Indian Journal of Computer Science and Technology
https://www.doi.org/10.59256/indjcst.20260503094
Volume 5, Issue3 (September-December 2026), PP: 798-805.
www.indjcst.com
ISSN No: 2583-5300

Cyber Threats in the Digital Era: Challenges, Impacts, and Prevention Strategies

Raksha Devi[1], Alka Pathania[2], Shubham Chauhan[3]
[1,2, 3]*Department of Computer Science and Engineering, APG Shimla University, Himachal Pradesh, India.*

To Cite this Article: *Raksha Devi[1], Alka Pathania[2], Shubham Chauhan[3], "Cyber Threats in the Digital Era: Challenges, Impacts, and Prevention Strategies", Indian Journal of Computer Science and Technology, Volume 05, Issue 03 (September-December 2026), PP: 798-805.*

Copyright: ©2026 This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract: *The rapid spread of internet-connected services has widened the attack surface faced by individuals, enterprises, and governments. This paper reviews the major categories of cyber threat—phishing, malware, ransomware, computer viruses, denial-of-service attacks, and advanced persistent threats—and examines how each operates, what damage it causes, and where existing defenses tend to fall short. We then survey the principal preventive and detective controls, namely firewalls, intrusion detection and prevention systems, encryption, multi-factor authentication, patch management, and security awareness training, and compare their strengths and limitations in a structured way. A layered, defense-in-depth model is presented as a practical means of combining these controls, and the technical, human, and organizational challenges that hinder adoption are discussed. The review closes with emerging directions, including zero-trust architecture, machine-learning-assisted detection, and post-quantum cryptography. The goal is to give students, practitioners, and policy makers a concise reference for understanding present-day threats and planning proportionate defense.*

Key Word: *cyber security; cyber threats; phishing; malware; ransomware; intrusion detection; multi-factor authentication; defense in depth.*

I.INTRODUCTION

In today's digital world, information technology plays a vital role in communication, business operations, education, healthcare, banking, and government services. As the number of internet-connected devices and digital systems keeps growing, cyber threats have become one of the most significant challenges faced by individuals, organizations, and nations[1,2]. Cyber security is the practice of protecting computer systems, networks, applications, and digital information from unauthorized access, attack, damage, or theft. The overall relationship between digital systems, cyber threats, cyber-attacks, and cyber security measures is illustrated in Fig. 1.

This growing dependence on digital technology has given cybercriminals new opportunities to exploit weaknesses in systems and networks. Attacks such as phishing, malware, ransomware, computer viruses, denial-of-service (DoS) attacks, and advanced persistent threats (APTs) can lead to financial loss, data breaches, operational disruption, and reputational damage. Educational institutions, businesses, government agencies, and critical infrastructure operators have become frequent targets because of the valuable information they store and process.

As threats grow in complexity, traditional security measures alone are no longer enough. Organizations need a multi-layered approach that combines technical solutions, security policies, risk management practices, and user awareness programs[3]. Techniques such as firewalls, intrusion detection and prevention systems, encryption, multi-factor authentication, software patch management, and cyber security training all help reduce risk and protect digital assets.

This paper presents a review of the major cyber threats—phishing, malware, ransomware, and computer viruses, together with DoS attacks and APTs—and of their impact on organizations and society. It also examines the main prevention techniques, compares their advantages and limitations, and discusses the challenges of putting effective security frameworks into practice. The contributions are threefold: (i) a compact taxonomy of the threats, summarized in Table no 1; (ii) a structured comparison of prevention techniques in Tables no 3 and 4; and (iii) a defense-in-depth view that shows how the controls fit together. The remainder of the paper is organized as follows. Section II gives background and related work, Section III describes the threats, Section IV discusses their impact, Section V reviews prevention techniques, Section VI compares them and discusses open challenges, Section VII outlines future directions, and Section VIII concludes.

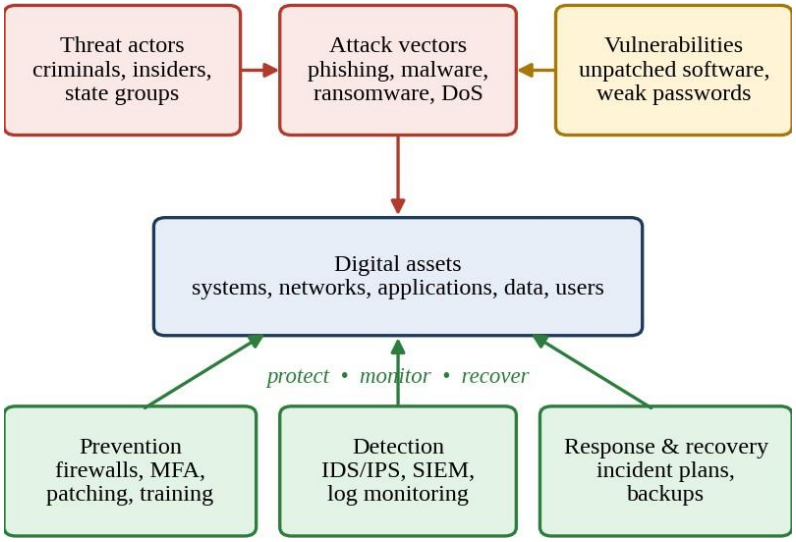


Fig. 1: Overview of the cybersecurity ecosystem: threat actors exploit vulnerabilities through attack vectors to reach digital assets, while layered controls protect, monitor, and recover.

II.BACKGROUND AND RELATED WORK

A. Basic Concepts

Cyber security is commonly framed around three goals: confidentiality, integrity, and availability, often called the CIA triad[4]. A *threat* is any circumstance or actor that could harm an asset, a *vulnerability* is a weakness that a threat can exploit, and *risk* is the likelihood and consequence of that exploitation. An *attack* is a deliberate attempt to exploit a vulnerability, and an *incident* is a security event that actually compromises an asset. Keeping these terms apart matters in practice, because controls are chosen to lower risk by reducing vulnerabilities or limiting what a threat can reach, not simply to stop "attacks" in general. Some authors also point out that cyber security is wider than traditional information security, because it covers the people and the assets reachable through cyberspace, not only the information itself[5].

B. Related Work

Most existing surveys look at one threat at a time. Alkhalil *et al.* analyze the anatomy of phishing attacks[6], Gupta *et al.* review the countermeasures proposed against them[7], and Krombholz *et al.* describe how social engineering has become more advanced[8]. Idika and Mathur review malware detection techniques[9], while Egele *et al.* survey the tools used to analyze malware dynamically[10]. Ransomware is covered by Kharraz *et al.*, who study how it behaves on infected systems[11], and by Oz *et al.*, who propose a taxonomy of its evolution and defenses[12]. Mirkovic and Reiher classify DDoS attacks and defenses[13], and Zargar *et al.* catalog defenses against flooding attacks[14]. For targeted attacks, Sood and Enbody examine APTs[15] and Alshamrani *et al.* survey their techniques and countermeasures[16]. Intrusion detection is reviewed broadly by Liao *et al.*[17], Buczak and Guven[18], and Khraisat *et al.*[19]. A systematic mapping study by Humayun *et al.* found that the literature concentrates on a few threats, namely phishing, denial of service, and malware[2]. On the process side, the intrusion kill chain model describes an attack as a sequence of stages that defenders can disrupt[20], and the NIST Cybersecurity Framework organizes defensive work into functions such as identify, protect, detect, respond, and recover[3]. Industry reports add field evidence on how breaches actually happen and what they cost[21,22]. The present review differs by putting several threat families and several prevention techniques side by side, so that a reader can see which control answers which threat.

C. Review Approach

The material was gathered from peer-reviewed surveys, standards and guidance from bodies such as NIST and ENISA, and well-known industry reports. Sources were chosen for relevance to the six threat families, for being widely cited or issued by recognized organizations, and for covering controls that organizations can realistically deploy. Where industry figures are quoted they are attributed to their source, and the qualitative ratings in Section VI are the authors' synthesis of the reviewed literature, not new measurements.

III. MAJOR CYBER THREATS

A. Phishing

Phishing uses deception rather than technical exploitation. The attacker poses as a trusted party, such as a bank, a colleague, or a delivery service, and persuades the victim to reveal credentials, open a malicious attachment, or approve a payment[8]. Delivery channels include email, text messages (smishing), voice calls (vishing), and cloned websites. Targeted variants such as spear phishing and whaling research a specific person or executive, and business email compromise abuses a convincing message to redirect payments[6]. Defenses combine blacklists, content filters, and learning-based classifiers, but each has coverage gaps, particularly against newly created sites[7]. Phishing remains attractive because it is cheap, scalable, and effective against users who are busy or unsure. Industry data consistently show that the human element is involved in roughly two-thirds of breaches[21], which explains why phishing so often serves as the first step of larger attacks.

B. Malware

Malware, short for malicious software, is the umbrella term for code written to damage systems or steal information. It includes trojans, worms, spyware, keyloggers, rootkits, bots, and fileless attacks that live only in memory. Early defenses relied on signatures, which are fingerprints of known samples, but attackers now use obfuscation, packing, and polymorphism to change a sample's appearance without changing its behavior[9]. Behavior-based and anomaly-based detection address this gap but tend to produce more false alarms. Running samples in a sandbox lets analysts observe what they actually do, although some malware checks for analysis environments and hides its behavior when it finds one[10]. Malware is frequently delivered through phishing, drive-by downloads, or compromised software updates, which is why it sits at the center of most attack chains.

C. Ransomware

Ransomware encrypts a victim's files, or locks the whole device, and demands payment for restoration. Studies of real samples show that modern families rely on strong cryptography and on quickly enumerating and encrypting user data, which leaves little room for recovery once execution starts[11]. Surveys also document how the field has moved from simple screen lockers to crypto-ransomware with worm-like spreading and extortion features[12]. Many groups now practice double extortion: they steal data before encrypting it and threaten to publish it, so that restoring from backup alone no longer ends the pressure. High-profile cases such as the 2017 WannaCry outbreak, which spread through an unpatched Windows file-sharing vulnerability[23], and the 2021 attack on the Colonial Pipeline operator[24] showed that ransomware can disrupt hospitals, transport, and fuel supply. Fig. 2 shows a typical attack sequence and the points at which a defender can interrupt it.

D. Computer Viruses

A computer virus is self-replicating code that attaches itself to a host file or program and spreads when the infected host is run or shared. Unlike worms, which spread across networks on their own, classic viruses depend on some user action such as opening a document or running a program. The idea was formalized in the 1980s[25]. Boot-sector viruses, macro viruses embedded in office documents, and file infectors are the best-known types. Although many headline incidents today involve other malware classes, viruses remain relevant because they motivated antivirus technology and because their replication ideas live on in modern worms and botnets[4].

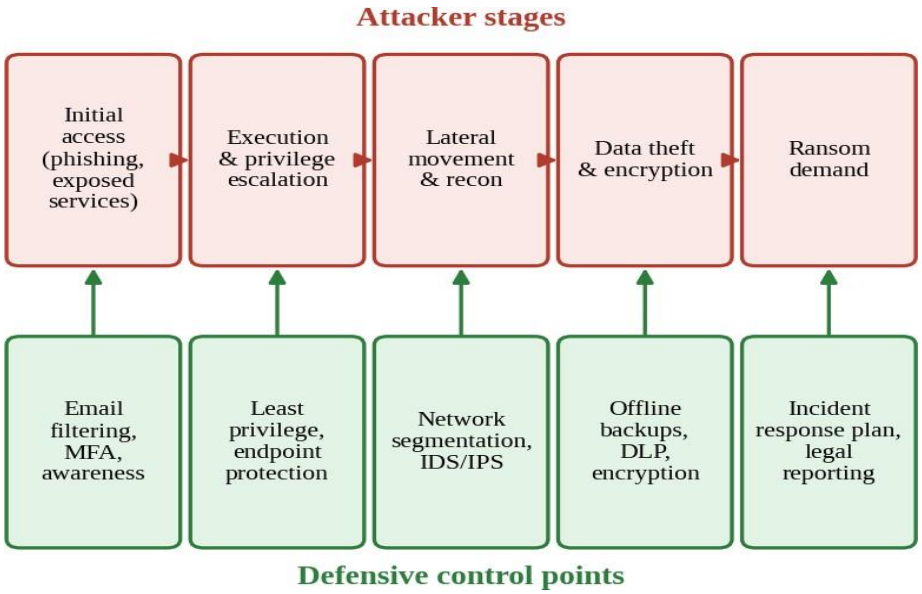


Fig. 2: Typical ransomware attack stages (top) and the defensive controls that can interrupt each stage (bottom).

E. Denial-of-Service Attacks

A DoS attack tries to make a service unavailable by exhausting its bandwidth, connection tables, or application resources. When the traffic comes from many compromised machines, usually a botnet, the attack is distributed (DDoS) and much harder to filter. Mirkovic and Reiher offer an early taxonomy that is still widely used for classifying both attacks and defenses[13]. The 2016 Mirai botnet, built from poorly secured IoT devices that still used default passwords, showed how easily large botnets can be assembled[26]. Zargar *et al.* divide flooding attacks into volumetric, protocol-based, and application-layer types, and note that defenses must be placed at several points, from the victim's network to the upstream provider[14]. Application-layer floods are especially troublesome because each request looks legitimate when examined alone.

F. Advanced Persistent Threats

An APT is a long-running, targeted intrusion, usually carried out by well-resourced groups, that aims to stay hidden while collecting information or preparing disruption[15]. The campaign typically moves through reconnaissance, initial compromise, establishing persistence, privilege escalation, lateral movement, and data exfiltration, which maps closely onto

the kill chain model[20]. Because APT operators use custom tools, stolen credentials, and legitimate administrative utilities, signature-based tools often miss them. Surveys note that no single technique covers every stage of an APT, which is one reason detection remains an open problem[16,27]. Detection therefore depends on correlating weak signals over time, such as unusual logins, odd data transfers, and small configuration changes.

Threat	Main mechanism	Typical impact
Phishing	Social engineering via email, SMS, voice, or fake sites	Credential theft, fraud, entry point for malware
Malware	Malicious code delivered through downloads, attachments, or updates	Data theft, system damage, remote control
Ransomware	Encrypts files and often steals data for extortion	Downtime, ransom payments, data exposure
Virus	Self-replicating code attached to host files	File corruption, spread through shared media
DoS / DDoS	Floods bandwidth, connections, or application resources	Service outage, lost revenue
APT	Stealthy, multi-stage, targeted intrusion	Long-term espionage, large-scale data loss

Table no 1: Comparison of Major Cyber Threats

IV. IMPACTS ON ORGANIZATIONS AND SOCIETY

A. Financial Impact

Direct costs include incident response, forensic investigation, system restoration, legal fees, and in some cases ransom payments. Indirect costs are usually larger and harder to measure: lost business during downtime, customer churn, higher insurance premiums, and regulatory penalties. A widely cited industry study put the global average cost of a data breach at about USD 4.88 million in 2024[22]. Smaller organizations may not survive an incident of that size, even though their absolute losses are lower.

B. Operational and Infrastructure Impact

When a hospital, utility, school, or logistics firm loses access to its systems, the harm goes well beyond money. Clinics may divert patients, schools may lose records and teaching time, and supply chains may stall. Attacks on critical infrastructure are especially serious because many services depend on one another, so a failure in one sector can spread to others[1].

C. Privacy, Legal, and Social Impact

Breaches expose personal data that can later be used for identity theft, targeted fraud, and harassment, and the damage to an individual can last for years. Public trust in digital services also suffers each time a major breach is reported. Data protection laws such as the EU General Data Protection Regulation[28] and India's Digital Personal Data Protection Act, 2023[29] now place explicit duties on organizations to protect personal data and to report breaches, which turns weak security into a legal as well as a technical risk.

D. Lessons from Notable Incidents

A handful of widely reported incidents illustrate how the threats in Section III play out in practice and why single controls fall short. Table no 2 summarizes them. The recurring lesson is that most of these events succeeded through ordinary weaknesses, such as an unpatched system, an unsecured device, or a trusted supplier, instead of through exotic techniques.

Incident	Year	Threat type	Key lesson
WannaCry	2017	Ransomware worm	Unpatched file-sharing flaw allowed rapid spread[23]
NotPetya	2017	Destructive malware	A compromised software update can reach many victims at once
Mirai	2016	DDoS botnet	Default passwords on IoT devices fuel large floods[26]
SolarWinds	2020	Supply-chain APT	Trusted vendors can become the path into well-defended networks[30]
Colonial Pipeline	2021	Ransomware	IT compromise can force shutdown of operational services[24]

Table no 2: Selected Notable Cyber Incidents

V. PREVENTION TECHNIQUES

No single control stops every attack, so prevention is best understood as a set of complementary measures. The following subsections describe the techniques most often recommended in the literature and in standards.

A. Firewalls

A firewall filters traffic between network zones according to rules based on addresses, ports, protocols, and, in newer products, applications and user identity. Firewalls are the first line of network defense and are effective at blocking

unsolicited inbound connections and at separating sensitive segments from the rest of the network[4]. Official guidance stresses that firewall policy must be documented, reviewed, and kept as restrictive as practical[31]. Their weakness is that they can only judge what they can see: traffic allowed by policy, encrypted content, or an attacker already inside the perimeter is largely outside their view.

B. Intrusion Detection and Prevention Systems

An intrusion detection system (IDS) monitors network or host activity and raises alerts, while an intrusion prevention system (IPS) can also block suspicious activity automatically. Detection is either signature-based, which is accurate for known attacks but blind to new ones, or anomaly-based, which can reveal novel behavior but produces more false positives[17,19]. Machine-learning methods are increasingly used to improve anomaly detection[18], and NIST guidance recommends planning for tuning, placement, and alert handling before deployment[32]. Tuning and staffing matter as much as the product itself, since an unread alert provides no protection.

C. Encryption

Encryption protects the confidentiality and, when combined with integrity checks, the authenticity of data at rest and in transit. Modern symmetric ciphers and public-key protocols are mature and efficient[4]. Encryption does not stop an attack by itself, however: if the keys are poorly managed, or an attacker steals valid credentials, the protection can be bypassed. It also limits network inspection, so organizations must plan where traffic is decrypted and monitored.

D. Multi-Factor Authentication

Multi-factor authentication (MFA) asks for two or more independent proofs of identity, such as a password plus a hardware token or a one-time code. This blunts credential theft because a stolen password alone is no longer enough[33]. Comparative studies also show that passwords remain hard to replace because alternatives usually lose on deployability[34], which is why MFA is often added on top of them. Not all factors are equally strong: codes sent by text message can be intercepted or socially engineered[35], whereas phishing-resistant authenticators based on public-key cryptography give better assurance. Usability and rollout cost remain the main obstacles.

E. Patch Management

Many successful attacks use vulnerabilities for which a fix already existed, as the WannaCry case showed. A disciplined patch management process inventories assets, ranks vulnerabilities by risk, tests updates, and deploys them within a defined time frame. In practice, legacy systems, operational downtime, and compatibility concerns slow the process, so compensating controls such as network isolation are often needed while patches are pending[36].

F. Security Awareness Training

Since phishing and other social engineering target people, training is a core control rather than an optional extra. Effective programs are short, repeated, and tied to realistic scenarios such as simulated phishing exercises, and they give staff an easy way to report suspicious messages. Studies of embedded training, in which a user is taught right after falling for a simulated phish, report better retention than static reading material[37]. Training reduces risk but cannot remove it, so it should be combined with technical filters and with a culture in which reporting a mistake is encouraged instead of punished.

G. Backup, Response, and Recovery

Offline or immutable backups, tested restoration procedures, and a rehearsed incident response plan limit the damage when prevention fails. The NIST framework treats response and recovery as first-class functions alongside protection and detection[3], and detailed incident-handling guidance is available for building a response capability[38]. These measures matter most against ransomware, where a clean and recent backup can make the difference between a short disruption and a prolonged crisis.

Technique	Advantages	Limitations
Firewall	Simple, mature; blocks unsolicited traffic; segments networks	Blind to encrypted or insider traffic; rules need upkeep
IDS / IPS	Detects known and unusual activity; IPS can block in real time	False positives; signature gaps; needs skilled analysts
Encryption	Protects data at rest and in transit; supports compliance	Key management burden; does not stop credential misuse
MFA	Neutralizes most password theft; widely supported	Weak factors can be bypassed; user friction
Patching	Removes known vulnerabilities at the source	Legacy systems; downtime; testing effort
Training	Low cost; addresses the human factor	Effect fades over time; cannot be the only control
Backup & IR	Enables recovery; limits ransomware leverage	Does not prevent data theft; needs regular testing

Table no 3: Advantages and Limitations of Prevention Techniques

These controls become far more effective when they are layered. Defense in depth places independent barriers between an attacker and the asset, so that a failure at one layer is caught by the next, an idea that traces back to classic design principles such as least privilege and fail-safe defaults[39]. Fig. 3 shows one way to arrange the controls discussed above, moving from organizational policy at the outside to the data itself at the core.

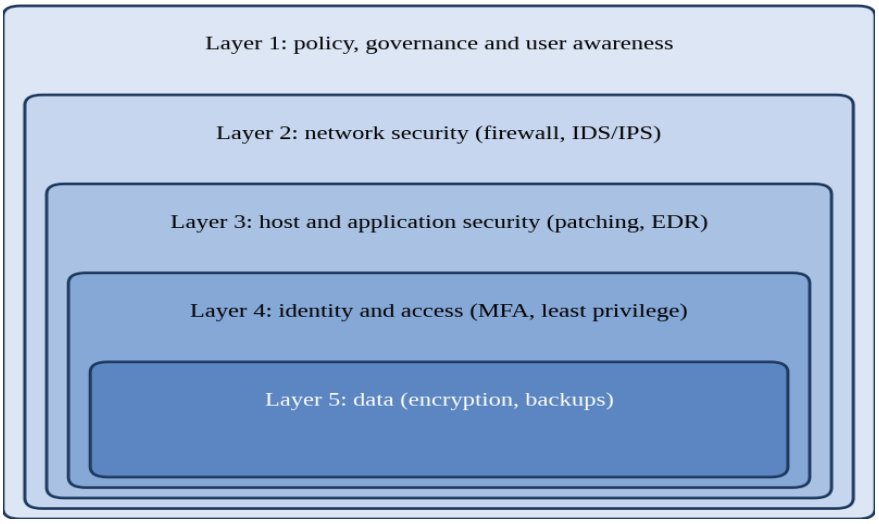


Fig. 3: Defense-in-depth model: independent control layers from policy and awareness (outer) to data protection (inner).

VI. COMPARATIVE ANALYSIS AND CHALLEGES

A. Mapping Controls to Threats

Table no 4 maps each control to the threats discussed earlier using a qualitative rating (H = strong, M = partial, L = limited) that reflects the literature reviewed here rather than a measured benchmark. The pattern is informative. No row is strong across every column, and no threat is fully covered by a single control. Phishing is best countered by a combination of training and MFA, ransomware by patching together with tested backups, and APTs by monitoring supported by segmentation and strict access control.

Control	Phish.	Malw.	Ransom.	DoS	APT
Firewall	L	M	M	M	M
IDS / IPS	L	H	M	H	M
Encryption	L	L	M	L	M
MFA	H	M	M	L	H
Patching	L	H	H	M	H
Training	H	M	M	L	M
Backup & IR	L	M	H	M	M

Table no 4: Qualitative Effectiveness of Controls Against Threats

B. Technical Challenges

Attackers adapt faster than defenders can update rules. Zero-day vulnerabilities, encrypted traffic, cloud and mobile environments, and the growing number of poorly secured Internet of Things devices all enlarge the attack surface and blur the old network perimeter. Machine-learning-based detectors bring their own weakness, because inputs can be crafted to evade them[40]. Detection tools must also balance sensitivity against alert fatigue, since too many false positives lead analysts to ignore real warnings[17].

C. Human and Organizational Challenges

Security measures that are hard to use tend to be bypassed. Staff who are asked to remember complex passwords, approve frequent prompts, and complete long training modules may look for shortcuts. Organizations also face limited budgets, a shortage of skilled security professionals, and dependence on third-party suppliers whose security they cannot directly control. Security is also an economic problem: the party that could prevent a loss is often not the one who bears its cost, which weakens the incentive to invest[41]. Small and medium-sized organizations are particularly exposed because they hold valuable data but lack dedicated security teams.

D. Regulatory and Compliance Challenges

Regulations differ across countries, and organizations that operate internationally must meet several breach-notification and data-protection regimes at once[28,29]. Compliance is necessary but not sufficient: an organization can satisfy a checklist and still be vulnerable, so frameworks should be used as a basis for continuous risk management rather than a one-time audit[3].

VII.FUTURE DIRECTIONS

Several developments are likely to shape the next stage of cyber defense. First, zero-trust architecture drops the assumption that anything inside the network is trustworthy and instead verifies every request based on identity, device state, and context[42]. Second, machine learning is being applied to detection tasks such as spotting phishing, classifying malware, and finding anomalies in network traffic. These models can raise detection rates, but they need good training data, regular retraining, and protection against adversarial manipulation[40]. The same technology also helps attackers write more convincing phishing messages, which raises the importance of phishing-resistant authentication. Third, advances in quantum computing threaten widely used public-key algorithms, and standards bodies have begun publishing post-quantum cryptographic standards[43], so organizations should start inventorying their cryptographic dependencies now. Finally, closer information sharing between organizations and with national agencies can shorten the time between the first sighting of a new technique and the deployment of defenses.

VIII.CONCLUSION

This paper reviewed the main cyber threats of the digital era—phishing, malware, ransomware, viruses, DoS attacks, and APTs—and the techniques used to prevent them. The comparison shows that every control has blind spots and that every threat can find a gap in a single-layer defense. The most dependable approach is therefore a layered one that combines technical safeguards, well-maintained systems, tested recovery plans, and a security-aware workforce, all governed by continuous risk management. Future work could complement this qualitative review with empirical evaluation, for example by measuring how combinations of controls perform against recorded attack scenarios, and by studying the effect of AI-assisted attacks and defenses on the comparisons made here.

REFERENCES

1. European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2024," Sep. 2024.
2. M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," Arab. J. Sci.Eng., vol. 45, pp. 3171–3189, 2020.
3. National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Feb. 2024.
4. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Boston, MA, USA: Pearson, 2017.
5. R. von Solms and J. van Niekerk, "From information security to cyber security," Comput. Secur., vol. 38, pp. 97–102, Oct. 2013.
6. Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," Front. Comput. Sci., vol. 3, Art. no.563060, Mar. 2021.
7. B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: State of the art and future challenges," Neural Comput. Appl., vol. 28, no. 12, pp. 3629–3654, 2017.
8. K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," J. Inf. Secur. Appl., vol. 22, pp. 113–122, Jun. 2015.
9. N. Idika and A. P. Mathur, "A survey of malware detection techniques," Dept. Comput. Sci., Purdue Univ., West Lafayette, IN, USA, Tech. Rep., Feb. 2007.
10. M. Egele, T. Scholte, E. Kirda, and C. Kruegel, "A survey on automated dynamic malware-analysis techniques and tools," ACM Comput. Surv., vol. 44, no. 2, Art. no. 6, Feb. 2012.
11. A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the Gordian knot: A look under the hood of ransomware attacks," in Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA). Cham, Switzerland: Springer, 2015, pp. 3–24.
12. H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A survey on ransomware: Evolution, taxonomy, and defense solutions," ACM Comput. Surv., vol. 54, no. 11s, Art. no. 238, 2022.
13. J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39–53, Apr. 2004.
14. S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE Commun.Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, 4th Quart. 2013.
15. A. K. Sood and R. J. Enbody, "Targeted cyberattacks: A superset of advanced persistent threats," IEEE Security & Privacy, vol. 11, no. 1, pp. 54–61, Jan./Feb. 2013.
16. A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1851–1877, 2nd Quart. 2019.
17. H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," J. Netw. Comput. Appl., vol. 36, no. 1, pp.16–24, Jan. 2013.
18. A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2nd Quart. 2016.
19. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," Cybersecurity, vol. 2, Art. no. 20, 2019.
20. E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Leading Issues in Information Warfare & Security Research, vol. 1, no. 1, p. 80, 2011.
21. Verizon, "2024 Data Breach Investigations Report," Verizon Business, 2024.
22. IBM Security, "Cost of a Data Breach Report 2024," IBM Corp., Armonk, NY, USA, 2024.
23. M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms," J. Telecommun. Inf. Technol., no. 1, pp. 113–124, 2019.
24. Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation, "Alert (AA21-131A): DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks," May 2021.
25. F. Cohen, "Computer viruses: Theory and experiments," Comput. Secur., vol. 6, no. 1, pp. 22–35, Feb. 1987.
26. M. Antonakakis et al., "Understanding the Mirai botnet," in Proc. 26th USENIX Secur. Symp., Vancouver, BC, Canada, 2017, pp.

1093–1110.
27. N. Virvilis and D. Gritzalis, "The big four—What we did wrong in advanced persistent threat detection?," in Proc. Int. Conf. Availability, Reliab. Secur. (ARES), Regensburg, Germany, 2013, pp. 248–254.
28. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), Official J. Eur. Union, L 119, Apr.2016.
29. Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, Government of India, Aug. 2023.
30. Cybersecurity and Infrastructure Security Agency (CISA), "Alert (AA20-352A): Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations," Dec. 2020.
31. K. Scarfone and P. Hoffman, "Guidelines on firewalls and firewall policy," NIST Special Publication 800-41 Rev. 1, Sep. 2009.
32. K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," NIST Special Publication 800-94, Feb. 2007.
33. P. A. Grassi et al., "Digital identity guidelines: Authentication and lifecycle management," NIST Special Publication 800-63B, Jun. 2017.
34. J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Proc. IEEE Symp. Secur. Privacy (SP), San Francisco, CA, USA, 2012, pp. 553–567.
35. A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi, "On the (in)security of mobile two-factor authentication," in Financial Cryptography and Data Security (FC), LNCS, vol. 8437. Berlin, Germany: Springer, 2014, pp. 365–383.
36. M. Souppaya and K. Scarfone, "Guide to enterprise patch management technologies," NIST Special Publication 800-40 Rev. 3, Jul. 2013.
37. P. Kumaraguru et al., "Protecting people from phishing: The design and evaluation of an embedded training email system," in Proc. SIGCHI Conf.Human Factors Comput. Syst. (CHI), San Jose, CA, USA, 2007, pp. 905–914.
38. P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," NIST Special Publication 800-61 Rev. 2, Aug. 2012.
39. J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," Proc. IEEE, vol. 63, no. 9, pp. 1278–1308, Sep. 1975.
40. B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," Pattern Recognit., vol. 84, pp. 317–331, Dec. 2018.
41. R. Anderson, "Why information security is hard—An economic perspective," in Proc. 17th Annu. Comput. Secur. Appl. Conf. (ACSAC), New Orleans, LA, USA, 2001, pp. 358–365.
42. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," NIST Special Publication 800-207, Aug. 2020.
43. National Institute of Standards and Technology, "Module-lattice-based key-encapsulation mechanism standard," FIPS 203, Aug. 2024.