Educational Administration: Theory and Practice
2025, 31(2), 232-238
ISSN: 2148-2403
https://kuey.net/

Review Article

Cyber property theft: protecting digital assets

Anup Kumar Patra[1*], Basant Kumar Behera[2], Pragyan paramita Priyadarshini[3]

[1*,2,3]college of pharmaceutical sciences, puri.

Citation: Anup Kumar Patra, et.al (2025). Cyber property theft: protecting digital assets, *Educational Administration: Theory and Practice*, 31(2) 232-238
Doi: 10.53555/kuey.v31i2.10553

ARTICLE INFO **ABSTRACT**

The spreading of the digital technologies has changed the contemporary economy, and the notion of ownership. Data, intellectual property and digital records are some of the most valuable assets that individuals, corporations and governments hold in the age of a very interconnected world. But with the increase in the digital ecosystem, the level of cyber property theft also increases on these assets. The unauthorized collection or manipulation of information, which characterizes this phenomenon, presents a serious danger to economic stability, organization security, and national sovereignty. The sophistication of online crimes, the anonymity that comes with the sophisticated technologies and the insufficiency of international law makes it an uphill task to guard against such theft. The current paper analyses the essence of cyber property theft, defines the core issues of the digital asset protection, critically analyses the drawbacks of the present protection methods. Considering the technical, legal, organizational, and geopolitical aspects, the review shows the urgency of the development of all-embracing, synchronized, and future-ready solutions to guarantee the integrity of the digital property in the 21 st century.

1. Introduction to Cyber Property Theft

In the era of the digital age, the issue of cyber property theft has become widely spread. As data and intellectual property have come to have an outsize influence in signaling organizational value, and as an organization most commonly foregoes tangible assets in favor of these data and intellectual property, the stakes have astronomically increased in terms of the willingness to defend these assets. Cyber theft deals with unlawfully entering, taking out, changing, or dropping digital assets. As opposed to physical crimes, which have geographical and physical limits, cyber theft takes advantage of the infinite and speedy cyber-world, which in most cases turns out to be extremely difficult to trace and trace.

With the arrival of new and advanced threats, including a vast network of single hackers to state-sponsored cyber units, the level of such theft is becoming more and more intense and intricate. Companies have been robbed of millions of dollars in the form of proprietary algorithms, source code and strategic business plans. Through the data breach, governments have detected breaches that undermine national security. This has at the individual level resulted in huge losses of money and emotional torment due to stolen identities and personal information.

The reasons why people may steal cyber property are also rather various: e. g. profit, competitive edge, political destabilization, or an ideological attack. Such overlap of interests confirms the need of an interdisciplinary, multi-layered response. It is not a technological problem alone but it is rather a legal, ethical, organizational and strategic problem. The emergence of remote work, cloud services and mobile technologies has contributed to the weaknesses of digital infrastructures only further. The presented introduction preconditions the further, more detailed evaluation of the challenges and barriers to the protection of digital assets in the subsequent sections.

2. The Nature and Scope of Digital Assets

Digital assets Digital assets are any information or other intellectual creation that holds some value in electronic form. Such are but not exhaustive, personal data, business records, digital communications, financial data, software, and intellectual property stored on cloud. Digital assets are trade secrets, customer databases and marketing strategies in the corporate world. They are subjected to government organisations that comprise secrets of intelligence reports, biometric data, and diplomatic relay.

Digital assets are presently enjoying a phenomenal expansion, attributed to progress in big data, artificially intelligent, and digital finance. The current cyber environment has seen the entire business model and the operations of a state rely on digital infrastructures, making it very lucrative to cybercriminals. These assets are intangible thus their ownership is more difficult to define and safe guard. You can make copies of a source code and not affect the original and customers data may be duplicated, sold and shapes up without the consent of a proprietor.

The decentralized and digital nature of these assets makes governing such assets to be cumbersome. The backups are maintained on two or more different servers in various jurisdictions around the world which adds to the flaws in the protective measures since these records are then in conflicting territories. This has caused the fact that despite having a robust local security system even then the attack can be carried out by foreign organizations using the loopholes in the law.

The growing numbers and speed of digital data additionally stress the normative models of asset management. Companies cannot find an effective way of cataloguing, monitoring, and securing the number of digital property that they produce. The fuzziness of the boundaries of the assets and the increased integration of information in day-to-day activities makes the threat environment difficult to characterize and to manage. The increase in complexity forms the basis of the changing methods used in cyber theft.

Common Cyber Property Theft Methods and Their Key Characteristics

Attack Vector	Description	Typical Target	Detection Difficulty	Example Incident
Phishing	Deceptive emails or messages to trick users into revealing credentials	Individuals, Small Businesses	Low–Medium	Google Docs Phishing Scam (2020)
Ransomware	Malware that encrypts data and demands payment	Hospitals, Corporations	Medium–High	WannaCry (2017)
Advanced Persistent Threats	Stealthy, long-term network infiltration for data exfiltration	Government, Critical Infra	High	SolarWinds Attack (2020)
Man-in-the-Middle (MITM)	Eavesdropping on or altering communications between two parties	Financial Institutions	Medium	Equifax Breach Vector (2017)
Insider Threats	Employees or contractors misusing access to steal digital assets	All Sectors	High	Snowden NSA Leak (2013)

3. Evolving Techniques of Cyber Theft

The methodologies employed in stealing of cyber property have also changed with times as technology has improved. Attackers used to depend on simple viruses and unethical hacking facilities in older times. Nowadays, though, cybercriminals are using a vast number of various innovative tactics that capitalise on technical vulnerabilities or human behaviour. The common methods used nowadays to access a secure system and extract digital wealth are phishing, social engineering, ransomware, insider manipulation, and advanced persistent threats (APTs).

Phishing has become one of the weapons in the repertoire of a cybercriminal. Attackers appear using the alias of the trusted parties and lure the users to sharing of credentials or downloading malicious attachments. Spear-phishing attacks are against a particular user in an organization, particularly those with high-level access to sensitive information. When credentials are infiltrated, the attacker can traverse on networks laterally to obtain and steal intellectual property or monetary information.

Ransomware attacks have also been on the increase and have become very complex. During such attacks, information is encrypted and used as ransom unless a payment, usually in cryptocurrencies that cannot be followed, is given. In addition to missing out on money, ransomware cases frequently generate damage to reputation and system paralysis. The demonstration of ransomware jeopardizing the security of a nation by recent attacks on critical infrastructure and healthcare facilities has indicated that the most important institutions can be at stake.

Advanced persistent threats are especially problematic in that they entail persistent and intrusive attack by other well-funded malicious parties. Such assaults can usually be arranged by state-bankrolled teams that aim to grab military designs, secret research, or diplomatic communications. APTs are so hard to uproot since they work behind the scenes and collect the intelligence in the span of weeks or months without tampering with the functions of the system.

The other emerging method is the use of zero-day vuln: these are software bugs that have not been publicised and so far, very few people have the opportunity to exploit them; these vulnerabilities are attacked before manufacturers can publish a patch. Malicious users use these to access the systems without the actual owners knowledge which in most cases is contrary to the conventional security controls.

The other threats in the past few years would be deepfakes and AI-produced impersonation. These tools are applied in order to evade identity checks or to mislead employees into allowing them access. As the distinction between human and machine generated interaction gets more and more blurry it gets harder to identify such deception.

In general, the development of higher complexity in cyber theft methodologies indicates that the threat is dynamic. The fact that attackers engage in continuous innovations is making security professionals work extra hard to ensure that they also innovate on their defense strategies.

4. Legal and Jurisdictional Complexities

One of the most complicated issues in cyber activity security related to digital assets is its legal aspect of cyber theft of property. Crimes involving cross-border actions, actors who remain anonymous, and crimes taking place in virtual worlds do not suit well in the traditional system of legal interpretation. The transnational character of cyber crime makes it difficult to conduct investigations, prosecute and prevent cyber theft of property.

Especially problematical are jurisdictional factors. Cyberattack could start in one country, target another entity and move through servers in a number of intervening countries. This raises the question on the law to be applied, whose country has the jurisdiction to prosecute becomes flight of a legal conundrum. This kind of fragmentation is often used to the advantage of attackers as they are backed with the knowledge of the slow, irregular, and politically restrained process of different law enforcers to coordinate over and between jurisdictions.

Not many countries have a cybercrime comprehensive law. In parts, laws that govern digital theft only cover old forms and are not inclusive of the advanced nature of modern threats. In those cases where laws already exist, their application remains impaired due to a shortage of technical know-how, a lack of international cooperation and the inability to access the required digital evidence. The lack of international laws enables the cybercriminals to do it in a jurisdiction that has permissive laws or jurisdiction that has weak enforcement of law.

Initiatives like the Budapest Convention on Cybercrime have at least tried to form a common framework of law, however, its inclusion is small and the means of enforcement is feeble. Mutual legal assistance treaties (MLATs) that allow one country to share evidence with another country to respond to the evidence legally are response processes that are not quick enough to keep up with the furious pace of a cyberattack. Additionally, state machinations could also be construed as being in the way of taking any legal action in case of an attack engineered by a state.

Other aspect of the legal challenge is attribution. The absence of proof of any particular attack on a particular actor or entity makes the construction of any legal argument and pursuing diplomatic action almost impossible. The task of establishing culpability becomes more difficult due to cybercriminals using anonymizing technologies and proxy servers as well as false flags to mask their location.

As well as with criminal law, right of civil liability in cases of information breach and theft is not well formed in accordance with many jurisdictions. The victims will find it hard to claim compensation since it is hard to single out perpetrators and establish the damage. In general, the issues of laws and jurisdiction can be defined as a significant international restriction in the war on cyber property theft.

5. Technological issues to the protection of the digital property

Although cybersecurity tools and processes have multiplied, a number of technological constraints still pose a challenge to the successful protection of digital assets. Technological development is usually ahead of the ability of organizations to take up related security practices. Vulnerabilities are new devices, platforms, and software applications that can be exploited even before they are developed and identified by the developers and cybersecurity teams.

The legacy system is a potential danger to most organizations, more so, to those with large decentralized IT infrastructure. Such old systems are not likely to be updated on a regular basis or not able to work with modern security standards, being prone to attack. Legacy infrastructure combined with newer technologies is known to produce complex and inconsistent network security, which is likely to result in breaches.

The unavailability of end-to-end encryption and secure data transfer protocol in most applications is another critical one. Data might not be safe even when stored in an encrypted form, as it can be affected when transferred or as it passes through the memory. These holes can be used by the attackers to read or modify information without being detected.

Firewalls, intrusion detection systems, and antivirus programs are some cybersecurity measures against them; they tend to be reactive. They are based on the known signature or behavior as the malicious activity detection method, which is ineffective against new or polymorphic attacks. The use of zero-day vulnerabilities, prior to any patch being issued by developers, forms a major vulnerability particularly with commonly used commercial software.

Cloud computing has brought in new complexities. Although cloud services provide scalability and flexibility, they are the cloud services that present the shared responsibility models where the service provider and the clients need to cooperate when it comes to managing security. Materal misconfiguration of cloud such as a cloud, visibility of vendor systems, and accountability can be performed.

Moreover, due to the proliferation of the Internet of Things (IoT), billions of connected devices create insurmountable vulnerability. Most of them do not have adequate security measures and cannot be updated remotely; hence they are long-term vulnerabilities in a network.

Machine learning and artificial intelligence are being applied more and more to boost cybersecurity and are also being used by the attackers to create automatic attacks and to evade detection. Technological arms race between the defenders and attackers keeps growing stronger, which indicates the inability of the dependence of technology alone without the support of other means, legal, organizational, and human aspects.

6. Human and Organizational Constrains

Human and organizational factors also endow much to the exposure of the digital assets. The advanced technological infrastructure can lose its power even with a great cybersecurity culture and well-trained staff members. The weaknesses that leave chances of cyber theft of property within a firm include human error, ignorance, poor managerial judgments made, and misuse of resources.

The likelihood to get attacked by social engineering can be dubbed as one of the most widespread limits of humanity. Psychological manipulation is an exploitation tool used by criminals to fool people into opening doors or leaking confidential information. Innocent users can open dangerous links, infected attachments, or divulge sensitive passwords, thus getting a back door to internal networks. This sort of offense is usually detected after immense damage has been caused.

Most companies are also not investing enough on cybersecurity trainings. In the absence of routine and continuously renewed awareness sessions, staff members will be unprepared and thus unable to identify and counter new threats successfully. High turnover rates also worsen this problem as newly hired employees are barely introduced to the security measures of the institution.

The next important factor is the incongruency between executive leadership and IT security staff. Cybersecurity in most organizations is regarded as a technical problem as opposed to a strategic one. This contributes to poor funding of security projects, low maintenance of important systems in a timely manner as well as weak involvement of senior managers in incident response preparation. Lack of leadership investment into a security proactive culture will sabotage the processes leading towards implementing a proactive security culture.

Also, through most organizations, IT ecosystems are fragmented and no single person is responsible. During decentralized activities or when a company goes through quick digital change, it is not easy to have a standard policy followed throughout various sections. Monitoring is made more difficult and exposure heightened by Shadow IT which refers to the utilisation of unapproved software or equipment by workers.

7. Sector-Specific Vulnerabilities

Although the risk of cyber property theft is universal, some sectors are overweighted as the result of the character of data they work with, their dependence on infrastructure, and the economic or strategic relevance of the digital assets to be stolen. Such industry-specific weaknesses emphasize the importance of customized cybersecurity measures, which consider the peculiarities of a given industry.

The large quantity of sensitive information and digital activity on a continuous basis put banks, insurance companies, as well as fintech firms under repeated attacks. Hackers want to get access to customer base, transaction log and payment gateway. Identity (identity theft), digital skimming, and ransomware incurs massive losses on financial investment and creates mistrust among consumers. In addition, financial organizations are growingly connected with external suppliers, which broadens their attack surface and makes managing incidents challenging.

The healthcare industry is another area which is extremely susceptible especially because their patient files are confidential and their services cannot be interrupted. Hospitals have also become vulnerable to attacks on medical devices that are connected to hospital networks because they are usually not designed with security in mind. Hacking of hospitals may postpone treatment, jeopardize diagnoses, and even take lives in the worst case. COVID-19 also revealed the vulnerabilities as a significant growth occurred in ransomware attacks: medical organizations were targeted more than any other sector of the economy.

The combination of (OT) and (IT) in manufacturing and industrial sectors has brought in new focal points of risk. Most of the industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems are old fashioned and with dated security capabilities. An effective attack would threaten to interrupt production lines, break equipment and/or lead to theft of intellectual properties. There are certain sectors that are prone to loss of trade-secrets like the aerospace industry, the defense sector and auto manufacturing industries.

The threats associated with government and defense sectors do not confine to losing money only but relate to national security. uma actors with espionage motives often come to diplomatic communications, military research and key facilities. When such data are stolen or tampered with, it may entail geopolitical ramifications, particularly when the nations are acted upon either as the initiators or as the inactive collaborators.

Learning institutions, and especially research universities, are becoming new targets given the fact that they produce able intellectual property. Some of the most common data targeted by hackers are the research work, patent and funding information. Academic networks that are predicted to increase collaboration by being open-access tend to sacrifice the level of security features.

The presence of these diverse vulnerabilities increases the reasons why industry best practices have to be embraced. A one-fit all solution to cybersecurity is insufficient rather, each industry should evaluate its individual threats and devise its own framework in response to technical as well as contextual threats.There should be proper plans on how to respond to incidents as there are either insufficient or non-existent plans in place. Organizations might not have an effective procedure of containment, communication or recovery when there is a cyber theft case. Such unpreparedness causes latent response, loss of data, and damage to reputation.

In addition, insider threats are likely to come as a result of malicious intent or accident, which is equally hard to tackle. Workers who have contact with sensitive information can be malicious or fall victims of outside forces. Such situations cannot be handled with traditional perimeter defenses, and they also require some form of shift to behavior-based monitoring and least-privilege access models.

8. International Work and Policy Lapses

The international community has come up to the point of having its own way of recognizing that stealing of property through cyberspace has become a global issue that has raised an urgency to come up with a number of initiatives to come up with cooperative security systems. Nevertheless, thus far, the international response to the protection of digital assets remains impeded by serious policy gaps and the absence of coordinated mechanisms of enforcement. Such difficulties are caused by the divergence between the national cybersecurity posture, legal frameworks, political agenda, and technological capacity.

Some of the popular international initiatives include the Budapest Convention on Cybercrime, the initial effort by the international community to ensure reduction in crime through harmonization of national legislations, bettering investigation methods and enhancing collaboration between international jurisdictions. On the one hand, it establishes a certain structural framework; on the other hand, its acceptability is hampered due to the absence of key stakeholders as its signatories (like Russia and China). Their inexistence deters the possibility of a legal and operational baseline that is acceptable and agreeable in terms of prevention and response of any cyber associated crime.

The United Nations also undertook different discussions and decisions, including the setting up of open ended working group (OEWG) on progress in area of information and telecommunications in the matter of international security. Although these forums offer good discussion points, they do not bear binding results, and they fail to fill geopolitical gaps especially between the western democracies and the authoritarian regimes.

The adoption of data protection and cybersecurity laws is still in progress, and regional block such as the European Union has achieved significant progress. The GDPR provides high standards of data deployment and breach warning, which can be used as an example by other regions. Nonetheless, it is subject to variations in compliance and inability of match with non-EU systems restricting its worldwide scope.

Another aspect of global cybersecurity strategies has become the public-private partnership. Teaming of governments and technology companies has made it possible to share threat intelligence as well as create industry standards. However, these collaborations are mostly unofficial or ad hoc and have focused most efforts in few, technologically advanced countries at the exclusion of various developing countries unable to join due to the needed instruction or resources.

Such a significant policy gap is that there is no common definition and structure of digital asset protection. This means that different countries treat and categorize the issue of digital property in varying ways, making it a legal nightmare and a nightmare of enforcement. Besides, other concerns like state-sponsored cyber espionage, cyber warfare and even politicization of cyber norms also make it even more difficult to come up with solid international policies.

To be effective in combating cyber property theft on an international level, one has to abandon piecemeal methods. The critically missing elements in the establishment of an effective and fair international cyber governance regime architect are a binding and universally ratified cyber convention, better attribution frameworks as well as more participatory and encompassing capacity building processes.

9. Challenges and Limitations

However, the costs and constraints in ensuring that cyber theft of property is prevented are immense and multi faceted irrespective of corporate and state efforts put to achieve cybersecurity. Such constraints are of technical, legal, organizational, and even geopolitical characters, which is why the process of protecting digital assets is very complicated on the basis of a highly interconnected digital environment.

Among the very second challenges will be the high rates of evolution of cyber threats. Hackers keep changing their methods, in most cases, renewing them faster than the defensive tools developed by operators and the State. The ever-evolving nature of zero-day issues, polymorphic malware, and AI-enabled security threats have rendered old-fashioned reactive security paradigms more and more obsolete. Security teams often find themselves at the mercy of playing catch up, they have little time or tools to expect the next threat and eliminate it before the damage has been done.

The other key limitation is the worldwide imbalance in preparedness against cybersecurity. Technologically advanced countries might have elaborate cyber defense systems but in most developing countries, the infrastructure, policy frameworks, or even skilled deserving staff might not be in place to tackle even simple form of cyber threats. The resulting imbalance leaves a patchwork of deficiencies that can be exploited by cyber criminals, who frequently attack a target using jurisdictions where law enforcement is limited at best or non-existent.

The next serious limitation is the legal and jurisdictional fragmentation. Cyber crimes can involve two or more different countries and national laws are being largely unsynchronized and unedified in defining the crimes and prescribing punishment or enforcement. There is no enforceability in international treaties and mutual legal assistance between nations is not timely and efficient. These are made even worse by the involvement of state sponsored actors which makes them almost legal impossible or impossible to solve through diplomacy.

The gaping holes among most vulnerability concerns are the human factors committed out of error. Even the most senior members of the company, workers, and contractors are not always adequately trained to detect cases of phishing, social engineering, or online unsafe practices. Cybersecurity within most organizations is not ingrained into the main culture of operation and therefore there is laxity in the application of access controls, poor passwords, and obsolete systems.

In addition, incident response and recovery planning is also seriously lacking. A lot of organizations do not develop detailed cyber incident response plans or there is a lack of their upgrading and testing. Such lack of preparedness leads to long downtimes, loss of data, and image loss in cases of breaches.

Budget constraints are also a hindrance to smaller organizations and institutions of the state carrying out cutting edge security work. Lack of manpower and operating within budget limits together with being reliant on exploited technology makes them easy pickings of predatory hackers.On the whole, despite all awareness of cyber property theft that has arisen worldwide, current protective systems are hardly adequate in size or sophistication to defend against this mounting threat. The interventions sought should be holistic so as to close the technological, legal, human and geopolitical divide to have a more robust digital ecosystem.

Conclusion

The theft of cyber property has become one of the most ultimate threats in the digital world which targets not only individuals but also, corporations and governments as well. Due to the pace of digital transformation taking place in all industries, the quantity, worth of digital adversities, and exposure to digital adversities have similarly expanded. Currently, the existence of parties compromising the security of cyber activities (cybercriminals) is because of financial investments in security technology and international trade partnerships.

This review discussed the changing methods of cyber thefts, the jurisdictional and legal complexities involved, the technological and organizational constraints and weaknesses and the susceptibilities effectively exposed by various sectors. It has also shown us what has been done on the global front and what are the points of strides which are still lacking in the policymaking, implementation and long term planning.

What comes out clearly is that there is need to have a multidisciplinary approach to tussing with cyber property theft. Technological protection is to be combined with legal initiatives, international liaison, managerialFW, and end-user education. An effective cybersecurity model should be flexible and ever-changing as it should adapt to the new challenges. In addition, security measures also need to go beyond a country and accept the norms of the world, mutual intelligence networks and capacities, especially in those areas that are not well developed.

Finally, such a topic as digital property protection cannot be considered exclusively technical or national. It requires a unified worldwide intervention based on legal transparency, technology and moral integrity. It is only when these issues and constraints are approached in their entirety that the world at large could aspire to create a secure online world where IP, privacy and innovativeness are not threatened by the constant threat of cyber-robbery

References

1. Ahmad, A., Webb, J. C., & Desouza, K. C. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security, 86*, 402–418.
2. Alqahtani, A., & Sheldon, F. T. (2022). A survey of crypto ransomware attack detection methodologies: An evolving outlook. *Sensors, 22*(5), 1837.
3. Begovic, K., Al-Ali, A., & Malluhi, Q. (2023). Cryptographic ransomware encryption detection: Survey. *arXiv preprint arXiv:2306.12008*.

4. Bodmer, S., Kilger, M., Carpenter, G., & Jones, J. (2012). *Reverse deception: Organized cyber threat counter-exploitation*. McGraw-Hill Education.
5. Krishnapriya, S., & Singh, S. (2024). A comprehensive survey on advanced persistent threat (APT) detection techniques. *Computers, Materials & Continua, 80*(2), 2675–2719.
6. Moussaileb, R., Cuppens, N., Lanet, J.-L., & Bouder, H. L. (2021). A survey on Windows-based ransomware taxonomy and detection mechanisms. *ACM Computing Surveys, 54*(6), 1–36.
7. Muniandy, M., Ismail, N. A., Al-Nahari, A. Y. Y., & Yao, D. N. L. (2024). Evolution and impact of ransomware: Patterns, prevention, and recommendations for organizational resilience. *International Journal of Academic Research in Business and Social Sciences, 14*(1), 585–599.
8. Murray, G., Falkeling, M., & Gao, S. (2024). Trends and challenges in research into the human aspects of ransomware: A systematic mapping study. *Information and Computer Security*.
9. Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2021). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys*.
10. Pattnaik, N., Nurse, J. R. C., Turner, S., Mott, G., MacColl, J., Huesch, P., & Sullivan, J. (2023). It's more than just money: The real-world harms from ransomware attacks. *arXiv preprint arXiv:2307.02855*.
11. Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms. (2024). *Journal of Network and Computer Applications, 223*, 103809.
12. Siddiqi, M. A., Mugheri, A., & Oad, K. (2022). Advanced persistent threat defense techniques: A review. *Pakistan Journal of Computer and Information System*.
13. Springer, J. C., Roy, S., & Kamhoua, C. (2018). Tracking advanced persistent threats in critical infrastructures through opinion dynamics. In *Lecture Notes in Computer Science* (Vol. 11098, pp. 640–659). Springer.
14. Sudheer, S. (2024). Ransomware attacks and their evolving strategies: A systematic review of recent incidents. *Journal of Technology and Systems, 6*(7), 32–59.
15. United Nations Office on Drugs and Crime. (n.d.). *Module 11: Cyber-enabled intellectual property crime*. In *Cybercrime Module 3: Key Issues*. United Nations.
16. Vasoya, S., Bhavsar, K., & Patel, N. (2022). A systematic literature review on ransomware attacks. *arXiv preprint arXiv:2212.04063*.
17. Vehabovic, A., Ghani, N., Bou-Harb, E., Crichigno, J., & Yayimli, A. (2023). Ransomware detection and classification strategies. *arXiv preprint arXiv:2304.04398*.
18. Worrell, J. L. (2024). A survey of the current and emerging ransomware threat landscape. *EDPACS, 69*(2), 1–11.
19. Xiao, N., Lang, B., Wang, T., & Chen, Y. (2024). APT-MMF: An advanced persistent threat actor attribution method based on multimodal and multilevel feature fusion. *arXiv preprint arXiv:2402.12743*.
20. Zhou, Y., & Jiang, X. (2012). Dissecting Android malware: Characterization and evolution. *IEEE Symposium on Security and Privacy*, 95–109.