भारत हेवी इलेक्ट्रिकल्स लिमिटेड

Bharat Heavy Electricals Limited

दिशा

सतर्कता विभाग की त्रैमासिक ई-पत्रिका

सैंतालीसवाँ संस्करण

(जनवरी - मार्च, 2025)

कॉर्पोरेट सतर्कता विभाग

CONTENTS

EDITORIAL COMMITTEE

MESSAGE FROM DIRECTOR (HR)

It gives me immense pleasure to contribute to this edition of the Vigilance Magazine 'DISHA', a platform that consistently upholds the values of integrity, transparency, and accountability which are the cornerstones of any progressive organization.

The strength of an organization lies in its ability to face obstacles without compromising its values. It's about ensuring that accountability is built into every system, every action, and every interaction. Vigilance is a mindset considered more than a department/subset of a successful organisation. Vigilance is not about suspicion but is about awareness. It's about staying alert, asking the right questions, and doing the right thing — even when no one's watching. It's the latent force driving ethical decisions, fair processes, and a workplace culture built on trust. It's intrinsic to building systems that support people in making ethical choices every day.

This magazine reminds us of our collective responsibility and encourages us to not only follow the rules, but to uphold the spirit behind them. I applaud the Vigilance Team for reminding the ethical ethos alive by communicating the relevant information.

Let's continue to create a culture where doing the right thing is the easiest thing.

(Krishna Kumar Thakur)
Director (HR)

ARTICLES

4.0 Securing Information Asset through Digital Vigilance

The internet has fast emerged as the most effective vehicle for integrated growth of business. Every company must seriously assess its potential for using this powerful technology in management of its supply / demand chain. This enables the customers to get direct link with the information systems and they can update themselves on different information of
their interest viz, production and market forecast etc. The only technical requirement is to have a PC, internet connection and browser and last but not the least a "Password" for authentication. This password is like the key of the locker wherein valuable information assets are stored.

Now let us understand what is "Information Asset". An Information Asset refers to any valuable piece of data or information that an organisation possesses and utilises to support its operations, decision-making processes, and strategic objectives. Essentially, any piece of information that contributes to an organisation's ability to function, innovate, or maintain a competitive edge can be considered an Information Asset. Identifying Information Assets is the first step in effective Information Management. Several methods can be used to identify and categorise Information Assets within an organisation, including conducting information audits, engaging stakeholders across departments to gather insights into information needs and usage patterns, utilising data classification frameworks, and leveraging automated tools and software solutions to scan and analyse digital repositories for valuable Information Assets. These assets come in various forms and can include anything from customer databases and financial records to proprietary intellectual property and operational manuals, research reports, industry analyses, and market studies etc.

Dividing Information Asset involves categorising them based on their attributes, such as sensitivity, value, and relevance to the organisation's goals and objectives. Information Assets can be divided into various categories, including:

1) **Strategic assets:** Information Assets that directly contribute to achieving the organisation's strategic objectives.

2) **Operational assets:** Information Assets that support day-to-day operations and processes.

3) **Regulatory assets:** Information Assets that are subject to regulatory requirements and compliance obligations.

4) **Intellectual property assets:** Information Assets that are protected by intellectual property rights, such as patents, copyrights, and trademarks.

Paradigm Shift in Business Processes from Physical to Digital

Deployment of information technology into it, with the goal of all-round improvement. Digitalisation is transformative. It changes how companies interact with their customers and often their revenue streams. The new generation business fundamentals are focussing more and more on speed of transmission and zero error operations.

Emergence of Digital Platform as a new Business Model in India:

In recent times, digital technologies have advanced quickly. It has made the globe more closely linked than ever. Statement of Sunder Pichai, the visionary leader and digital maestro, which proves the real-life situation of significant revolutionary growth prospects of digital transformation initiatives in India setting aside legacy trends of traditional Indian Businesses is quoted below:

“India will be a global player in the digital economy and it will be competitive with any country in the world.

There is a timing issue. We are doing well as a country. We need to stay at it. We need a few more years and we will get to it. I am absolutely confident”.

Risks Involved

Fundamentally, individuals might put themselves into unknowingly through the lack of security while working in a digital platform is defined as Digital Vulnerability.

Vulnerabilities at a glance:

A risk might include:

 possible financial loss

 data loss or corruption

 reputational damage

 legal and compliance problems.

Following examples will elaborate the concerns in an effective way:

 Large scale invoice manipulations concerning the payment of bills.

 Manipulation of account balances and balance sheets of banks.

 Misusing ATM cards either by using stolen cards or manufacturing duplicate cards.

 Sabotage by virus programs and worm programs.

 Computer Extortion of systems and data stocks.

 Hacking through telephone system, voice mail system, etc.

 Unauthorised copying and use of foreign computer programs

 Attack on life by manipulating fight control system etc.

The internet has become the target of hackers because common people, business organisations, banks and financial institutions use the internet without adequate awareness of the security risks. Computers connected to the internet are vulnerable to hacking.

India has been plagued by several recent ransomware attacks, disrupting critical services and causing widespread panic.

Let's take a closer look at some of the recent ransomware attacks that have hit India:

Plethora of Cyberattacks in India: Few Examples and consequences faced

 In 2023, hackers attacked AIIMS Delhi, causing server shutdowns and disrupting health services

 Telangana and Andhra Pradesh power utility systems attack: Telangana and Andhra Pradesh, two

southern states in India, got hit by a ransomware attack on their power utility systems last year.

These recent ransomware attacks in India is a growing concern. The attacks on critical infrastructure like power utilities and seaports highlight the need for better cybersecurity measures to protect against such attacks. As India continues to digitalize its economy, it is vital to invest in cybersecurity infrastructure to safeguard the country's critical assets and prevent significant economic and societal consequences.
Significance of Digital Vigilance:

In the realm of digital interactions, the need for vigilance is constant. The domain of Vigilance function is passing through a paradigm shift from the Legacy Mode of Preventive, Punitive and Surveillance to Digital Mode of security monitoring, establishing a Security Operation Centre (SOC), continuously improving security, detecting and responding to threats, and safeguarding business data supporting operations, decision-making processes, and strategic objectives, to enhance resilience. It is no longer a watchdog only but a roaring lion in the cyberspace also inviting attention of others. The crux of digital vigilance is to secure information asset which could be illustrated as need for **V**-Vision, **I**-Integrity, **G**-Goal, **I**–Intelligence, **L**–Leadership, for **A** – Achieving against, **N**-New, **C**–Challenges, with **E**–Excellence.

BHEL, with the vision of becoming "A global engineering enterprise providing solutions for a better tomorrow" must work with the mission of "monetising information assets to create, protect, and increase business value". Digital Vigilance is the defence mechanism in this Global Order of Business where Integrity & Intelligence are the "Cause" for building asset and Innovation is the "Effect" resulting in Enhanced Business Value. So, the clarion call for the business organisations is to create increasing information asset alongside innovative business process and enhancement of Business Security with Digital Vigilance.

Josh Hain.....**.**

References:

Dr. R. Gokilavani and Dr. R. Durgarani, Evolution of Digital Economy in INDIA. International Journal of Marketing and Human Resource Management, 9(1), 2018.

Website References:

https://www.drishtiias.com/daily-updates/daily-news-editorials/india-s-cybersecurity-challenge-threats- and-strategies.

https://www.theknowledgeacademy.com/blog/what-is-an-information-asset.

https://www.statista.com/statistics/617136/digital-population-worldwide.

https://www.axians.co.uk/news/digital-vigilance-in-our-connected-world.

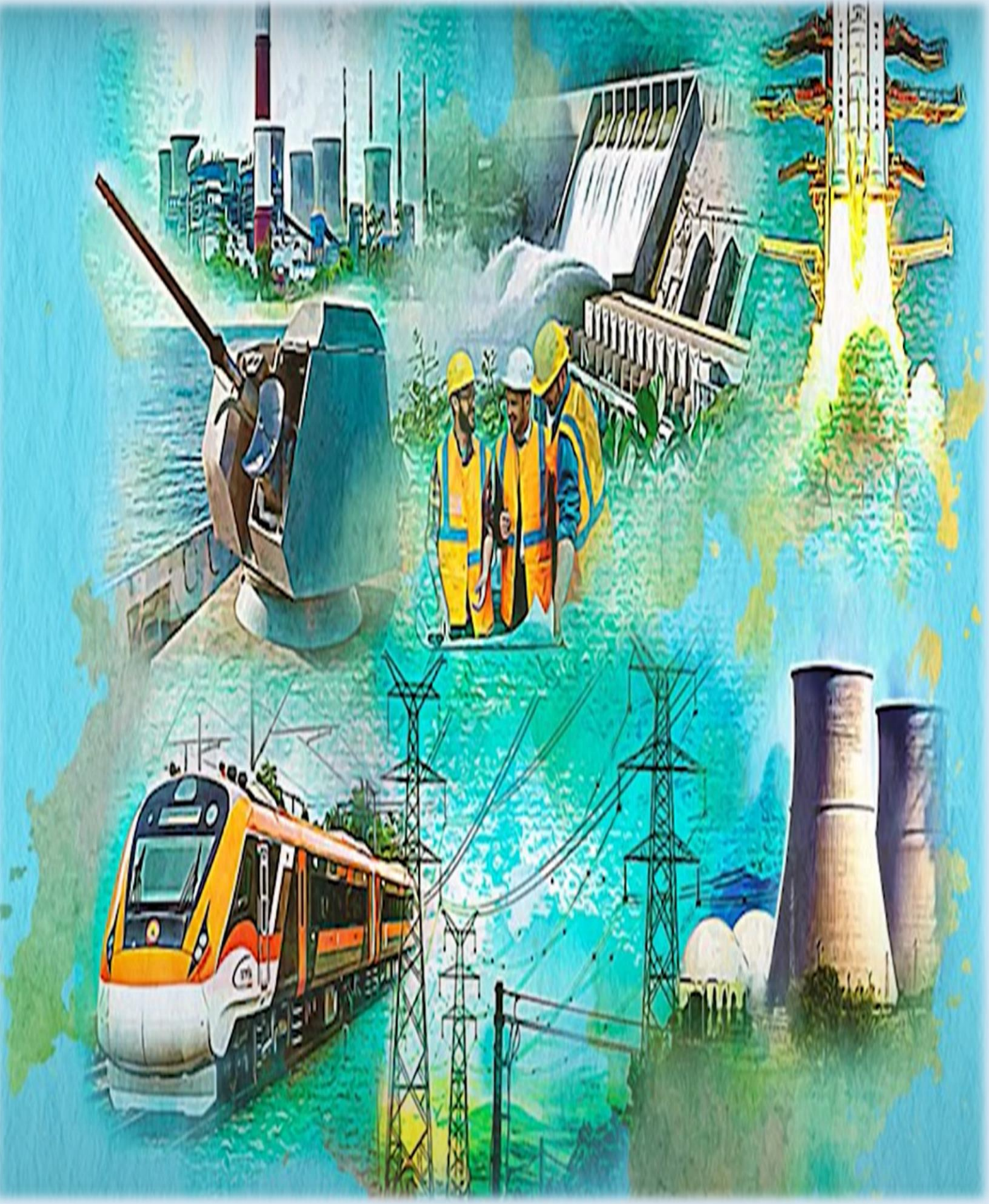
https://timespro.com/blog/what-led-to-the-growth-of-digital-marketing-in-india-recently.

https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html.

https://www.diva-portal.org/smash/get/diva2:1576133/FULLTEXT03.

https://ccoe.dsci.in/blog/7-biggest-ransomware-attacks-in-india.

Amitava Chakrabarti
Retd. AGM & Head (Commercial)
BHEL, PS-ER



Any suggestion(s) / article(s) upto 1200 words may be mailed to vigilance@bhel.in