International Journal of Commerce and Economics
www.commercejournal.in
Online ISSN: 2664-7540
Received: 15-05-2026, Accepted: 15-06-2026, Published: 30-06-2026
Volume 8, Issue 2, 2026, Page No. 100-102

Battling against cyber threats-the cyber security audit way

Jitendra Kumar Giri
Research Scholar, Department of Commerce and Business Administration, Lalit Narayan Mithila University, Darbhanga, Bihar, India
DOI: https://doi.org/10.66856/ijce.2026.8.2.8044

Abstract
The enormous rise of digital connectivity has resulted in a significant increase in cyber-attack events. The risk of cyber-attacks is growing as companies adopt new digital technology. The growing network complexity resulting from digital innovation typically creates new network loopholes for cyber attackers. In addition, companies affected by cybersecurity threats have long-lasting economic and reputation damage. Organizations can detect gaps in their cybersecurity infrastructure by conducting frequent cybersecurity audits. Audits may also be used by organizations to assess their compliance with various rules and legislation. Businesses can efficiently assess their safety position as their networks expand and become more complicated through an established cybersecurity audit program. We cannot deny that cybersecurity has become one of the serious challenges faced by every type of organization and society. A cybersecurity audit is a complete evaluation and analysis of the IT infrastructure of a business organisation. In protecting businesses in the ongoing battle against cyber threats, the cybersecurity audit plays a vital role.

Keywords: Compliance and audit, confidentiality of data, cyber security, internal auditor, risk management

Introduction

Cyber security is an attempt to minimising any risk of financial loss, disruption or damage to the reputation of an organisation that may arises from the failure of its information technology systems. The American Institute of Certified Public Accountants (2018) stated that "Cybersecurity is one of the top issues on the minds of management and boards in nearly every company in the world-large and small, public and private."

Cybersecurity is about more than simply technological resilience or IT security; it is also about the protection of information and data (Solms & Niekerk, 2013). The main reasons why hackers succeed are misguided assurances from the internal team or cybersecurity company and a false sense of security, they focus on your processes, people, procedures, and weakest connections.

Cybersecurity is the collection of technologies, procedures, and strategies that are intended to safeguard networks. computers, programs, and data from cyberattacks, damage, or illegal access (Haapamäki & Sihvonen, 2019). Data is becoming digitized more and more and the internet is utilized to store, access, and retrieve critical data. A research from cybersecurity Ventures forecasted that cyber-attacks would cost the global economy a shocking USD 6 trillion per year by 2021 [7]. Protecting this information is no longer a luxury, but rather a mandate for most companies and government organizations throughout the world. Thus, cybersecurity comprises the protecting information transferred over any computer network.

Cyber Security Audit -A Systematic Evaluation

A cybersecurity audit is a systematic and impartial evaluation of an organization's cybersecurity. An audit ensures adequate safety controls, policies, and procedures are implemented and operated efficiently.

Cybersecurity audits serve as a checklist for businesses to utilize when evaluating their security policies and processes. Organizations conducting an audit can check if they have the necessary safety procedures in place and ensure that they comply with the relevant requirements, or not. This enables organizations to be more vigilant when developing cybersecurity strategies and policies. To avoid conflicts of interest, cybersecurity audits are done by third-party vendors. They can also be managed by an internal team as long as they operate independently of their parent company.

A cybersecurity audit provides the greatest degree of confidence for existing cyber risk management system. It provides a new point of view for evaluating and improving security management. The following are significant advantages of IT security audits:

- Address and highlight weak areas,
- Provides a thorough internal and external security examination,
- Identify security loopholes,
- Determines whether business firms need to improve system security,
- Provides advice on how to use technology to improve corporate security,
- Keeping a step ahead of hackers,
- Better Reputation, and
- Enhanced technology and safety performance.

Objective of Cyber Security Audit

The objective of the cyber audit is to provide an assessment of the operating effectiveness of cyber security policies and procedures, identify, protect, detect, respond and recover processes and activities to the board. The Cyber audit program generally covers sub-processes such as asset management, awareness training, data security, resource planning, recover planning and communications. In order to identify internal control and regulatory deficiencies that could put the organization at risk.

The security and control issues which deals under cyber security audits includes

1. Protection of sensitive data and intellectual property
2. Protection of networks to which multiple information resource is connected
3. Responsibility and accountability for the device and information contained in it.

Scope of Cyber Security Audit

Scope of cyber security audit includes

- Data security policies relating to the network, database and applications in place,
- Data loss prevention measures deployed,
- Effective network access controls implemented,
- Detection/prevention systems deployed,
- Security controls established (physical and logical),
- Incident response program implemented.

Dimension of the Cyber Security Audit Process

Management

Management of the Company ultimately owns the risk decisions made for the organization. Therefore, it has a vested interest in ensuring that cyber security controls exist and are operating effectively. Decisions are typically made based on guidance received during the risk management processes, for taking appropriate decisions

Risk Management

Risk assessments are typically mode based on guidance by the Cyber security officer at an organization and enterprise management make decisions, employing risk management processes. The objective in any risk assessment is twofold. First, it is critical to communicate the state of the risk so that it is easy to understand and be clear on the level of risk involved. Secondly and just as significantly the ways in which to address that risk must be identified as well. This provides both problem and solution and mitigates the negative impact of that risk to on enterprise. The risk landscape is ever-changing. It is important to have defined processes, trained and competent cyber security resources, and a governance framework to ensure that appropriate actions are carried out by enterprise leadership and managed effectively to address current and emerging threats.

Internal Audit

Internal auditors and risk management professionals have key roles to play, as does enterprise management. Cyber Auditing is a security measure not an inconvenience. It is critical to protecting an enterprise in today's global digital economy. The internal audit department plays a vital role in cyber security auditing in many organizations, and often has a dotted-line reporting relationship to the audit committee to ensure an independent view is being communicated at the board level of the enterprise. Audit helps enterprises with the challenges of managing cyber threats, by providing an objective evaluation of the controls and making recommendations to improve them as well as assisting the senior management and the board of directors understand and respond to cyber risks. Organizations, especially within the public sector, also contract for the services of external auditors to provide independent assurance of the financial and operational controls primarily to ensure the controls design is effective and the needs of the organization are being met

Illustrative checkpoint on the Cyber Security Audit

Personnel Security

1. Whether the staff wears ID badges?
2. Whether it is a current picture part of the ID badge?
3. Are authorized access levels and type (employee, contractor, visitor) identified on the Badge?
4. Whether the credentials of external contractors' ore checked?
5. Whether the company has policies addressing background checks for employees and contractors?
6. Whether the Company has a process for effectively cutting off access to facilities and information systems when on employee/contractor terminates employment?

Physical Security

1. Whether the Company has policies and procedures that address allowing authorized and limiting unauthorized physical access to electronic information systems and the facilities in which they are haused?
2. Whether the Company's policies and procedures specify the methods used to control physical access to your secure areas, such as door locks, access control systems, security officers, or video monitoring?
3. Whether the access to the computing area is controlled (single point, reception or security desk, sign-in/sign-out log, temporary/visitor badges)?

Account and Password Management

1. Whether the Company has policies and standards covering electronic authentication, authorization, and access control of personnel and resources to your information systems, applications and data?
2. Whether the Company ensures that only authorized personnel have access to the computers?
3. Whether the Company requires and enforces appropriate passwords?
4. Are your passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?

Confidentiality of Data

1. Whether the Company is exercising responsibilities to protect sensitive data under their control?
2. Whether the most valuable or sensitive data encrypted?
3. Whether the Company has a policy for identifying the retention of information (both hard and soft copies)?

Compliance and Audit

1. Whether the Company reviews and revises the security documents, such as: policies, standards, procedures, and guidelines, on a regular basis?
2. Whether the Company audits the processes and procedures for compliance with established policies and standards?
3. Whether the Company test the disaster plans on a regular basis?
4. Does management regularly review lists of individuals with physical access to sensitive facilities or electronic access to information systems.

Summing-up

With the rapid growth of cyberattacks, cybersecurity is increasingly important in all organizations. This increase requires auditors to evaluate cybersecurity practices, programs, and tools to ensure that their businesses have

good cyber governance Cybersecurity vulnerabilities can represent a severe threat to the whole organization, thereby increasing the requirement for highly trained IT auditors in cybersecurity audits

Finally, we may conclude that the business firm has to take all feasible efforts to establish a strong cybersecurity capacity in this era of global digital flows. Protection plans cannot be exclusively centred on companies must also include the human aspect. They must aim to establish digitally sustainable cultures in which cybersecurity is an everyday responsibility for key stakeholders at all levels.

References

1. Agrafiotis I, *et al*. A Taxonomy of Cyber-harms: Defining the Impacts of Cyber-attacks and Understanding How they Propagate. Journal of Cybersecurity,2018:4(1):1-15.
2. Bhushan M, Rathore RS, Jamshed A. Fundamentals of Cyber Security. BPB Publications, New Delhi, 2017.
3. Jaccard JJ, Nepal S. A Survey of Emerging Threats in Cybersecurity. Journal of Computer and System Sciences,2014:80(5):973-993.
4. Khilari S, Jadhav R, Abraham A. Information Security and Audit. Everest Publishing House, Pune, 2015.
5. Singh A. Introduction to Cyber Security. University Press, Hyderabad, 2024.
6. Singh G. Fundamentals of Cyber Security. Chyren Publication, Palwal, 2023.
7. Vishnu PK, Anil PV. Emergence of Cyber Security Audit: How Cyber Security Audit will be Helpful for Business in the Age of Digital Transformation. The Management Accountant,2021:56(9):62-64.
8. www.bridewell.com.
9. www.consultedge.global.
10. www.isaca.org.
11. www.pwc.com.