पेंशन निधि विनियामक और
विकास प्राधिकरण
बी–14/ए, छत्रपति शिवाजी भवन,
कुतुब संस्थागत क्षेत्र,
कटवारिया सराय, नई दिल्ली–110016
दूरभाष : 011–26517501, 26517503, 26133730
फैक्स : 011–26517507
वेबसाईट : www.pfrda.org.in

**PENSION FUND REGULATORY
AND DEVELOPMENT AUTHORITY**
B-14/A, Chhatrapati Shivaji Bhawan,
Qutub Institutional Area,
Katwaria Sarai, New Delhi-110016
Phone : 011-26517501, 26517503, 26133730
Fax : 011-26517507
Website : www.pfrda.org.in

File No.: PFRDA/33/1/1/0001/2021-ICS INTRDY 15th September 2021

To,

All Stakeholders

Subject: Pension Cyber Spotlight – Quarterly Newsletter

As the economy is becoming more digitized, Cyber security incidents have also grown manifold with adoption of Digitalization and extensive use of *Emerging Technologies* such as Internet of Things (IOT), Artificial Intelligence (AI) and Cloud. The pandemic has further exacerbated the vulnerabilities with remote working becoming ubiquitous across organizations and digitalization penetrating the Financial Intermediation activities with rise of digital payments and personal investment through mobile application/online mode becoming the new normal.

The *data breaches, cyber jacking, ransomware attacks and deep fakes* across the world have shown the need for creating awareness and up-skilling among NPS Subscribers and the critical stake holders to protect their pension wealth, prosperity and reputation.

2. **'PENSION CYBER SPOTLIGHT'** The Quarterly Cyber Security and Technology Newsletter of PFRDA has been compiled and designed in a lucid way towards the objective of creating much needed awareness in a *rapidly evolving cyber threat scenario*, in order to safe guard one's priced assets.

3. **'Pension Cyber Spotlight – Volume 1'**, the first such issue has been attached at Annexure for the benefit of the stakeholders. The newsletter aims to brief the Financial Industry and Pension Sector stakeholders on the cyber-security issues and the latest Financial Technology developments.

This bulletin is issued under section 14(2)(j) of PFRDA Act 2013 towards undertaking steps for educating subscribers and the general public on issues relating pension, retirement savings, and is placed at PFRDA's website (*www.pfrda.org.in*) under the '*Pension Cyber Spotlight*' in the 'About Us' section.
The stake holders are welcome and may feel free to write to *daulath.khan@pfrda.org.in* for any suggestions, contributions or ideas.

Yours Sincerely,

K Mohan Gandhi

Chief General Manager

(k.mohangandhi@pfrda.org.in)

पीएफआरडीए pfrda

Pension Fund Regulatory and Development Authority
(PFRDA)

नेशनल पेंशन सिस्टम nps

PENSION CYBER SPOTLIGHT

PFRDA'S CYBER SECURITY AND TECHNOLOGY NEWSLETTER

Volume 1|AUG 2021

CONTENTS

From Chairman's desk,

With the Covid pandemic, the financial sector and organisational behaviour have undergone drastic changes. Digital technology has pervaded all aspects of our lives and the façade separating work and home has vanished. In this scenario the challenges to cybersecurity have grown manifold. With funds and data being stored and transferred digitally, the financial sector has become a primary target for numerous cyberattacks and crimes.

These developments necessitate a continuous knowledge enhancement and cyber security awareness to prevent and prepare against the cyber threats and protect subscriber data. It is a prerequisite for the financial regulators, industry stakeholders and the subscribers to keep themselves apprised of the latest trends and regulatory developments to build a resilient financial sector.

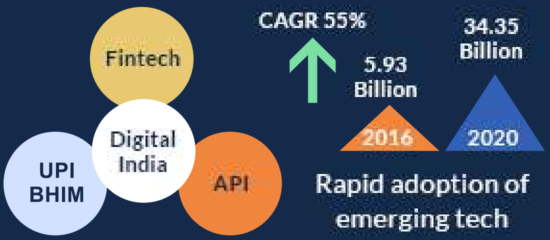
The Pension Cyber Spotlight newsletter thus seeks to curate the relevant content with expert insights to satiate the knowledge requirement of readers. I congratulate the team on the launch of the first volume of Pension Cyber Spotlight and wish them all the best for the future editions.

Regards,
Shri Supratim Bandhopadhyay
Chairman, PFRDA

Focal Point

Why Cyber Security is important now more than ever?

India's Digital Transformation Digital Payments

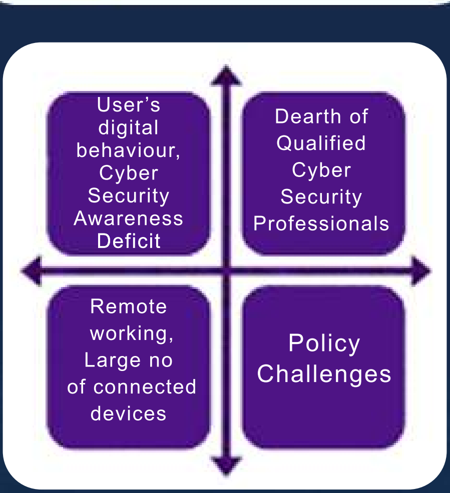


Rapid adoption of emerging tech

Cloud Big Data AI IOT

30 Billion No. of IOT connections expected by 2025. Almost 4 IOT devices per person on average.

Digital Dilemma



User's digital behaviour, Cyber Security Awareness Deficit

Dearth of Qualified Cyber Security Professionals

Remote working, Large no of connected devices

Policy Challenges

Digital literacy, Cyber Defense Capability, and policy frameworks have lagged behind the rapid adoption of digitalisation.

This scenario has been succinctly expressed by the 2021 World Economic Forum Global Risks Report:

"Business, government, and household cybersecurity infrastructure and/or measures are outstripped or rendered obsolete by increasingly sophisticated and frequent cyber-crimes, resulting in economic disruption, financial loss, geopolitical tensions and/ or social instability. "

Cyber Threat Landscape in India

Cyberattacks surged **3-fold** to 1.16 mn last year in India: CERT-IN

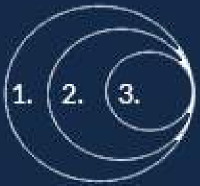
Survey by SophosLabs has reported the impact of ransomware attacks in India has tripled to **3.38 mn $** in 2021.

The major data breaches in India which happened recently i.e in 2021 such as Big Basket, Dominos, Upstox, etc. are a reality check on the level of cyber security protection in the nation.

Cyber Spotlight Funda

Protecting organisations against costly data breaches and resultant losses in money and reputation starts with understanding the fundamentals of the security infrastructure.

Information Security, Cyber Security and Network Security



1. InfoSec | 2.Cyber Security | 3.Network Security

Infosec is the larger set protecting info and info systems in all forms be it digital or not.

Cyber Security a subset of Infosec deals with protection of the cyber/ digital spaces from cyber-attacks.

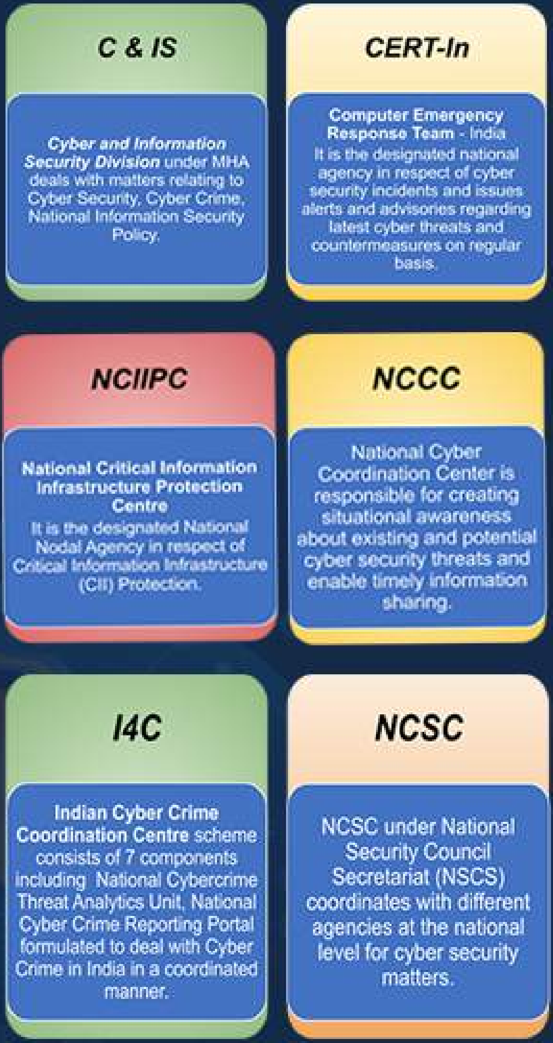
Network Security is a subset of Cyber Security protecting the data being transmitted through devices form being intercepted or corrupted.

These terms are so closely linked that they are often used interchangeably. However, they are not the same and it is important to recognise the difference between the terms.

Policy Track

India's Cyber Security Institutions

This edition of Cyber Spotlight will provide an overview of the cyber security institutions operational in India. Further insights and analysis to be continued in the upcoming editions.



C & IS

Cyber and Information Security Division under MHA deals with matters relating to Cyber Security, Cyber Crime, National Information Security Policy.

CERT-In

Computer Emergency Response Team - India
It is the designated national agency in respect of cyber security incidents and issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.

NCIIPC

National Critical Information Infrastructure Protection Centre
It is the designated National Nodal Agency in respect of Critical Information Infrastructure (CII) Protection.

NCCC

National Cyber Coordination Center is responsible for creating situational awareness about existing and potential cyber security threats and enable timely information sharing.

I4C

Indian Cyber Crime Coordination Centre scheme consists of 7 components including National Cybercrime Threat Analytics Unit, National Cyber Crime Reporting Portal formulated to deal with Cyber Crime in India in a coordinated manner.

NCSC

NCSC under National Security Council Secretariat (NSCS) coordinates with different agencies at the national level for cyber security matters.

News in Cyber Spotlight

Domestic Data Breaches

Big Basket Dominos Upstox and more

Database of about 20 million Big Basket users was allegedly leaked on the dark web in April 2021. This is said to be the data from a breach in November 2020. Big Basket has responded by incorporating OTP based mechanism as an enhanced security measure.

The attack on Dominos exposed 18 crore order details placed by Indian consumers. The details were made public by attackers who created a webpage on the darkweb enabling a simple search using Mobile Nos., jeopardising the privacy of the customers.

Upstox, one of India's largest brokerage firm suffered a data breach with hackers stealing data of around 25 lakh customers and shared on dark web. Upstox took proactive measures by alerting the customers of the hack and initiated multiple security enhancements.

These breaches raise considerable user privacy concerns and negatively influence public trust.

Ransomware attacks

Ransomware Attacks in India

Research by two leading cyber security firms – Sophos and Check Point have conducted studies on the Ransomware attacks in india.

Checkpoint Survey finds that an average of 213 weekly ransomware attacks occur per organisation in India. The Sophos survey found that in India, the approximate recovery cost from the impact of a ransomware attack

Kaseya Attack

Touted as the largest ever Ransomware attack, the Kaseya attack on July 2nd 2021 paralysed hundreds of businesses who use the products of the IT management software provider. The cyberattack has been attributed to the REvil/Sodinikibi ransomware group. Kaseya is central to global software supply chain servicing over 40000 organisations. Many Managed Service Providers (MSPs) use Kaseya platform to manage networks of other businesses which increases the extent of potential damage exponentially.

How did the attack take place?

As per the security experts who investigated the attack, zero-day vulnerabilities were exploited by the attackers to trigger a bypass authentication and upload a malicious payload as a software update which is a REvil Ransomware.

Advisories

Beware of fake SMS & Apps

In May 2021, CERT-In issued an advisory warning about fake apps that were being spread through SMS. As per the advisory these apps on being installed spread to the victim's contacts via SMS and also gain unnecessary permission to access user data.

Some of the malicious APKs under circulation are Covid-19.apk, Vccin-Apply.apk, Cov-Regis.apk, Vaci__Regis.apk, and MyVaccin_v2.apk.

Vulnerabilities in Microsoft Products

CERT-In issued a public advisory CIAD – 2021 - 0024 on the multiple vulnerabilities reported in the Microsoft products which could be exploited by an attacker to access sensitive information, perform a Denial of Service (DoS) attack etc. This advisory suggests applying the updates to solve the vulnerabilities.

Other updates

ITU Global Cyber Security (GCI) Index 2020

India has made it to the top 10 in GCI 2020 released by ITU. India has moved up 37 places to the 10th rank with a total score of 97.5 points out of a maximum of 100.

The ranking is based on the assessment of 5 parameters of cyber security:

1. Legal measures
2. Technical measures
3. Organisational Measures
4. Capacity Development
5. Cooperation

National helpline No. to report Cyber Crime

The Ministry of Home Affairs (MHA) has operationalised the national helpline 155260 and reporting platform for preventing financial loss due to cyber fraud. Currently, the number is operational in these 7 territories (Chhattisgarh, Delhi, Madhya Pradesh, Rajasthan, Telangana, Uttarakhand and Uttar Pradesh).

Editorial Team

Information and Cyber Security Department, PFRDA

Feedback/Suggestions

Mail to:

Shri Mohan Gandhi
CGM
k.mohangandhi@pfrda.org.in

Shri Daulath Ali Khan
DGM
daulath.khan@pfrda.org.in

Shri Srinivas Bhoosarapu
CISO
Srinivas.bhoosarapu@pfrda.org.in

Shri Vignesh C
Assistant Manager
Vignesh.c@pfrda.org.in