costs include stolen funds, ransom payments, and data extortion.
- Indirect costs involve business downtime, lost customer trust, and brand erosion.

Components of Cybercrime Costs

Understanding how financial damages accumulate during and after a security breach.

- Detection and Escalation
  - Forensic investigation fees
  - Crisis management consulting
  - Legal and regulatory notification costs
- Notification and Response
  - Credit monitoring services for affected customers
  - PR campaigns for damage control
  - Regulatory fines and penalties
- Post-Breach Recovery
  - System restoration and patching
  - Loss of revenue from interrupted operations
  - Increased future insurance premiums



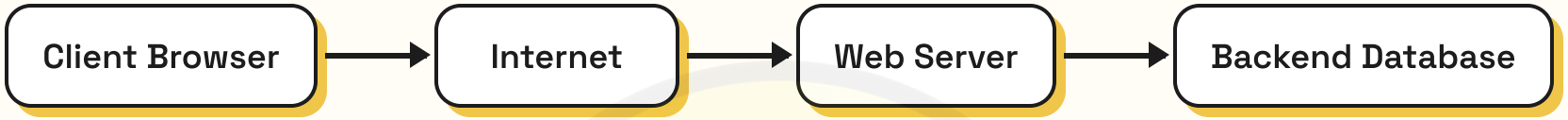
Webservers

WEB SERVER ARCHITECTURE

A computer system that stores, processes, and delivers web pages to users over the Internet using the Hypertext Transfer Protocol (HTTP) or HTTPS.

- Acts as the bridge between client browsers and backend databases.
- Processes incoming requests and serves static content (HTML, images) or dynamic content.
- Popular examples include Apache HTTP Server, Nginx, and Microsoft IIS.

Web Server Request-Response Flow

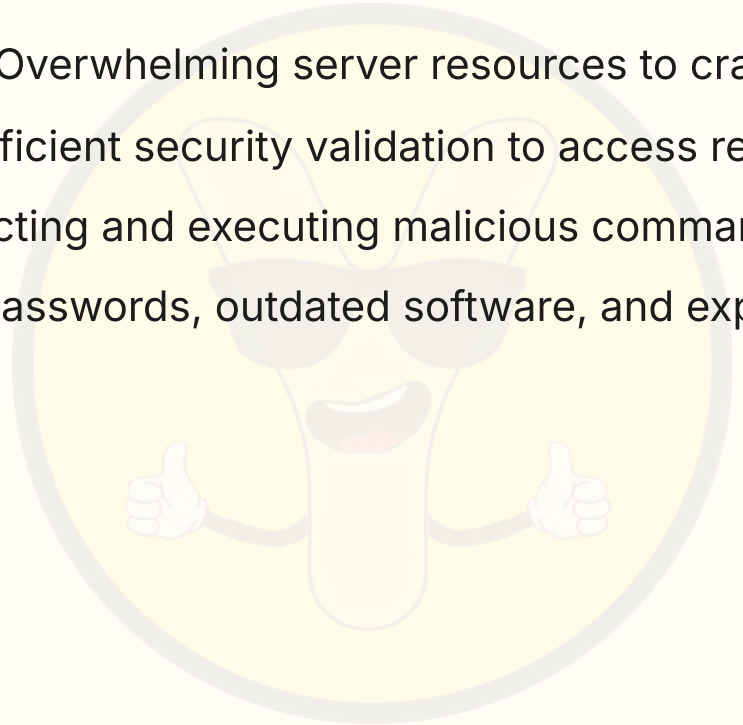


Standard workflow of an HTTP request passing from client to web server and application database.

Attacks on Webservers

Web servers are prime targets because they are publicly accessible 24/7.

- Denial of Service (DoS) and DDoS: Overwhelming server resources to crash the service.
- Directory Traversal: Exploiting insufficient security validation to access restricted files.
- Remote Code Execution (RCE): Injecting and executing malicious commands on the host server.
- Misconfiguration Exploits: Default passwords, outdated software, and exposed administrative panels.



Web Application Vulnerabilities

APPLICATION-LAYER FLAWS

Security bugs or weaknesses in the design, coding, or implementation of web applications that allow attackers to bypass security controls.

- Categorized systematically by the OWASP Top Ten project.
- Includes Injection flaws, Broken Authentication, and Security Misconfigurations.
- Occurs primarily due to lack of input validation and insecure coding practices.

Cross-Site Scripting (XSS)

XSS VULNERABILITY

An injection vulnerability where malicious scripts are injected into otherwise benign and trusted websites, executing in the victim's browser.

- Happens when an application includes untrusted data in a web page without proper validation or escaping.
- Allows attackers to steal session cookies, capture keystrokes, or redirect users.
- Three primary types: Stored XSS, Reflected XSS, and DOM-based XSS.

Types of Cross-Site Scripting (XSS)

Type	Mechanism	Persistence
Stored XSS	Malicious script is permanently saved on the target server (e.g., in a database comment).	High (affects every user viewing the page)
Reflected XSS	Script is reflected off a web server in an immediate error message or search result.	Low (requires victim to click a crafted link)
DOM-based XSS	Vulnerability exists in client-side code rather than server-side code.	Variable (manipulates the Document Object Model)

Cyber Security: Organizational Implications

Cyber security is no longer just an IT issue; it is a core enterprise governance priority.

- Strategic Impact: Board-level accountability for cyber risk management and incident response planning.
- Operational Continuity: Maintaining business operations during and after an attack without severe revenue loss.
- Reputational Damage: Loss of customer loyalty, negative media coverage, and reduced stock valuation.
- Legal and Regulatory Compliance: Mandatory adherence to data protection laws (e.g., GDPR, IT Act 2000).

Understanding Intellectual Property Rights (IPR)

INTELLECTUAL PROPERTY RIGHTS

Legal rights that protect creations of the mind, such as inventions, literary and artistic works, designs, symbols, and names used in commerce.

- Grants creators exclusive rights to use and commercialize their creations for a specific period.
- Encourages innovation by ensuring creators reap financial and recognition rewards.
- Digital transformation makes IPR highly vulnerable to cyber theft and unauthorized duplication.

Internet Intellectual Property

The extension of traditional intellectual property laws into the digital and networked domain.

- Covers digital assets including source code, website designs, digital media, and domain names.
- Domain Name Disputes: Cybersquatting involves registering domain names of well-known brands in bad faith.
- Digital Rights Management (DRM): Technologies used by hardware manufacturers and copyright holders to control access to digital content.
- Jurisdictional Challenges: Enforcing IPR across international borders on the internet is complex.

Copyright Infringement

COPYRIGHT VIOLATION

The unauthorized use, reproduction, distribution, performance, or display of copyrighted material without permission from the copyright holder.

- Protects original works of authorship fixed in any tangible medium of expression.
- In cyber security, this includes unauthorized downloading of software, cracking digital rights management, and pirating digital media.
- Remedies include statutory damages, injunctions, and criminal prosecution.

Patents

PATENT PROTECTION

A government authority or license conferring a right or title for a set period, especially the sole right to exclude others from making, using, or selling an invention.

- Must be novel, non-obvious, and useful.
- In software and cyber security, patents protect unique cryptographic algorithms, security protocols, and hardware architectures.
- Lasts typically for 20 years from the filing date.

Trademarks

TRADEMARK PROTECTION

A symbol, word, or words legally registered or established by use as representing a company or product.

- Protects brand identity, logos, slogans, and company names.
- Prevents competitors from confusing consumers with deceptive branding.
- Crucial online to combat phishing sites that mimic legitimate trademarked domain names and logos.

Data Theft

DATA EXFILTRATION

The unauthorized stealing, copying, or retrieval of confidential, sensitive, or proprietary data from a computer or corporate network.

- Involves internal threats (malicious insiders) and external threats (APT groups, hackers).
- Targets personally identifiable information (PII), financial records, and proprietary source code.
- Mitigated via Data Loss Prevention (DLP) tools, encryption at rest, and strict access controls.

Exam corner

- **Q1** Define cost of cybercrimes and explain the components contributing to financial loss in an enterprise.
- **Q2** What are webservers? Discuss common attacks launched against web servers.
- **Q3** Explain Cross-Site Scripting (XSS) with its types and prevention mechanisms.
- **Q4** What are the organizational implications of poor cyber security practices?
- **Q5** Differentiate between Copyright, Patents, and Trademarks in the context of internet intellectual property.
- **Q6** Explain copyright infringement and its legal consequences in digital environments.
- **Q7** Discuss data theft, its causes, and methods used by organizations to prevent data exfiltration.

Unit 4 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 5 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

