



# Cybercrime Trends and Data Protection in India (2020–2024)

## *A Review of Official Statistics, Regulatory Frameworks, and Security Practices*

<sup>1</sup>Mohammad Naeem Kanyar

<sup>1</sup>Independent Researcher

<sup>1</sup>Punjab, India

**Abstract:** India's expansion of digital payments, online public services, cloud platforms, mobile applications, and data-driven business operations has increased the importance of cybersecurity and data protection. These systems create substantial benefits but also expose individuals and organizations to phishing, financial fraud, identity misuse, ransomware, unauthorized access, and personal-data exposure. This paper presents a structured narrative review of official Indian publications, statutory materials, recognized security frameworks, and selected academic literature. To ground the analysis in official evidence, it examines National Crime Records Bureau (NCRB) figures for registered cybercrime cases during 2020–2024. The number of cases increased from 50,035 in 2020 to 52,974 in 2021, 65,893 in 2022, 86,420 in 2023, and 101,928 in 2024, an increase of approximately 103.7% across the five-year series. These figures measure registered cases involving communication devices as a medium or target; they do not represent all cyberattacks or data breaches. The review identifies five priorities: stronger identity and access management, lifecycle protection of personal and organizational data, faster detection and response, improved security capacity among smaller organizations, and measurable implementation of legal and governance obligations. It proposes a risk-based framework that combines governance, asset identification, prevention, monitoring, incident response, recovery, and privacy-by-design practices. The paper concludes that India's cybersecurity resilience depends on sustained implementation, institutional coordination, responsible data handling, and transparent evidence about incidents and outcomes.

**Index Terms** - Cybersecurity, data security, India, cybercrime, data protection, digital privacy, CERT-In, NCRB, risk management, incident response.

## I. INTRODUCTION

Digital transformation has changed how people in India access financial services, communicate, obtain public services, study, work, and conduct business. Mobile banking, digital payment systems, online marketplaces, cloud applications, and digital public infrastructure have made many activities more accessible. At the same time, these systems process increasing volumes of personal, financial, commercial, and operational information. Protecting the confidentiality, integrity, and availability of that information is therefore central to the reliability of digital services.

Cybersecurity and data security are related but distinct. Cybersecurity concerns the protection of systems, networks, applications, and digital environments from threats that may disrupt operations or compromise information. Data security focuses on protecting information from unauthorized access, alteration, disclosure, destruction, or loss throughout its lifecycle. Privacy adds a further dimension: information may be stored securely but still be collected, used, retained, or shared in inappropriate ways.

India's official cybercrime statistics provide a useful starting point. The Ministry of Home Affairs reports 50,035 cases registered under cybercrimes involving communication devices as a medium or target in 2020 and 101,928 in 2024 [1], [2]. The official series also records 52,974 cases in 2021, 65,893 in 2022, and 86,420 in 2023. These figures are important but must be interpreted carefully: registered cases reflect reporting and police-registration processes and do not count every attempted attack, successful intrusion, exposed record, or unreported incident. Foundational security literature emphasizes that protection depends on layered design and carefully bounded authority, not only on perimeter controls [17], [24].

This review connects official evidence with established cybersecurity principles and Indian data-protection developments. Its objectives are to examine registered cybercrime trends; distinguish cybercrime, cybersecurity incidents, data breaches, and privacy risks; review relevant legal and institutional arrangements; identify technical and organizational challenges; and propose a practical framework for improving protection.

## II. RESEARCH METHODOLOGY

This paper uses a structured narrative review with descriptive analysis of official secondary data. It is not a registered systematic review, meta-analysis, field survey, or experimental study. The evidence base is organized into four groups: (i) official Indian cybercrime statistics and government publications; (ii) Indian legislation, rules, and institutional guidance relevant to information security and personal data; (iii) international standards and technical guidance; and (iv) selected academic publications on security, privacy, and human factors.

The principal quantitative source is the NCRB state/Union Territory data for cases registered under cybercrimes involving communication devices as a medium or target during 2020–2024, reproduced in Annexure I of the Ministry of Home Affairs release dated 21 July 2026 and associated with the NCRB Crime in India 2024 reporting series [1], [2]. National totals are used to calculate annual percentage changes and the cumulative change. The analysis is descriptive and does not infer causality.

Sources were organized thematically around registered crime trends, threats to accounts and data, governance and legal responsibilities, preventive and detective controls, incident response, and implementation challenges. Official documents were prioritized for Indian statistics and legal claims. International standards were used as implementation references, not as evidence of the prevalence of cybercrime in India.

The method has limitations. NCRB figures measure registered cases, not the complete number or financial impact of cyber incidents. This paper does not analyze individual state records beyond the national totals, organization-level logs, or a dataset of confirmed breaches. The literature synthesis is thematic rather than exhaustive: no database-by-database search protocol, duplicate screening, or formal risk-of-bias scoring is claimed. Legal and regulatory requirements may change and should be checked against the official text before operational use.

### III. ANALYSIS OF OFFICIAL CYBERCRIME TRENDS IN INDIA

The official NCRB series provides national totals for registered cybercrime cases from 2020 through 2024 [1], [2]. Table I presents all five annual totals and the year-on-year changes calculated from those figures.

TABLE I. REGISTERED CYBERCRIME CASES IN INDIA, 2020–2024

| Year | Registered cases | Absolute change | Percentage change |
|------|------------------|-----------------|-------------------|
| 2020 | 50,035           | —               | —                 |
| 2021 | 52,974           | +2,939          | +5.9%             |
| 2022 | 65,893           | +12,919         | +24.4%            |
| 2023 | 86,420           | +20,527         | +31.2%            |
| 2024 | 101,928          | +15,508         | +17.9%            |

Between 2020 and 2024, registered cases increased by 51,893, or approximately 103.7%. The annual growth rate was highest in 2023 within this period (approximately 31.2%), while the total continued to rise in 2024 by approximately 17.9%. These calculations describe the recorded series; they do not establish why the increase occurred. Possible influences include growth in digital activity, changes in criminal methods, public awareness, reporting behavior, law-enforcement capacity, and registration or classification practices. Aggregate totals cannot isolate the contribution of these factors.

Three distinctions are important. First, a registered case is not necessarily equivalent to one unique attack: a campaign may generate multiple complaints, while another incident may never be reported. Second, cybercrime is broader than data breaches; recorded cases may involve offenses without a confirmed database compromise, while some security incidents may not appear in criminal-case statistics. Third, the totals do not describe the number of affected individuals, exposed records, financial losses, recovery time, or conviction outcomes. NCRB data should therefore be complemented by breach reports, organizational incident metrics, financial-loss data, and victimization studies where available.

### IV. MAJOR CYBERSECURITY AND DATA-SECURITY THREATS

#### A. Phishing and social engineering

Phishing manipulates people into disclosing credentials, approving transactions, downloading malicious files, or visiting fraudulent websites. Messages may imitate banks, delivery services, employers, government departments, or familiar contacts. Awareness training is useful but insufficient on its own. Organizations should combine education with multifactor authentication, phishing-resistant authentication where practical, transaction verification, email filtering, domain protection, and accessible reporting channels.

#### B. Identity theft and account compromise

Stolen passwords, reused credentials, weak recovery procedures, and compromised devices can enable unauthorized access to email, banking, cloud storage, and business applications. Email accounts are particularly valuable because they can reset credentials for other services. Recommended controls include multifactor authentication, unique credentials, password managers, least-privilege access, prompt removal of former employees' access, and monitoring for unusual sign-in activity.

#### C. Malware and ransomware

Malware may steal information, monitor activity, establish unauthorized access, or disrupt operations. Ransomware can encrypt files and may also involve theft of information. Organizations should maintain supported software, restrict administrative privileges, filter suspicious files, segment networks, monitor endpoints, and preserve protected backups. Backup availability is not enough: restoration should be tested and backup credentials and storage should be protected against compromise.

#### D. Data breaches and unauthorized disclosure

Data exposure can result from malicious activity, misconfigured cloud storage, excessive permissions, vulnerable applications, lost devices, insecure transfers, or mistakes by authorized personnel. Data security should cover collection, storage, use, transfer, retention, and deletion. Data minimization reduces the volume of information an organization must protect, while encryption, access controls, retention schedules, and secure deletion reduce exposure through the lifecycle. Privacy scholarship and formal models such as k-anonymity and differential privacy offer complementary ways to reason about disclosure risk, although they do not replace access control or operational security [25], [29].

## E. Application, API, cloud, and supplier risks

Weak authentication, insufficient authorization, insecure session management, poor input validation, exposed secrets, and unpatched dependencies can expose applications and APIs. Cloud misconfiguration and supplier compromise can expand the attack surface. A secure development process should include threat modelling, code review, dependency management, security testing, controlled deployment, and remediation tracking. The OWASP Top 10 and Application Security Verification Standard provide practical references for application security [7], [8], while the NIST Secure Software Development Framework supports the integration of security practices throughout software development [35].

## F. Insider threats and human error

Insider-related incidents may involve malicious conduct, negligence, accidental disclosure, or misuse of legitimate access. Role-based permissions, separation of duties, audit trails, staff training, clear policies, and proportionate investigation procedures help reduce risk. Access should be reviewed when responsibilities change and revoked when no longer needed.

# V. INDIAN DATA-PROTECTION AND INSTITUTIONAL CONTEXT

## A. Information Technology Act and related rules

The Information Technology Act, 2000 provides a foundational legal framework for electronic records, electronic transactions, and specified cyber-related matters [9]. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 are also relevant to the historical development of information-security and personal-information requirements [10]. Their present application must be assessed alongside later legislation, rules, commencement notifications, and any relevant transition or supersession provisions.

## B. Digital Personal Data Protection Act and Rules

The Digital Personal Data Protection Act, 2023 establishes a statutory framework for processing digital personal data in India [11]. The Digital Personal Data Protection Rules, 2025 were notified in November 2025 [12]. The Rules use a staged commencement: some provisions took effect on publication, Rule 4 is scheduled to commence one year after publication, and Rules 3, 5–16, 22, and 23 are scheduled to commence eighteen months after publication. Consequently, as of October 2026, not every rule is yet in force. Organizations should verify the current commencement notifications and applicable obligations rather than assuming that all provisions apply on the same date.

## C. CERT-In and incident response

The Indian Computer Emergency Response Team (CERT-In) is a national institution for cybersecurity incident response and guidance. Its directions issued on 28 April 2022 address specified information-security practices, incident reporting, maintenance of logs, and related requirements for entities within scope [13]. Organizations should consult the official directions and subsequent clarifications to determine the reporting timelines and obligations that apply to them. An incident plan should define event classification, containment, evidence preservation, recovery, communications, external reporting, and post-incident review. NIST incident-handling guidance provides a useful implementation reference [14].

## D. Sectoral regulation and critical infrastructure

Financial institutions, telecommunications providers, healthcare organizations, educational institutions, government bodies, and critical infrastructure operators face different operational and regulatory requirements. Financial institutions should consider applicable Reserve Bank of India requirements [15]. The National Critical Information Infrastructure Protection Centre is relevant to the protection of designated critical information infrastructure [16]. A generic checklist is a starting point, not a substitute for sector-specific legal and operational analysis.

## E. International standards

NIST Cybersecurity Framework 2.0 organizes cybersecurity outcomes into Govern, Identify, Protect, Detect, Respond, and Recover [3]. ISO/IEC 27001:2022 specifies requirements for an information security management system, while ISO/IEC 27701 addresses privacy information management [4], [5]. These standards can support implementation and continual improvement, but they do not replace Indian law or automatically establish compliance with every applicable requirement.

# VI. PROPOSED RISK-BASED FRAMEWORK

This review proposes a practical framework that combines organizational governance with technical controls and privacy-by-design practices. It adapts established risk-management principles for organizations with different sizes and maturity levels. The framework is a synthesis proposed by this paper; it has not been empirically validated through a field deployment. Its emphasis on risk assessment, access control, identity, continuity, and secure software development is consistent with established NIST and ISO guidance [6], [21]–[24], [34], [35].

## A. Govern

Assign accountable owners for cybersecurity risk, incident coordination, and data-protection responsibilities. Maintain a risk register, approve exceptions, define supplier expectations, and connect security decisions to business continuity and applicable legal obligations.

## B. Identify

Inventory servers, endpoints, applications, cloud services, APIs, privileged accounts, suppliers, and data repositories. Record data categories, purposes, storage locations, access rights, retention periods, and the impact of disclosure or loss. Keep inventories usable and current.

**C. Protect**

Apply multifactor authentication for remote and privileged access; least-privilege permissions; timely updates; encryption for sensitive data in transit and where appropriate at rest; secure configuration; endpoint protection; secure development; vulnerability management; and protected backups. Select controls proportionate to risk and operational context.

**D. Detect**

Collect useful logs, define alert ownership, and investigate suspicious activity. Indicators may include repeated failed logins, unexpected privilege escalation, abnormal access to large data volumes, unusual outbound transfers, suspicious mailbox rules, or unauthorized changes to security settings. Monitoring should be lawful and proportionate.

**E. Respond**

Define the incident coordinator, technical responders, management decision-maker, legal or privacy contact, and communications lead. Procedures should cover classification, containment, evidence handling, remediation, applicable notifications, and communication. Test the plan through tabletop exercises and technical drills.

**F. Recover and improve**

Define recovery-time and recovery-point objectives for important services. Test restoration under realistic conditions and confirm that restored systems are trusted, data integrity has been assessed, compromised credentials have been addressed, and the root cause has been mitigated. Assign owners and deadlines to corrective actions.

**TABLE II. PROPOSED CONTROL FRAMEWORK AND MEASURES**

| Function | Priority actions                                                | Example measure                                |
|----------|-----------------------------------------------------------------|------------------------------------------------|
| Govern   | Assign accountability; maintain risk register; review suppliers | High risks with an assigned owner              |
| Identify | Inventory critical assets, data stores, and privileged accounts | Percentage of critical assets inventoried      |
| Protect  | MFA, patching, least privilege, encryption, backups             | MFA coverage; overdue critical vulnerabilities |
| Detect   | Centralize relevant logs; triage alerts                         | Median time to detect and triage               |
| Respond  | Maintain playbooks; rehearse escalation                         | Time to contain; exercise actions closed       |
| Recover  | Test restoration and continuity                                 | Successful restoration tests                   |
| Improve  | Review incidents and track remediation                          | Corrective actions completed on time           |

The measures in Table II are proposed indicators, not results from an organizational field study. Their value depends on consistent definitions, appropriate baselines, and review of unintended effects. Purchasing security products without improving access management, patching, or recovery capability may leave substantial risks unresolved.

**VII. IMPLEMENTATION CHALLENGES****A. Uneven capability and limited resources**

Large organizations may have specialist security teams, while smaller enterprises, schools, local service providers, and nonprofits may lack dedicated expertise. A manageable baseline—MFA, reliable patching, restricted administrator access, tested backups, secure email practices, and a clear incident contact—can be a practical first step. Outsourcing can provide expertise but does not remove internal accountability.

**B. Skills and awareness**

Training should be tailored to roles. Developers need secure coding and dependency management; finance staff need transaction verification; administrators need privileged-access safeguards; and managers need risk ownership and incident decision-making. Attendance alone is not evidence of effectiveness. Reporting rates, time to report, recurring violations, and remediation outcomes are more informative.

**C. Legacy systems and technical debt**

Unsupported or difficult-to-update systems can leave known weaknesses unresolved. Organizations should identify unsupported components, assess exposure, restrict connectivity, strengthen monitoring, and prioritize replacement. Temporary compensating controls should be documented and reviewed rather than treated as permanent substitutes.

**D. Privacy, usability, and reporting**

Controls should be proportionate and usable. Excessive friction can encourage insecure workarounds, while unnecessary monitoring can undermine trust. Clear incident-reporting routes should distinguish police complaints from regulatory or sectoral notification. Better consistency in definitions and reporting would support stronger comparisons, provided differences in coverage and classification are acknowledged.

**VIII. DISCUSSION AND RECOMMENDATIONS**

Three conclusions follow from the review. First, registered cybercrime cases increased substantially over 2020–2024, but the aggregate series cannot explain the causes or measure all cyber incidents. Second, cybersecurity and data protection must be managed together: a system may resist external intrusion yet expose information through excessive permissions, unnecessary retention, insecure supplier access, or inadequate recovery. Third, organizations need a model that can be scaled according to risk and resources.

**A. Recommendations for organizations**

(1) Assign clear accountability. (2) Inventory critical assets, sensitive data, suppliers, and privileged accounts. (3) Strengthen identity security through MFA, least privilege, secure recovery, and prompt access revocation. (4) Prioritize critical vulnerabilities and maintain supported software. (5) Apply data minimization, access control, encryption, retention schedules, and secure

deletion. (6) Prepare and rehearse incident procedures. (7) Test backups and restoration. (8) Review supplier access and incident responsibilities. (9) Track a small set of meaningful security measures and corrective actions.

## B. Recommendations for institutions and policymakers

Continue practical cybersecurity guidance, incident-reporting information, and capacity building. Improve coordination among relevant agencies and sectoral bodies. Where reliable data are available, distinguish registered cases, reported complaints, confirmed incidents, data breaches, financial losses, and investigation outcomes, and document definitions and coverage so comparisons are meaningful.

## C. Recommendations for users

Use unique passwords, enable MFA, install updates, verify payment requests through independent channels, and never disclose authentication codes. Research on usable security shows that security advice must be practical and compatible with human behavior to be followed consistently [30], [31]. Threat reports also provide a useful reminder that attackers exploit both technical weaknesses and human workflows [32], [33]. Report suspected fraud through the appropriate official channel, particularly where a financial or account compromise may have occurred. These measures reduce exposure but cannot prevent every attack.

## IX. FUTURE RESEARCH DIRECTIONS

Future work could analyze NCRB state/UT data over a longer period while accounting for population, internet usage, reporting practices, and classification changes. Raw case counts should not be treated as direct risk measures without appropriate denominators.

A carefully constructed incident dataset could distinguish financial fraud, account compromise, ransomware, unauthorized disclosure, and other categories, helping researchers examine which forms of cybercrime are associated with confirmed personal-data exposure.

Surveys or structured audits could assess MFA adoption, patch management, backup testing, incident preparedness, and supplier risk among small and medium-sized organizations. Representative sampling would be necessary before generalizing findings across India.

Longitudinal case studies could compare detection time, containment time, recovery performance, and recurring incidents across organizations with different security practices. Research on privacy implementation could examine how legal requirements translate into data inventories, retention controls, access reviews, and incident procedures.

## X. CONCLUSION

Cybersecurity and data security are essential to the reliability of India's expanding digital ecosystem. Official NCRB figures show that registered cybercrime cases increased from 50,035 in 2020 to 101,928 in 2024, a rise of approximately 103.7% [1], [2]. The series describes recorded cases and should not be mistaken for a complete count of cyberattacks or data breaches. Effective protection requires more than individual security products: organizations need to understand their assets and data, manage identity and access, maintain systems, monitor suspicious activity, prepare for incidents, protect backups, and learn from security failures. These practices should be integrated with privacy responsibilities and the applicable Indian legal and sectoral context. The proposed framework combines governance, identification, protection, detection, response, recovery, and continual improvement. Future research should develop more comparable evidence on incident types, financial impacts, data exposure, organizational readiness, and recovery outcomes. Stronger cybersecurity ultimately depends on sustained implementation, responsible data handling, institutional coordination, and reliable evidence about what works.

## ACKNOWLEDGEMENT AND DATA LIMITATIONS

The author acknowledges the National Crime Records Bureau (NCRB), the Ministry of Home Affairs, the Indian Computer Emergency Response Team (CERT-In), and other cited public institutions for making official reports, statistics, advisories, and legal materials available for research. These institutions are cited as information sources only; their inclusion does not imply that they reviewed, approved, or endorse this article.

**Data scope and interpretation:** The annual figures discussed in this review represent cybercrime cases registered and reported in the cited official sources for the specified years. They should not be read as a complete count of all cyber incidents, attempted attacks, unreported offences, affected individuals, or data breaches in India. Recorded figures may be influenced by reporting behaviour, police registration and classification practices, changes in definitions or procedures, and the availability and timing of official publications. Year-to-year comparisons are descriptive and do not, by themselves, establish the causes of an increase or decrease. The analysis is limited to the sources and period identified in the article; any figures or interpretations should be checked against the original cited publications before reuse. Where a source does not provide a measure, this article does not claim that the measure is known.

**Disclaimer:** This article is an academic review and is not legal advice, an official government statement, or a guarantee of compliance with any law. The discussion of statutes and regulatory requirements is informational and should be verified against the applicable legislation, rules, amendments, and official guidance in force at the relevant time. The author has taken care to attribute information to cited sources, but readers should consult the original records for decisions requiring authoritative or legal reliance.

## REFERENCES

- [1] Ministry of Home Affairs, Government of India, "National Cyber Crime Data," Press Information Bureau, 21 July 2026. Annexures I–II: State/UT-wise and crime-head-wise cases registered under cybercrimes during 2020–2024. Available: <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2287039>
- [2] National Crime Records Bureau, Ministry of Home Affairs, Government of India, Crime in India 2024, Volume I. New Delhi: NCRB, 2026. Available: <https://www.ncrb.gov.in/uploads/files/CrimeinIndia2024-Volume1.pdf>
- [3] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, 2024. doi: 10.6028/NIST.CSWP.29.

- [4] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27001:2022—Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements, 2022. <https://www.iso.org/standard/27001>
- [5] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27701:2025—Information Security, Cybersecurity and Privacy Protection—Privacy Information Management Systems—Requirements and Guidance, 2nd ed., October 2025. <https://committee.iso.org/standard/27701>
- [6] National Institute of Standards and Technology, Guide for Conducting Risk Assessments, NIST SP 800-30 Rev. 1, 2012. doi: 10.6028/NIST.SP.800-30r1.
- [7] OWASP Foundation, OWASP Top 10: The Ten Most Critical Web Application Security Risks. <https://owasp.org/www-project-top-ten/>
- [8] OWASP Foundation, Application Security Verification Standard (ASVS). <https://owasp.org/www-project-application-security-verification-standard/>
- [9] Government of India, The Information Technology Act, 2000, Act No. 21 of 2000, as amended. India Code: <https://www.indiacode.nic.in/>
- [10] Ministry of Communications and Information Technology, Government of India, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Official portals: <https://www.meity.gov.in/> and <https://www.indiacode.nic.in/>
- [11] Government of India, The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023. India Code: <https://www.indiacode.nic.in/>
- [12] Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, 13 November 2025. <https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf>
- [13] Indian Computer Emergency Response Team, Directions Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents under Section 70B of the Information Technology Act, 2000, 28 April 2022. <https://www.cert-in.org.in/>
- [14] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST SP 800-61 Rev. 3, April 2025. doi: 10.6028/NIST.SP.800-61r3.
- [15] Reserve Bank of India, Cyber Security Framework in Banks, Circular DBR.No.BP.BC.99/21.06.102/2015-16, 2 June 2016. <https://www.rbi.org.in/>
- [16] National Critical Information Infrastructure Protection Centre, Guidelines and resources for critical information infrastructure protection. Government of India. <https://nciipc.gov.in/>
- [17] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Hoboken, NJ: Wiley, 2020.
- [18] W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th ed. Pearson, 2018.
- [19] M. Bishop, Computer Security: Art and Science, 2nd ed. Boston, MA: Addison-Wesley, 2018.
- [20] B. Schneier, Secrets and Lies: Digital Security in a Networked World. New York: Wiley, 2000.
- [21] Joint Task Force, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5, 2020, updated. doi: 10.6028/NIST.SP.800-53r5.
- [22] D. Temoshok et al., Digital Identity Guidelines, NIST SP 800-63-4, July 2025. doi: 10.6028/NIST.SP.800-63-4.
- [23] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST SP 800-207, 2020. doi: 10.6028/NIST.SP.800-207.
- [24] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, 1975. doi: 10.1109/PROC.1975.9939.
- [25] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*, LNCS 4052. Berlin: Springer, 2006, pp. 1–12. doi: 10.1007/11787006\_1.
- [26] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, nos. 3–4, pp. 211–407, 2014. doi: 10.1561/04000000042.
- [27] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002. doi: 10.1142/S0218488502001648.
- [28] D. J. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, pp. 477–560, 2006. doi: 10.2307/40041279.
- [29] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015. doi: 10.1126/science.aaa1465.
- [30] C. Herley, "So long, and no thanks for the externalities: The rational rejection of security advice by users," in *Proceedings of the 2009 Workshop on New Security Paradigms*, 2009, pp. 133–144. doi: 10.1145/1719030.1719050.
- [31] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link'—A human/computer interaction approach to usable and effective security," *BT Technology Journal*, vol. 19, pp. 122–131, 2001. doi: 10.1023/A:1011902718709.
- [32] Verizon, 2024 Data Breach Investigations Report. Verizon Business, 2024. <https://www.verizon.com/business/resources/reports/dbir/>
- [33] European Union Agency for Cybersecurity, ENISA Threat Landscape 2023. Athens: ENISA, 2023. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- [34] International Organization for Standardization, ISO 22301:2019—Security and Resilience—Business Continuity Management Systems—Requirements, 2019. <https://www.iso.org/standard/75106.html>
- [35] National Institute of Standards and Technology, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST SP 800-218, 2022. doi: 10.6028/NIST.SP.800-218.