

15

Chapter

Impact of Cyber Security in the Digital Economy

Mampi Devi¹ & Arpan Datta Roy²

¹Assistant Professor, School of Cyber Security and Digital Forensics,
NFSU Tripura Campus, Agartala, Tripura

²Assistant Professor, School of Forensic Science,
NFSU Tripura Campus, Agartala, Tripura

Abstract

As the whole world turns into digital, so the technological devices have impacted nearly every part of our lives. The uses of these devices are growing very rapidly to simplify our day to day lives that directly proportional to the growth of Digital Economy. Resultant, exponential growth of the international economy and interconnections of global landscape. However, others side of the coin, is also being misused for these technological devices that give birth to cybercrime. Since digital technology align with business strategy so cyber security is not only the responsibility of IT department only, it also the responsibility of each individual employee to maintain the growth of Digital Economy. To resolve the issues of cybercrime Cyber forensic plays vital role in this society. This paper provides the awareness knowledge of dynamic development of digital economy and, how cybercrime effect the growth of digital economy. Moreover, this paper also discusses about the overview of different forensic investigation methodology in perspective of cyber forensic investigator which allows law enforcement, private detectives, and cyber security experts to reveal digital action after a cyber event.

Keywords: *Digital Economy, Cybercrime, Cyber Security, Cyber Awareness, Forensic Investigation Tools.*

1. Introduction

The rapid growth of digital technologies is impact on the global world, giving birth to a interlinked digital economy. So Journey from online banking to cloud computing via e-commerce using of different smart devices, change our life to modern life, Upgrading efficiency, accessibility, and economic growth. Therefore, we have been very familiar on digital systems, and resultant significant challenges in the form of cyber threats, data breaches, and privacy concerns. Consequently, cyber security and data protection have become essential priorities for individuals, organizations, and governments across the globe.

The various form of cyber crime has been rapidly growing and targeting different individual, Government and non government organization officials. Due to this crime, not only cause financial loss but also rescinded the trust on technology which directly impact on our digital economy. To resolve these issues, it is considerable to understand the different types of cyber crime, risk associated with this crime and the challenges for securing digital environment.

In this regards, cyber forensics plays a vital role such as providing the tools and methodologies required to investigate cyber incidents and uncover digital evidence. The main steps for Cyber forensic are detecting, analyzing, and responding to cybercrimes. It also supporting legal proceedings.. For this proceeding one forensic investigation team will be allotted to investigate team that is very much familiar with FSL and CFSL. Their systematic investigative procedure ensure that digital evidence is handled with integrity and can be used effectively in legal and regulatory contexts.

This paper focuses on main impacts of cybersecurity in the domain of digital economy with special focus on cybercrime and its types, challenges faced in data protection, risk assessment strategies, and the role and investigation team of cyber forensic investigators. In this research, it has been providing a brief overview of the domain, the paper aims to highlight the importance of cybersecurity awareness and forensic readiness n to ensure secure and sustainable growth of the digital economy.

A. Motivation

The reason behind this research is to analysis the dynamic relationship between cybercrime and digital economy, while special focus on the crucial role of cyber forensic investigation team to ensure the maintain of CIA (Confidentiality, Integrity and Accessability) so that trust in the digital ecosystem consistent. This paper aims to raise awareness and provides awareness of the continuous growth of the digital economy through robust forensic and cybersecurity practices.

B. Issues and Challenges

The rapid growth of the digital economy has introduced numerous cybersecurity and data protection challenges that influence individuals, governments and non government organizations. These challenges grows geometrical progress due to technological advancements and digital dependency.

1. Increasing Advancement of Cyber Attacks

Cyber threats are becoming more technicality, including ransomware attack, phishing, vishing, Advanced Persistent Threats (APTs), and zero-day attacks. Attackers are utilizing automation such as AI and social engineering techniques to bypass established security mechanisms.

2. Data Privacy and Authentication

The classification of private and sensitive data raises significant challenges. Unauthorized access, data breaches, and misuse of personal information can lead to identity theft, financial fraud, and reputational damage.

3. Lack of Digital Literacy

Human emotions is one of the weakest links in cybersecurity. Unawareness about password setting, phishing attacks, vishing attacks, digital arrests and negligence about classification of data such as handling data increase the risk of security breaches.

4. Rapid Growth of Internet of Things(IoT) and Connected Devices

The expansion of Internet of Things (IoT) devices has increases the probable of attack. Different cheap IoT devices has lack of security features, resulting vulnerable to exploitation and large-scale attacks such as botnets.

5. Deficiency of Cybersecurity Infrastructure

Many organizations, especially small and medium enterprises (SMEs) used old version of software and hardware devices, not used proper antivirus, firewall. Due to resources constraints, skilled staffs, and advanced tools to implement effective cybersecurity measures.

6. Inequality of laws and Compliance Challenges

Different countries have their different data protection laws and regulations, making complex compliance for global organizations. The digital agreement among all the countries are not same.

7. Insider Threats dishonesty and fraud

Employees within the organizations may access intentionally or unintentionally compromise data security. To detect and prevent insider threats is very challenging due to trust and access advantages.

8) Risks for Cloud Data

Now all the data we store in the cloud, cloud is very concern about data storage, access control, multi-tenancy, and third-party dependency. So there is chances of misleading data if high security is not implemented.

9. Lack of a standard policy for cyberforensic practices.

The cyberforensic investigation tool often faces challenges such as lack of standardized procedures, jurisdictional issues, and difficulties in collecting and preserving digital evidence.

10. Cross-Border Cybercrime and Jurisdiction Issues

Cybercrimes often cross national boundaries, and make investigation and prosecution challenging due to differences in legal frameworks and lack of international cooperation.

11. Emerging Technologies and Unknown Threats

Latest technology, such as artificial intelligence, blockchain, and quantum computing, introduces new vulnerabilities and unknown risks that require continuous adaptation of security strategies.

12. Cost and Resource Constraints

Implementing robust cybersecurity measures requires significant investment in technology, training, and infrastructure, which may not be feasible for all organizations.

2. Cybercrime and its Type

Cybercrime defined as a crime related to illegal activities that are carried out using computers, digital devices, or networks as a weapon or target or both. In today's digital economy, where most of the transaction happen in online with the help of technology such as banking, communication, education, and business operations are conducted online, cybercrime has emerged as a serious global concern. It not only causes financial losses but also threatens privacy, data security, and national security.

The increasing dependence on digital platforms has made individuals and organizations more vulnerable to cyber threats. One major category of cybercrime is crimes against individuals, which primarily target personal information and privacy.

These include identity theft, where attackers steal sensitive personal data for fraudulent purposes, and phishing attacks, where users are tricked into revealing confidential information through fake emails or websites. Cyberstalking and online harassment are also common, causing psychological distress to victims. Such crimes exploit human vulnerabilities and lack of awareness.

Another important category is crimes against property, which involve unauthorized access, damage, or theft of digital assets. Hacking is one of the most common forms, where attackers gain unauthorized entry into systems or networks. Malware attacks, including viruses, worms, and Trojans, are used to disrupt or damage systems. Ransomware is a growing threat that encrypts user data and demands payment for its release. Intellectual property theft, such as software piracy and illegal distribution of digital content, also falls under this category.

Cybercrimes against organizations target businesses, institutions, and government bodies, often with the aim of financial gain or operational disruption. Data breaches are a major concern, where confidential information of customers or employees is exposed. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks disrupt services by overwhelming systems with traffic. Insider threats, where employees misuse their access privileges, and corporate espionage, involving theft of sensitive business information, also pose significant risks.

Crimes against society represent a broader category that affects public order and national security. Cyber terrorism involves attacks on critical infrastructure to create fear and instability. The spread of fake news and misinformation through digital platforms can influence public opinion and create social unrest. Illegal online activities such as gambling, trafficking, and distribution of harmful content also fall under this category.

Financial cybercrimes are specifically aimed at monetary gain and have increased significantly with the rise of digital transactions. These include online banking fraud, credit and debit card fraud, e-commerce scams, and cryptocurrency-related frauds. Attackers use sophisticated techniques to exploit vulnerabilities in financial systems and deceive users into transferring money or revealing sensitive financial information.

With the advancement of technology, new and emerging forms of cybercrime are continuously evolving. These include AI-based attacks such as deepfakes and automated phishing, IoT-based attacks targeting connected devices, and cloud security breaches. Social engineering attacks, which manipulate human behavior to gain unauthorized access, are also becoming more prevalent.

In conclusion, cybercrime is a complex and rapidly growing threat in the digital age. Its diverse types affect individuals, organizations, and society at large. Understanding these categories is essential for developing effective cybersecurity measures and implementing cyber forensic techniques to detect, prevent, and investigate cyber incidents.

3. Risk Assessments in Cyber Security for Digital Growth

Risk assessment in cybersecurity is a systematic process of identifying, analyzing, and evaluating potential threats and vulnerabilities that can affect digital systems, data, and infrastructure. In the context of digital growth, where organizations increasingly rely on technology for operations, services, and innovation, risk assessment plays a crucial role in ensuring secure and sustainable development. It helps organizations understand their risk posture and implement appropriate safeguards to protect digital assets.

The first step in cybersecurity risk assessment is the identification of assets and potential threats. Assets may include sensitive data, software systems, hardware infrastructure, and network

resources. Threats can arise from various sources such as cybercriminals, insider attacks, malware, phishing, and natural disasters. Identifying these elements is essential to understand what needs protection and from whom.

The next stage involves identifying vulnerabilities within the system. Vulnerabilities are weaknesses that can be exploited by attackers, such as outdated software, weak passwords, misconfigured systems, or lack of proper security controls. Regular vulnerability assessments and penetration testing are important to detect these weaknesses before they are exploited.

Risk analysis is then conducted to determine the likelihood and impact of potential threats exploiting identified vulnerabilities. This step evaluates how severe a risk could be and how often it might occur. Risks are often categorized as low, medium, or high based on their potential impact on business operations, financial stability, and reputation.

Following analysis, risk evaluation and prioritization are carried out. Organizations prioritize risks based on their severity and focus on addressing the most critical ones first. This ensures efficient allocation of resources and timely implementation of security measures, which is particularly important for organizations undergoing rapid digital transformation.

Risk mitigation involves implementing appropriate security controls and strategies to reduce or eliminate identified risks.

These may include technical measures such as firewalls, encryption, intrusion detection systems, and multi-factor authentication, as well as administrative controls like security policies, employee training, and incident response planning.

Continuous monitoring and review are essential components of cybersecurity risk assessment. As technology evolves and new threats emerge, risks also change over time. Regular monitoring, auditing, and updating of security measures help organizations stay resilient against evolving cyber threats and ensure ongoing protection.

In the context of digital growth, effective risk assessment not only safeguards data and systems but also builds trust among users, customers, and stakeholders. It enables organizations to innovate confidently while maintaining compliance with legal and regulatory requirements. Thus, cybersecurity risk assessment is a foundational element for achieving secure and sustainable digital transformation.

4. Role of Cyber Forensic Investigator in Digital Economy

In the rapidly expanding digital economy, cyber forensic investigators play a crucial role in maintaining security, trust, and accountability across digital platforms. As businesses, financial systems, and communication networks increasingly rely on digital technologies, the occurrence of cybercrimes such as data breaches, fraud, and unauthorized access has also grown.

Cyber forensic investigators are responsible for identifying, collecting, analyzing, and preserving digital evidence to investigate such incidents and support legal proceedings.

One of the primary roles of a cyber forensic investigator is evidence collection and preservation. They ensure that digital evidence from computers, mobile devices, networks, and cloud systems is collected in a legally admissible manner without altering its integrity. Maintaining the chain of custody is essential so that the evidence can be presented in court without any challenge to its authenticity.

Another important responsibility is the analysis of digital evidence. Investigators use specialized tools and techniques to examine logs, files, network traffic, and system activities to reconstruct the sequence of events leading to a cyber incident.

This helps in identifying the source of the attack, the methods used, and the extent of the damage caused.

Cyber forensic investigators also play a key role in incident response and recovery. They work closely with cybersecurity teams to contain breaches, mitigate damage, and restore affected systems. Their findings help organizations understand vulnerabilities and prevent future attacks by improving security measures.

In the digital economy, financial transactions and online services are highly vulnerable to fraud. Cyber forensic experts assist in fraud detection and investigation by tracing illegal transactions, identifying fraudulent activities, and supporting financial institutions in resolving disputes. This helps in maintaining trust in digital financial systems.

Legal support is another significant role of cyber forensic investigators. They prepare detailed forensic reports and may act as expert witnesses in court, explaining technical findings in a clear and understandable manner. Their work assists

law enforcement agencies in prosecuting cybercriminals and ensuring justice. Furthermore, cyber forensic investigators contribute to policy development and compliance. Their insights help organizations design better security policies, adhere to regulatory requirements, and implement best practices for data protection. They also conduct awareness programs and training to educate employees about cyber threats and safe digital practices.

In conclusion, cyber forensic investigators are essential in ensuring the secure functioning of the digital economy. By uncovering cybercrimes, supporting legal processes, and strengthening cybersecurity frameworks, they help build a safe and trustworthy digital environment that supports continuous economic growth.

A. Methodology of cyber forensic Investigator

Cyber forensic investigation follows a systematic and structured methodology to ensure that digital evidence is properly identified, collected, analyzed, and presented in a legally admissible manner as shown in the figure 1.

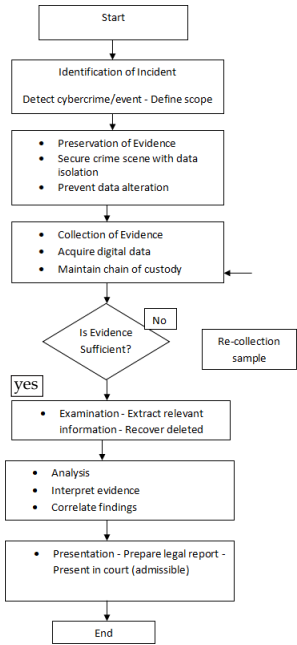


Fig. 1. Cyber Forensic Investigation Process

This process is essential for maintaining the integrity of evidence and supporting legal and organizational decision-making in the digital economy.

The first stage is identification, where the investigator determines the scope of the incident and identifies potential sources of digital evidence. These sources may include computers, mobile devices, servers, network logs, cloud storage, and other digital media. Proper identification helps in defining the objectives and direction of the investigation.

The next step is preservation, which involves securing and isolating the digital evidence to prevent any alteration, damage, or loss. Investigators create forensic copies (bit-by-bit images) of storage devices instead of working on the original data.

Maintaining the chain of custody is crucial at this stage to ensure that evidence remains authentic and admissible in court. Following preservation is the collection phase, where relevant data is acquired using specialized forensic tools and techniques. This may include extracting files, system logs, metadata, and deleted data. The process must be carried out carefully to avoid contamination or modification of evidence.

The examination phase involves processing the collected data to identify relevant information. Investigators filter, recover, and organize the data to make it suitable for analysis. Techniques such as keyword searching, file carving, and timeline reconstruction are commonly used during this phase.

Next is the analysis phase, where the investigator interprets the examined data to reconstruct events and draw conclusions. This includes identifying the attack vector, understanding the behavior of the attacker, determining the impact of the incident, and linking the evidence to specific individuals or activities.

The documentation and reporting phase is critical, as investigators prepare a detailed report outlining the procedures followed, tools used, findings, and conclusions. The report must be clear, accurate, and legally sound so that it can be understood by non-technical stakeholders such as lawyers and judges.

Finally, the presentation phase involves presenting the findings in a court of law or to organizational authorities. The investigator may act as an expert witness, explaining the evidence and methodology used during the investigation in a simple and credible manner.

In conclusion, the methodology of cyber forensic investigation ensures a structured approach to handling digital evidence. By following these steps—identification, preservation, collection, examination, analysis, documentation, and presentation—investigators can effectively uncover cyber incidents while maintaining the integrity and reliability of the evidence.

5. Conclusion and Future Direction

The digital economy has significantly transformed the way individuals, businesses, and governments operate, enabling seamless connectivity, innovation, and economic growth. However, this rapid digitalization has also increased exposure to cyber threats, making cybersecurity a fundamental pillar for sustaining trust and stability in digital systems. Effective cybersecurity measures not only protect sensitive data and critical infrastructure but also enhance user confidence, facilitate secure online transactions, and support the overall resilience of the digital ecosystem. Thus, cybersecurity is not merely a technical requirement but a strategic necessity for the sustainable development of the digital economy.

Looking forward, the future of cybersecurity in the digital economy will be shaped by emerging technologies such as artificial intelligence, blockchain, cloud computing, and the Internet of Things (IoT). There is a growing need for advanced threat detection systems, automated response mechanisms, and robust data protection frameworks to counter increasingly sophisticated cyberattacks. Additionally, strengthening international cooperation, developing adaptive regulatory policies, and promoting cybersecurity awareness and skill development will be essential. Future efforts should also focus on integrating proactive security-by-design approaches into digital infrastructures to ensure a secure, resilient, and trustworthy digital economy.

6. References

- M. T. Britz, *Computer Forensics and Cyber Crime: An Introduction*. Pearson, 2013.
- B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*. Cengage Learning, 2018.

National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, 2018. [Online]. Available: <https://www.nist.gov/cyberframework>

International Organization for Standardization (ISO), ISO/IEC 27001 Information Security Management, 2022. [Online]. Available: <https://www.iso.org/isoiec-27001-information-security.html>

European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape Report, 2023. [Online]. Available: <https://www.enisa.europa.eu>

INTERPOL, Cybercrime Report, 2023. [Online]. Available: <https://www.interpol.int>

Reserve Bank of India (RBI), Cyber Security Framework in Banks, 2023. [Online]. Available: <https://www.rbi.org.in>