International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Study on Cyber Crime Trends and Predictive Analysis

Dhananjay Rao 1, Dr. Sandeep Yadav2, Prof. Nishant Kushwaha3, Prof. Shekhar Choudhary4

Department of Fire Technology & Safety Engineering1,2,3,4

School of Engineering and Technology1,2,3,4

Vikrant University,Gwalior(M.P)

ABSTRACT

Organizations strive to prevent unauthorized access to their information systems and protect the data entrusted to them by clients, partners, and other stakeholders. Safeguarding these systems from malicious or inadvertent actions that may destroy information or disrupt operations is essential. Equally important is preventing attackers from impersonating legitimate entities. To operate securely in a connected digital environment, organizations must trust the systems from which they retrieve information and conduct online transactions. A lack of security can lead to theft, data loss, operational disruptions, and—crucially—loss of trust.

Cyber crime refers to the criminal or irresponsible actions of users who exploit the widespread reach of computer networks. These acts pose major challenges to the ethical use of information technology. Cybercrime threatens the confidentiality, integrity, and availability of data, underscoring the need for strong security controls. This paper presents selected case studies that illustrate the vulnerability of web services to sophisticated attacks. It also emphasizes the importance of effective controls that ensure the accuracy, integrity, and safety of information and information system activities.

INTRODUCTION

The need for robust information security has been highlighted by recent incidents, including a warning issued by Kapil Sibal, former Union Minister for Communications, regarding the circulation of defamatory and morphed images of national leaders on Facebook. During meetings with representatives of Facebook, Google, YouTube, and Yahoo, the Minister urged these platforms to develop mechanisms to filter such content. However, platform representatives expressed their limitations due to high content volume and overseas server locations (Joshi, 2011). This incident underscores the potential for misuse of online platforms and the resulting security implications.

Historically, organizational computer systems operated in isolation, centrally managing all business functions. In contrast, today's enterprises are deeply interconnected through the Internet, transforming isolated computing environments into globally networked systems. The rapid expansion of the Internet and the World Wide Web, which now support millions of users, has significantly increased accessibility—and with it, vulnerability (Ackermann, 2002).

Any system connected to the Internet can potentially be accessed by others on the network. This interconnectedness necessitates a heightened concern for information security, both to protect one's own systems and to ensure trust in the systems of others (Ackermann, 2002). A computing system—comprising hardware, software, storage media, data, and people—can be targeted at any point (Pfleeger et al., 2009). The diversity of targets and the sophistication of attacks make computer security increasingly challenging.

Organizations must prevent unauthorized access to confidential information, safeguard against data destruction, and avoid impersonation attacks. The growing need for security arises from several factors (Pfleeger et al., 2009):

1. Increasing sophistication and frequency of cyber-attacks
2. Availability of powerful attack tools on the Internet
3. Rapid growth of networked systems
4. Increased sharing of confidential data across enterprise networks
5. Market products prioritizing usability over security
6. Shortage of specialized cybersecurity professionals

Missing or compromised information can severely damage an organization's reputation and lead to loss of clients. As networks become pervasive, computer security now encompasses securing not only standalone systems but also the broader network infrastructure. The major technical pillars of security—Confidentiality, Integrity, and Availability (CIA)—form the foundation of modern security practices (Kinkus, 2002).

With the widespread adoption of IT, cybercrimes have escalated, often committed by organized groups skilled in exploiting system vulnerabilities. These groups manipulate unsuspecting victims, resulting in large-scale financial losses. This paper presents real case studies to illustrate such vulnerabilities and highlights the pressing need for strong controls to protect information.

CYBER CRIMES

Cyber crime involves criminal or irresponsible activities carried out using computer systems and networks. These actions compromise the ethical use of information technology and threaten the integrity, safety, and reliability of business information systems. Common forms of cybercrime include theft of money, data, and services; destruction of data through malware; and unauthorized system access via hacking.

This section presents selected case studies illustrating the vulnerability of web services and the innovative techniques employed by attackers.

Case Study 1: Fake Website and Fake Employment Scam

Two engineering graduates created a fraudulent website mimicking a legitimate IT company. Using stolen candidate databases—acquired with assistance from a security guard of the real company—they conducted fake interviews and emailed job offers. Selected candidates were instructed to deposit ₹30,000 into what they believed was the company's bank account. The account, however, belonged to an unrelated person from Assam whose debit card had been stolen earlier. The scammers withdrew the money using ATMs in remote areas, cheating applicants of ₹2.4 lakh (Vijay Kumar, 2010).

Case Study 2: Stolen Emails at the Climate Summit

During the Climate Summit in Copenhagen, thousands of stolen emails and files from a leading climate research institute were leaked. This incident triggered a global debate, with some countries—such as Saudi Arabia—questioning the scientific foundation of the climate negotiations (Revkin & Broder, 2009). This case highlights the high stakes involved when sensitive information is compromised.

SECURITY IN NETWORKS

Computing networks are prime targets for attackers. While standalone systems may face minimal risk, networked computers introduce significantly greater exposure. Information security involves protecting information from

unauthorized access, disclosure, disruption, modification, or destruction. Although terms like "information security," "computer security," and "information assurance" are often used interchangeably, they differ slightly in approach and emphasis.

Governments, corporations, hospitals, and financial institutions rely heavily on secure information systems. The massive volume of sensitive data stored and transmitted electronically makes strong network security practices essential.

SECURITY CLASSIFICATION OF INFORMATION

Effective information security begins with recognizing the value of information and assigning appropriate protection levels. Information classification ensures that sensitive data receives adequate safeguards.

The classification process includes:

1. Assigning ownership of the information to a senior manager
2. Developing a classification policy that defines labels and criteria
3. Determining required security controls for each classification level

Classification depends on factors such as the information's value, age, relevance, and legal or regulatory requirements.

Common classification levels include:

- **Business Sector:** Public, Sensitive, Private, Confidential
- **Government Sector:** Unclassified, Restricted, Confidential, Secret, Top Secret
- **Cross-Sector:** Traffic Light Protocol (White, Green, Amber, Red)

WHY CONTROLS ARE NEEDED

Managers are responsible for monitoring the performance, quality, and security of information systems. Like other vital business assets, hardware, software, networks, and data must be protected through well-designed controls.

Effective controls ensure:

- Accuracy of information
- Integrity of data
- Security of system operations
- Protection against fraud, errors, and system destruction

Controls enhance the quality and reliability of computer-based information systems and reduce vulnerabilities in complex, interconnected environments (O'Brien, 1999).

CONCLUDING REMARKS

In today's digital world, networks are indispensable, enabling countless essential services. However, as demonstrated through the case studies, web services remain vulnerable to attacks by malicious actors. Effective security controls are crucial to safeguarding information systems, ensuring data accuracy, preserving integrity, and protecting organizational assets from fraud and disruption.

REFERENCES

1. Ackermann, E., (2002), "Legal Issues, Ethical Issues, Privacy, and Security," Webliminal.com Production, Legal Issues, Ethical Issues, Privacy, and Security.mht.

2. Bisaerts, D., (2011), "Dutch Police Closes Websites from 2 Escort Agencies,"Information Security News, Tuesday, 11 January.

3. Bisaerts, D., (2010), "ABN-Amro Looses 5.6 million Euro inCyber theft," Information Security News, Wednesday, 22 December.

4. FinCen, (2003), "Fraudulent Use of Canada Post Money Orders," Financial Crimes of Enforcement Network, United States Department of Treasury, December 2003.

5. Guido, (2011), "US Cyber security Research Lab Hacked,"Information Security News, Wednesday, 20 April.

6. Joshi, S., (2011), "Sibal Warns Social Websites over Objectionable Content," The Hindu, Chennai, Vol. 134, No. 288, Tuesday, December 6, pp. 14.

7. Revkin, A.C. and Broder, J.M., (2009), "Leaked Emails Give Naysayers Ammo," Times Global, The Times of India, Tuesday, December 9, Vol. 2, Issue 290, pp. 11.

8. Umstead, M., (2010), "Former Red Cross Worker Charged with Embezzling Agency's Funds," The Herald Mail, MAY 24.

9. Vijay Kumar, S., (2010), "Two Engineering Graduates Held for Fraud," The Hindu, Vol. 133, No. 32, February 8, pp. 1.