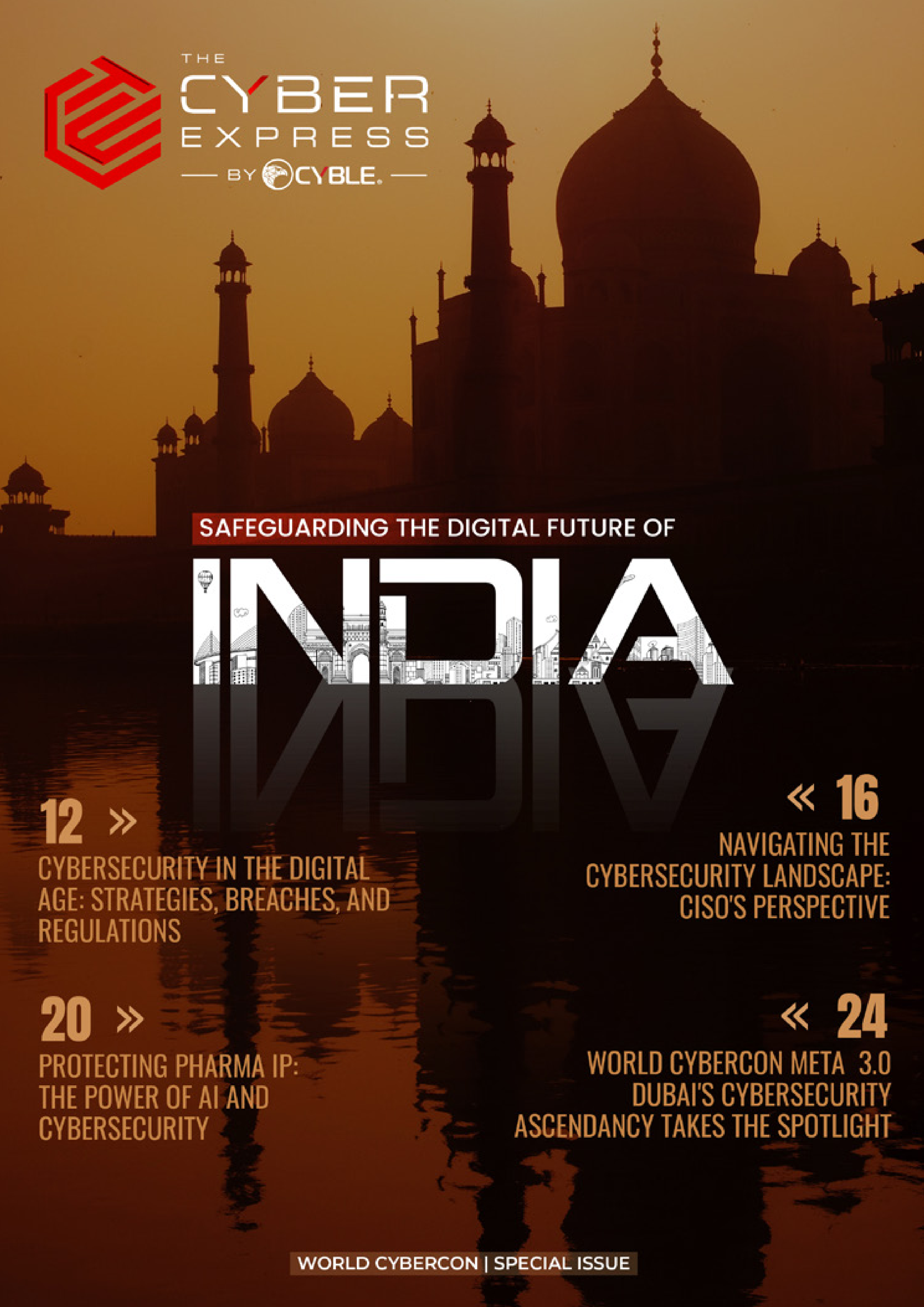


THE CYBER EXPRESS

BY CYBLE.

SAFEGUARDING THE DIGITAL FUTURE OF

INDIA

12 »

CYBERSECURITY IN THE DIGITAL AGE: STRATEGIES, BREACHES, AND REGULATIONS

« 16

NAVIGATING THE CYBERSECURITY LANDSCAPE: CISO'S PERSPECTIVE

20 »

PROTECTING PHARMA IP: THE POWER OF AI AND CYBERSECURITY

« 24

WORLD CYBERCON META 3.0 DUBAI'S CYBERSECURITY ASCENDANCY TAKES THE SPOTLIGHT

WORLD CYBERCON | SPECIAL ISSUE

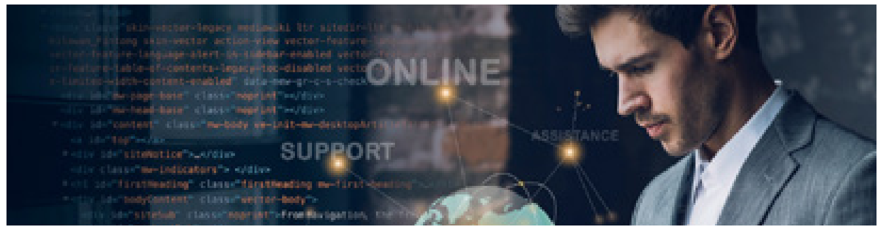
CYBLE®

STAY SECURE WITH **CYBLE'S ADVANCED** AI-POWERED CYBERSECURITY PLATFORM WITH **CYBLE VISION**

Organizations can now get total visibility and control over their attack surface, ensuring a robust security posture amid evolving cyber threats

See **Cyble Vision** in Action

Contents



STAFF

Editorial

Augustin Kurian
Editor-in-Chief
editor@thecyberexpress.com

Paul Shread
International Editor
paul.shread@thecyberexpress.com

Krishna Murthy
Deputy Editor
krishna.murthy@thecyberexpress.com

Avantika Chopra
Associate Editor
avantika@thecyberexpress.com

Samiksha Jain
Magazine Producer
samiksha.jain@thecyberexpress.com

Mihir Bagwe
Principal Correspondent
mihir.bagwe@thecyberexpress.com

Ashish Khaitan
Correspondent
ashish@thecyberexpress.com

Alan Joseph
Technical Writer
alan.joseph@cyble.com

Management

Rajashakher Intha
Director of Marketing
And Product Management
raj@thecyberexpress.com

Ashish Jaiswal
Conference Manager
ashish.j@thecyberexpress.com

Priti Chaubey
Manager - Communications
priti.c@thecyberexpress.com

Pallavi Dash
Social Media Manager
pallavi.dash@thecyberexpress.com

Ravi Gupta
SEO Analyst
ravi@thecyberexpress.com

Vittal Chowdry
Design Lead
vittal@thecyberexpress.com

Some of the Images in this magazine are provided by ***Freepik***

Image credits: Shutterstock & Freepik

*Responsible for selection of news under PRB Act. Printed & Published by Augustin Kurian, The Cyber Express LLC.,
The publishers regret that they cannot accept liability for errors & omissions contained in this publication, howsoever caused. The opinion & views contained in this publication are not necessarily those of the publisher. Readers are advised to seek specialist advice before acting on the information contained in the publication which is provided for general use & may not be appropriate for the readers' particular circumstances. The ownership of trade marks is acknowledged. No part of this publication or any part of the contents thereof may be reproduced, stored in a retrieval system, or transmitted in any form without the permission of the publishers in writing.

FROM THE EDITOR´S DESK

AUGUSTIN KURIAN

Editor-in-Chief

Dear Readers,

Welcome to the World CyberCon Special Edition of our magazine, where we dive deep into the escalating cyber threats that have the potential to disrupt the very foundations of Indian society and beyond.

In the first half of 2024 alone, India experienced surge in number of cyberattacks, including 593 cases of data breaches, leaks, ransomware attacks, and illegal trading of access credentials.

This sharp rise clears that the current cybersecurity measures and regulations are struggling to keep pace with the evolving complexity of these threats.

In this issue, we are privileged to feature thought-provoking articles by some of the leading cybersecurity experts in the industry.

Amit Joshi, CISO at Adani Cement, offers critical insights on Cybersecurity in the Digital Age: Strategies, Breaches, and Regulations, providing a roadmap for staying ahead of increasingly sophisticated attacks.

Dhiraj Ranka, CISO at TATA AIG General Insurance Limited, shares his expertise in Navigating the Cybersecurity Landscape: A CISO's Perspective, while Prianshu Khandwala, CISO at Sun Pharma, explores Protecting Pharma IP: The Power of AI and Cybersecurity.

This edition also takes you to the heart of the World CyberCon 3.0 META Cybersecurity Conference, recently held at the iconic Al Habtoor Palace in Dubai.

This pivotal event drew over 100 cybersecurity professionals from around the globe to engage in discussions around the most pressing cybersecurity challenges and emerging trends. It was a dynamic platform for dialogue, knowledge-sharing, and collaboration in an increasingly complex cyber landscape.

In addition, we delve into articles exploring critical issues such as cyberattacks on India's wind sector and other vital infrastructure. The Convergence of IT and OT is a key topic, analyzing the cybersecurity implications for critical infrastructure and the new risks arising from this integration.

This issue is more than just a collection of insights; it is a call to action.

As we advance in the digital age, protecting the infrastructure that underpins our societies must remain a top priority. Our strategies need to be vigorous, unified, and forward-thinking, aimed at mitigating the risks that could disrupt our way of life.

We hope you find this special edition both insightful and essential.

Your feedback is invaluable as we continue to sail across these challenges together, and we encourage you to share your thoughts with us at editorial@thecyberexpress.com. .

Stay informed, stay secure.

Augustin Kurian
Editor-in-Chief
The Cyber Express

THE CYBER EXPRESS

ADVISORY BOARD

Mohammad khaled
VP Growth and Business Transformation,
Reach Digital

Dina ALSALAMEN
VP, Head of Cyber and Information Security,
Bank ABC

Saeed AlShebli
Deputy Director of Digital Security,
Ministry of Interior, UAE

Talal Albalas
CISO, ADQCC

Prashant Warankar
Chief Information Security Officer,
Angel One Wealth

Irene Corpuz
Co-Founder & Board Member,
Women in Cyber Security Middle East

Satnam Narang
Senior Staff Research
Engineer, Security Response,
Tenable

David B. Cross

Senior Vice President
and CISO, Oracle

Celia Mantshiyane

CISO, MTN South Africa

Holly Foxcroft

Head of Neurodiversity,
Cyber Research and
Consulting, Stott and May
Consulting

Lanx Goh

Senior Director & Global Head
of Privacy, Prudential plc

Jo Mikleus

Advisory Board Convenor,
The Cyber Express

Chuck Brooks

President, Brooks
Consulting International

Jane Teh

Chief of Staff to CEO
Office & Senior Director -
Security Consulting Services,
vCyberiz

Jennifer Cox

Director for Ireland, Women
in CyberSecurity (WiCyS) UK &
Ireland

Pooja Shimpi

Founder, SyberNow

Asmae E.

CISRCO, HPS

Alexandra Mercz

Founder, Synterra Asia

Ankit Satsangi

Director, BEEAH Group

Ankur Ahuja

Senior Vice President,
CISO, Billtrust

Kaustubh Medhe

Vice President, Research and Cyber
Threat Intelligence, Cyble Inc

Mel Migrino

Southeast Regional Director
and Adviser, Gogolook

Cybersecurity in the Digital Age Strategies, Breaches, and Regulations

- By Amit Joshi

CISO Adani Cement, Adani Enterprises Limited

In today's digital landscape, cybersecurity is a critical concern for individuals, businesses, and governments alike. With the increasing reliance on technology and the internet, the risk of cyber-attacks and data breaches has never been higher. In this article, we will explore the importance of cybersecurity strategies, the devastating impact of data breaches, and the role of cybersecurity laws and regulations in protecting our digital world.

Cybersecurity Strategies

A robust cybersecurity strategy is essential for any organization that wants to protect its digital assets from cyber threats. This includes implementing robust security measures such as firewalls, intrusion detection systems, and encryption technologies. Additionally, organizations must ensure that their employees are aware of the risks of cyber-attacks and are trained to identify and respond to potential threats.

One of the most effective cybersecurity strategies is the implementation of a Zero Trust model. This approach assumes that all users and devices, whether inside or outside the organization's network, are potential threats. By verifying the identity and permissions of all users and devices, organizations can significantly reduce the risk of cyber-attacks.

Another important strategy is the implementation of regular security audits and penetration testing. These tests help identify vulnerabilities in the organization's systems and networks, allowing for prompt remediation and reducing the risk of cyber-attacks.

Data Breaches

Data breaches are a devastating consequence of cyber-attacks. When an organization's systems or networks are compromised, sensitive data such as personal information, financial data, and intellectual property can be stolen or compromised. The impact of a data breach can be severe, resulting in financial losses, damage to reputation, and legal liabilities.

One of the most notable data breaches in recent history is the Equifax breach, which exposed the personal information of over 147 million people. The breach was caused by a vulnerability in the company's website, which was exploited by hackers. The incident highlighted the importance of robust cybersecurity measures and the need for organizations to be proactive in protecting their digital assets.

Cybersecurity Laws and Regulations

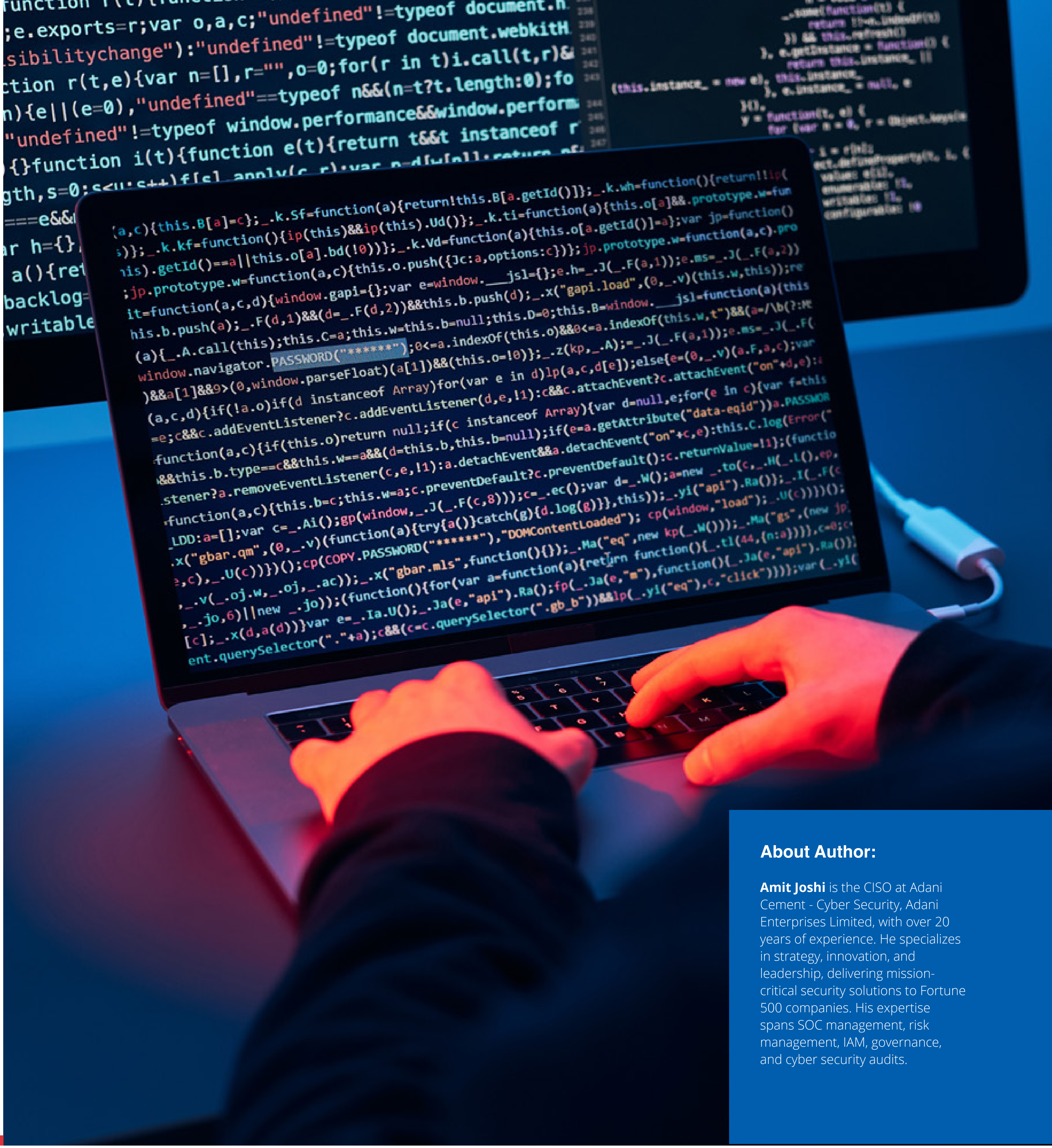
Cybersecurity laws and regulations play a critical role in protecting our digital world. These laws and regulations provide a framework for organizations to follow, ensuring that they implement robust cybersecurity measures to protect sensitive data.

One of the most notable cybersecurity laws is the General Data Protection Regulation (GDPR) in the European Union. The GDPR provides individuals with greater control over their personal data and imposes strict regulations on organizations that handle personal data.

In the United States, the Cybersecurity Act of 2015 provides a framework for organizations to share cybersecurity threat information with the government. The law also provides liability protections for organizations that share threat information in good faith.

Conclusion

Cybersecurity is a critical concern in today's digital landscape. With the increasing reliance on technology and the internet, the risk of cyber-attacks and data breaches has never been higher. Organizations must implement robust cybersecurity strategies, including the implementation of Zero Trust models, regular security audits, and penetration testing. Additionally, cybersecurity laws and regulations provide a framework for organizations to follow, ensuring that they implement robust cybersecurity measures to protect sensitive data.



About Author:

Amit Joshi is the CISO at Adani Cement - Cyber Security, Adani Enterprises Limited, with over 20 years of experience. He specializes in strategy, innovation, and leadership, delivering mission-critical security solutions to Fortune 500 companies. His expertise spans SOC management, risk management, IAM, governance, and cyber security audits.

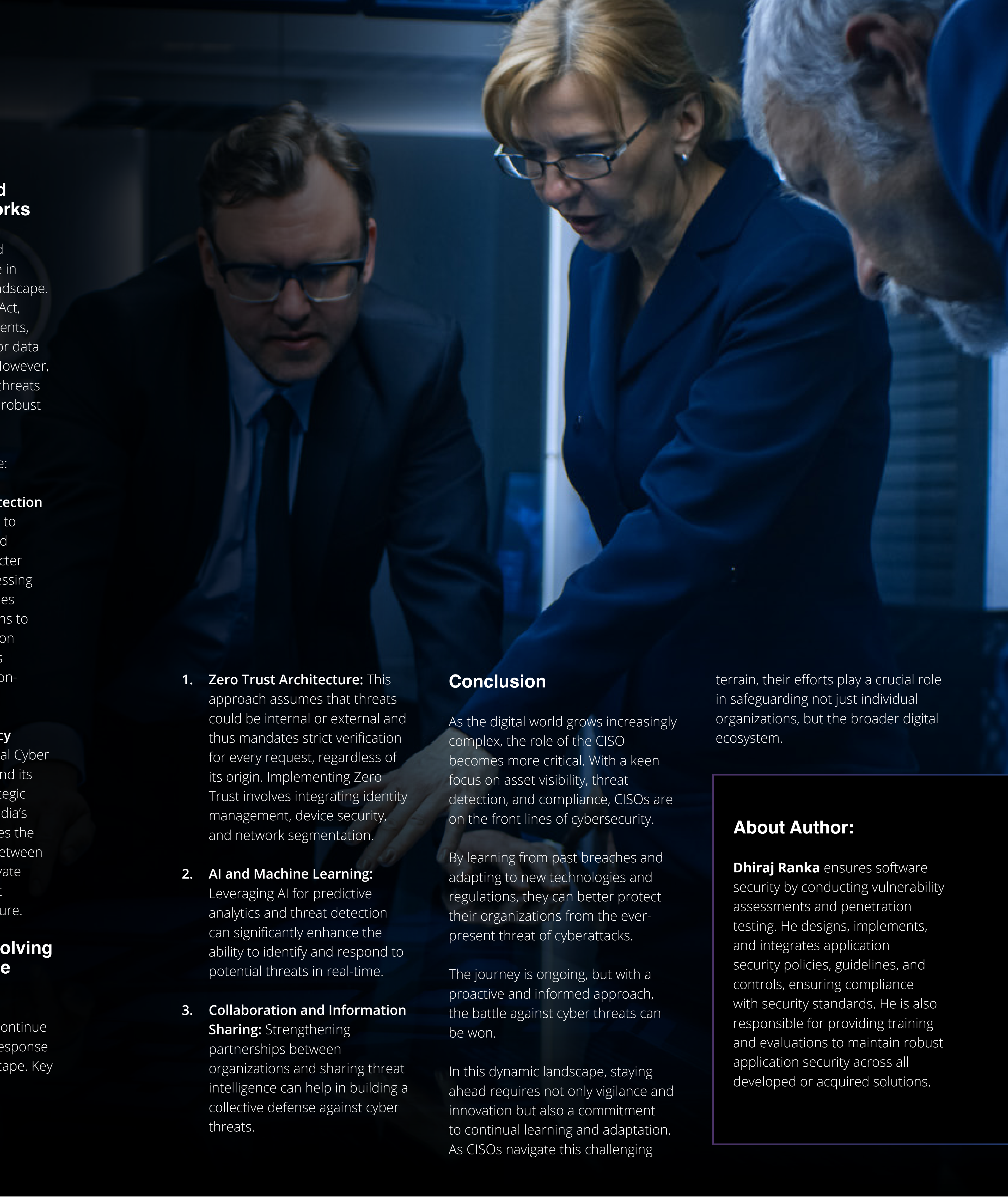
CISO STRATEGIES

Navigating the Cybersecurity Landscape: CISO's PERSPECTIVE

- By Dhiraj Ranka

CISO, TATA AIG General Insurance Limited

In the ever-evolving digital world, cybersecurity stands as the first line of defense against increasingly sophisticated threats. As Chief Information Security Officers (CISOs) in India grapple with these challenges, they are constantly adapting their strategies to stay ahead. This article explores the current landscape of cybersecurity from the viewpoint of an CISO, focusing on asset visibility, threat detection, and recent data breaches that underscore the urgency of robust cybersecurity measures.



The Modern Battlefield: Cybersecurity Strategies

In today's digital environment, cybersecurity strategies must be as dynamic as the threats they aim to mitigate. For CISOs, this means developing comprehensive strategies that address both current vulnerabilities and emerging threats. The foundation of any effective strategy includes:

1. **Asset Visibility:** Knowing what assets are on your network is crucial. This involves maintaining an up-to-date inventory of hardware and software, which can be a daunting task given the rapid pace of technological change. Tools like Security Information and Event Management (SIEM) systems and Network Detection and Response (NDR) solutions are essential for gaining visibility and ensuring that no asset is overlooked.

2. **Threat Detection and Response:** Detecting threats before they can cause significant damage requires advanced threat intelligence and proactive monitoring. Techniques such as behavioral analysis and machine learning are increasingly used to identify anomalies that could indicate a breach.

3. **Incident Response Planning:** Preparing for potential incidents through detailed response plans is critical. This includes having a clear protocol for containment, eradication, and recovery, along with regular drills to ensure that the team is ready for any eventuality.

4. **Compliance and Training:** Ensuring compliance with regulatory standards and conducting regular training for employees on security best practices are also vital components.

Recent Breaches: A CISO's Nightmare

Despite the best strategies, breaches are an unfortunate reality. In India, several high-profile data breaches have highlighted the vulnerabilities that exist even in well-secured environments:

- **The 2023 Data Breach at a Major Financial Institution:** This breach involved the compromise of sensitive customer data, including personal and financial information. The attack was executed through a sophisticated phishing campaign that exploited weaknesses in the institution's email security. The breach not only resulted in significant financial loss but also damaged the institution's reputation.

- **The 2024 Ransomware Attack on a Healthcare Provider:** This incident saw a ransomware group lock down critical healthcare systems, disrupting patient care and compromising medical records. The attackers demanded a substantial ransom, leading to a tense negotiation period and an extensive recovery effort.

These breaches underscore the importance of not only having strong preventative measures but also a well-defined incident response plan.

Navigating Legal and Regulatory Frameworks

India's cybersecurity laws and regulations play a pivotal role in shaping the cybersecurity landscape. The Information Technology Act, 2000, along with its amendments, provides a legal framework for data protection and cybercrime. However, the evolving nature of cyber threats has prompted calls for more robust regulations.

Recent developments include:

- **The Personal Data Protection Bill:** This legislation aims to enhance data privacy and security by imposing stricter guidelines on data processing and storage. It emphasizes the need for organizations to implement data protection measures and mandates stringent penalties for non-compliance.

- **The Cybersecurity Policy Framework:** The National Cyber Security Policy of 2013 and its updates outline the strategic approach for securing India's cyberspace. It emphasizes the need for collaboration between the government and private sector to build a resilient cybersecurity infrastructure.

The Road Ahead: Evolving Strategies and Future Trends

Looking ahead, CISOs must continue to evolve their strategies in response to the changing threat landscape. Key areas of focus include:

1. **Zero Trust Architecture:** This approach assumes that threats could be internal or external and thus mandates strict verification for every request, regardless of its origin. Implementing Zero Trust involves integrating identity management, device security, and network segmentation.

2. **AI and Machine Learning:** Leveraging AI for predictive analytics and threat detection can significantly enhance the ability to identify and respond to potential threats in real-time.

3. **Collaboration and Information Sharing:** Strengthening partnerships between organizations and sharing threat intelligence can help in building a collective defense against cyber threats.

Conclusion

As the digital world grows increasingly complex, the role of the CISO becomes more critical. With a keen focus on asset visibility, threat detection, and compliance, CISOs are on the front lines of cybersecurity.

By learning from past breaches and adapting to new technologies and regulations, they can better protect their organizations from the ever-present threat of cyberattacks.

The journey is ongoing, but with a proactive and informed approach, the battle against cyber threats can be won.

In this dynamic landscape, staying ahead requires not only vigilance and innovation but also a commitment to continual learning and adaptation. As CISOs navigate this challenging terrain, their efforts play a crucial role in safeguarding not just individual organizations, but the broader digital ecosystem.

About Author:

Dhiraj Ranka ensures software security by conducting vulnerability assessments and penetration testing. He designs, implements, and integrates application security policies, guidelines, and controls, ensuring compliance with security standards. He is also responsible for providing training and evaluations to maintain robust application security across all developed or acquired solutions.

PROTECTING PHARMA IP: THE POWER OF AI AND CYBERSECURITY

- By Prianshu Khandwala

CISO - Head Information Security,
Sun Pharma

The pharmaceutical industry, a cornerstone of modern medicine, is undergoing a profound transformation driven by advancements in artificial intelligence (AI). In today's digital landscape, the convergence of cybersecurity and AI plays a vital role in protecting pharmaceutical innovations. The industry needs to understand the significance of this convergence and its impact on securing valuable intellectual property.

The pharmaceutical industry constantly advances with innovations in drug development, biotechnology, and healthcare solutions. AI is revolutionizing drug discovery, pioneering personalized medicine and uncovering new uses for existing drugs. These advancements bring about a wealth of valuable intellectual property and sensitive data that must be safeguarded from cyber threats. This is where the convergence of cybersecurity and AI comes into play.

Cybersecurity has long been indispensable in protecting sensitive information from malicious threats. However, with the rapid advancement of technology, traditional cybersecurity measures are no longer adequate to counter sophisticated cyber-attacks, including those targeting AI systems themselves. Finding trained cyber resources is a challenge on its own.

AI can significantly enhance the cybersecurity posture of pharmaceutical companies through several key mechanisms:

1. Real-Time Threat Detection and Response: AI systems can monitor network traffic and user behaviour in real-time to detect unusual patterns indicative of a cyber threat. Machine learning algorithms can quickly recognize these patterns, allowing for immediate response to potential breaches, preventing data breaches, and minimizing damage from cyber-attacks.

2. Predictive Analytics: AI can analyze historical data to predict future cyber threats. By understanding trends and patterns in cyber-attacks, AI can anticipate potential vulnerabilities and recommend preventive measures, enabling pharmaceutical companies to implement security measures before an attack occurs.

3. Automated Threat Mitigation: AI can automate the process of responding to cyber threats, reducing the time between detection and mitigation. Automated systems can isolate affected systems, block malicious traffic, and implement security patches without human intervention, crucially minimizing the impact of cyber-attacks.

4. Enhanced Data Security: AI can secure sensitive data through advanced encryption techniques and access controls. AI-driven systems ensure that only authorized personnel access critical data, reducing the risk of insider threats and data leaks, continuously monitoring access patterns to detect unauthorized attempts.

5. Protection Against Phishing and Social Engineering: AI can analyze communication patterns and identify phishing attempts or social engineering attacks, preventing employees from falling victim to these threats, which is particularly important in the pharmaceutical industry.

6. Secure AI Models: AI can protect the integrity of AI models used in drug discovery and development through techniques such as model obfuscation and adversarial training, ensuring the security and reliability of pharmaceutical research.

7. Continuous Learning and Adaptation: AI systems can continuously learn from new data and adapt to emerging threats, staying up-to-date with the latest threats and providing ongoing protection for pharmaceutical companies.

8. Resource Optimization: AI can optimize the allocation of cybersecurity resources by prioritizing threats based on their severity and potential impact, allowing pharmaceutical companies to focus their efforts on the most critical threats.

9. Compliance and Reporting: AI can assist in complying with regulatory requirements by automating the monitoring and reporting of security incidents, generating detailed reports on cybersecurity posture, incidents, and responses.

By leveraging AI in these ways, pharmaceutical companies can enhance their cybersecurity measures, protect their valuable intellectual property and sensitive data, and maintain the trust and confidence of their stakeholders.

About Author:

Prianshu Khandwala is a visionary security leader with a proven track record in building and maturing security practices. With extensive experience across multiple industries, he excels in aligning security solutions with business goals, managing diverse teams, and communicating effectively with C-level executives to drive organizational success.

World CyberCon meta 3.0: Dubai's Cybersecurity Ascendancy Takes the Spotlight

Panel Discussion
Predictive Cyber Threat Intelligence:
Anticipating Tomorrow's Attacks Today
Presenting Partner
CYBLE
THE CYBER EXPRESS
AZHAR ZAHIRUDDIN
Director of Data Protection
Group DPO, Chalhoub Group
WAQAS HAIDER
CISO, HBL Microfinance Bank
(Moderator)WAQAS HAIDER
MODERATOR
MAY 23, 2024

- By Samiksha Jain

The UAE's cybersecurity market is on a rapid growth trajectory, expected to expand from USD 0.59 billion in 2024 to USD 1.07 billion by 2029, with a strong compound annual growth rate (CAGR) of 12.72%. As the UAE embraces digitalization, the surge in connected devices has exposed new vulnerabilities, amplifying the need for vigorous cybersecurity measures. In the wake of the COVID-19 pandemic, digital transformation has accelerated, leading to a rise in cybercriminal activities, making cybersecurity a top priority for governments and businesses alike.

To counter growing threats, the UAE government has introduced strict cybersecurity standards, particularly for its agencies, reflecting its commitment to safeguarding its digital infrastructure. Last October, the UAE outlined a five-year budget prioritizing cybersecurity, a response to rising cyber threats, terrorism risks, and the nation's digital evolution. However, challenges such as budget constraints and the high cost of cybersecurity solutions continue to pose hurdles in fully securing the nation's digital assets.

In this context, the World CyberCon 3.0 META Cybersecurity Conference, held at Al Habtoor Palace in Dubai, emerged as a pivotal event. Drawing over 100 cybersecurity professionals and experts from across the globe, the event provided a dynamic platform to discuss the most pressing cybersecurity challenges and trends. Spanning six hours of collaboration, the conference attracted participants from more than 20 industries, highlighting the widespread importance of cybersecurity in today's digital world.

With the UAE's cybersecurity market projected to reach nearly USD 1.07 billion by 2029, the event highlighted the growing demand for effective defense mechanisms.

Augustin Kurian, Editor-in-Chief at The Cyber Express, emphasized the importance of this gathering, remarking, "The support and engagement from the cybersecurity community have been truly remarkable. This year's conference not only facilitated valuable knowledge exchange but also reinforced Dubai's position as a global tech hub addressing digital challenges."

A keynote address by Irene Corpuz, co-founder of Women in Cyber Security Middle East, captivated the audience. She highlighted the increasing risks startups face from cyberattacks, noting that even small businesses are prime targets for cybercriminals, stressing the urgency for heightened vigilance across all sectors.

"Even small startups are enticing prey to cybercriminals," Corpuz remarked, underlining the critical need for startups to embed cybersecurity measures from the very beginning of their journey.

World CyberCon META Edition: Diverse Sessions and Expert Panels

This year's World CyberCon META Edition also featured a rich lineup of sessions and expert-led panels. A standout panel, led by Jo Mikleus, Senior Vice President at Cyble, brought together an all-women lineup of cybersecurity experts, including Irene Corpuz, Sithembile Songo, Eng. Dina AlSalamen, and Afra Mohammed Almansoori. They discussed the pivotal role of AI in cybersecurity, showcasing how AI and machine learning (ML) are revolutionizing threat detection, incident response, and overall security frameworks.

Another highly anticipated session focused on cyber risk scoring, a critical tool in today's digital age. Moderated by Waqas Haider, CISO of HBL Microfinance Bank, the panel included Beenu Arora, CEO of Cyble; Azhar Zahiruddin, Director of Data Protection at Chalhoub Group; Ankit Satsangi, Director at Beeah Group; and Suhaila Hareb, ISR Auditor at Dubai Electronic Security Center.

Arora delivered compelling global insights, highlighting staggering statistics on data breaches, noting that 50,000 companies have been compromised in the past thousand days.

"In the last two and a half years, let's say, the last thousand days. Can anybody guess how many companies have reportedly been breached? The number we have exactly at the moment is 50 thousand! So 50 thousand companies, globally, have been breached, in the last thousand days", said Arora at The Cyber Express META Cybersecurity Conference in Dubai.

Throughout the event, the experts reinforced a key takeaway: while technological advancements are vital for cybersecurity, human elements—like employee awareness and training—are equally crucial in strengthening defenses against cyber threats.

Celebrating Excellence: The META Cybersecurity Awards

The World CyberCon 3.0 META Cybersecurity Conference didn't just provide a platform for insightful discussions—it also celebrated outstanding achievements in the cybersecurity community through its prestigious META Cybersecurity Awards. These awards honored the innovators, leaders, and trailblazers driving the industry forward, recognizing their dedication to protecting the digital landscape.

In a standout moment, Thomas Heuckeroth from Emirates Group and Dr. Hoda A. Alkhzaimi from EMaratsec were named The Cyber Express Cybersecurity Persons of 2024 for their remarkable contributions. These accolades underscore their pivotal roles in shaping cybersecurity practices across the META region.

Here's a complete rundown of this year's esteemed winners:

The Cyber Express Cybersecurity Person of 2024 (META): Man

Thomas Heuckeroth,

SVP IT Infrastructure & Digital Platforms, Emirates Group

Dr. Hoda A Alkhzaimi,

President, Emirates Digital Association for Women & Co-Chair for Global Future Council for Cyber Security, World Economic Forum

The Cyber Express Cybersecurity Person of 2024 (META): Woman

The Cyber Express Cybersecurity Diversity and Inclusion Advocates of 2024

Yana Li
WebBeds

Dina AlSalamen
Bank ABC (Jordan)

Rudy Shoushany
DxTalks

Aus Alzubaidi
MBC Group

Saltanat Mashirova
Honeywell

The Cyber Express Infosec Guardians of 2024 (BFSI)

Anthony Sweeney
Deribit

Bipin Mehta
HSBC Bank

Syed Muhammad Ali Naqvi
HBL Bank

Kiran Kumar PG
Alpheya

Ahmed Nabil Mahmoud
Abu Dhabi Islamic Bank

The Cyber Express Infosec Guardians of 2024 (Government & Critical Entities)

Talal AlBalas
from Abu Dhabi Quality and Conformity Council (ADQCC)

Abdulwahab Abdullah Algamhi
UAE ICP

Vinoth Inbasekaran
Dubai Government Entity – Alpha Data

Dr Hamad Khalifa Alnuaimi
Abu Dhabi Police

Dr Saeed Almarri
Dubai Police

The Cyber Express Top Cybersecurity Influencers of 2024

Dr. Mohammad Al Hassan
Abu Dhabi University

Maryam Eissa Alhammadi
Ministry of Interior

Hadi Anwar
CPX

Waqas Haider
HBL Microfinance Bank

Chenthil Kumar
Red Sea International

Nishu Mittal
Emirates NBD

Nisha Rani
Emirates Leisure Retail

The Cyber Express Top Cybersecurity Influencers of 2024

The Cyber Express Top InfoSec Leaders 2024

Mohamad Mahjoub
Veolia Near and Middle East

Ankit Satsangi
Beeah Group

Gokul Vasudev
Dubai Health Authority

Ashish Khanna
SHARAF GROUP

Abhilash Radhadevi
Oq Trading

Prashant Nair
Airtel Africa PLC

Jasim Al Abdouli
Sharjah Cooperative Society

The Cyber Express Top Infosec Entrepreneurs 2024

May Brooks Kempler
Helena

Illyas Kooliyankal
CyberShelter

Kazi Monirul
Spider Digital

Muneeb Anjum
AHAD

Craig Bird
CloudTech24

Zaqiuddin Khan
Tech Experts LLC

Alireza Shaban Ghahrod
Diyako Secure Bow

Loic Falletta
Yinkozi, Ltd

The Cyber Express
Top Infosec
Entrepreneurs
2024

To Wrap Up

As the UAE continues to embrace digital transformation, the country's cybersecurity strategy is evolving to meet new demands. With government initiatives, investments in advanced technologies, and a strong focus on upskilling its workforce, the UAE is laying the groundwork for a strong digital ecosystem.

Events like World CyberCon serve as a catalyst, bringing together industry leaders to share knowledge, inspire innovation, and collectively strengthen the security frameworks that will protect the region's—and the world's—digital future.

Protecting Wind Energy Infrastructure Vital for India’s Energy Security

- By Samiksha Jain

India’s ascent as a global leader in renewable energy is nothing short of remarkable. Standing fourth worldwide in both installed renewable energy capacity and wind power capacity, the country has become a beacon of green energy progress.

With a current installed capacity of 45.887 GW as of March 2024 and a remarkable potential to generate up to 132 GW from onshore wind alone, India’s commitment to renewable energy is both ambitious and clear.

The sector’s appeal to investors is evidenced by a substantial Foreign Direct Investment inflow of $14.12 billion from April 2000 to March 2023, complemented by over $70 billion invested in renewable energy since 2014. India’s impressive standing on the EY Renewable Energy Country Attractive Index and its substantial installed capacity of 532.48 GW from renewable sources underscore the country’s growing influence in this domain. However, despite this progress, only 6% of India’s assessed wind energy capacity has been realized, revealing a vast potential yet to be tapped.

Reliance on China Raises Cybersecurity Concerns

Yet, as India gears up to meet its renewable energy targets, a critical challenge looms large—cybersecurity.

A recent report by Niti Aayog, titled "Domestic Manufacturing Capacity and Potential Cyber Security Challenges in the Wind Sector and Way Forward," casts a spotlight on the urgent need for fortified security measures. With a significant portion of wind turbine components imported from China, the vulnerabilities inherent in these systems present a pressing risk to the nation's energy infrastructure.

The report highlights that while India races to expand its wind energy sector, it must concurrently address these cybersecurity threats to protect its investments and maintain its competitive edge against global players like China, which dominates 61% of the world's wind turbine assembly capacity.

As the wind sector's expansion accelerates, safeguarding this critical infrastructure from cyber threats has become paramount.

In this article, we will delve into the critical intersection of India's booming wind energy sector and the escalating cybersecurity challenges it faces.

We'll explore the vulnerabilities that threaten this vital sector, the implications for India's energy strategy, and the necessary steps to fortify its defenses against the backdrop of a rapidly evolving digital landscape.

Cybersecurity Threats Facing the Wind Sector

The integration of digital technologies in wind farms—ranging from advanced monitoring systems to automated controls—has revolutionized the way wind energy is harnessed. These innovations promise significant improvements in efficiency, predictive maintenance, and overall operational reliability. However, they also introduce a myriad of cybersecurity risks.

As wind turbines and associated infrastructure become increasingly interconnected through digital networks, the attack surface for cyber threats expands, making them more susceptible to malicious activities.

Future of Data Protection with AI

Without a doubt, AI will continue to play a profound role in data privacy and protection, where future developments of AI technology will expand its current capabilities and use cases that offers more advanced and efficient data security solution.

Emerging technologies such as Fully Homomorphic Encryption (FHE) is the next breakthrough technology, where we could process encrypted data without decryption.

Another revolutionary technology is a sub-category of encryption such as Secure Multi-Party Computation (SMPC), its purpose is to secure digital assets and protect information whilst being distributed to multiple parties, without revealing the information in transit.

These emerging technologies hold promise in preserving data anonymity and privacy while allowing collaborative efforts to continue. However, policymakers must update existing regulations to address these novel technologies, ensuring that privacy concerns remain at the forefront.

Types of Threats

1. **Hacking and Data Breaches:** Wind energy systems, often connected to larger power grids, are prime targets for hackers seeking to exploit vulnerabilities. Unauthorized access to control systems or data repositories can lead to operational disruptions or manipulation of critical functions.

2. **Ransomware:** This form of attack involves encrypting vital data or locking down systems until a ransom is paid. Ransomware attacks can incapacitate wind farms, disrupting energy production and compromising critical operational data.

3. **Insider Threats:** Employees or contractors with access to sensitive systems may pose a risk if they exploit their access for personal gain or are manipulated by external attackers.

The wind sector's reliance on imported components, particularly from countries like China, introduces additional cybersecurity challenges. Key issues include:

- **Data Sovereignty:** Many Original Equipment Manufacturers (OEMs) have data collection servers located outside India. This poses risks related to data privacy and control, as sensitive information may be exposed to foreign jurisdictions.

- **Unauthorized Updates:** The potential for unauthorized updates or modifications to wind plant devices by OEMs can introduce vulnerabilities into the operational technology. Such breaches could compromise the integrity and security of power system networks.

Compromised Supply Chains: The global nature of wind energy component supply chains can lead to security gaps if components are not thoroughly vetted or if cybersecurity standards are not uniformly enforced across suppliers.

.

The High Stakes of Cyberattacks on Wind Energy

The potential consequences of a cyberattack on the wind energy sector are far-reaching, threatening not just operational efficiency but also the safety, financial stability, and overall reliability of the power grid.

One of the most immediate impacts is operational disruption. In the event of a successful cyberattack, essential systems responsible for monitoring and controlling wind turbines can be compromised, leading to a complete halt in energy production.

For example, in 2019, a ransomware attack severely disrupted the power utility systems in Telangana and Andhra Pradesh.

The interconnected nature of their computer systems allowed the malicious software to spread quickly, causing a full shutdown across both states' power systems. Such disruptions can cripple energy supply, affecting millions of consumers and leading to costly downtime for the affected utility providers.

Cyberattacks also pose significant safety risks. Wind turbines and other renewable energy assets are complex machines operating under harsh conditions. If hackers gain control of these systems, they could manipulate operational settings, potentially causing malfunctions or accidents. For instance, an attacker might disable critical safety mechanisms or overload the grid, putting workers and nearby communities at risk of physical harm.

In addition to operational and safety concerns, financial losses can be devastating. A prime example is the ransomware attack on the Uttar Haryana Bijli Vitran Nigam (UHBVN) in Haryana. Hackers stole customer billing data and demanded Rs.1 crore (approximately $10 million) as ransom. Beyond the immediate ransom demand, such breaches can erode public trust, result in legal liabilities, and necessitate costly recovery efforts. Moreover, wind energy companies often operate under tight margins, and any prolonged downtime or loss of customer data can lead to significant revenue loss.

These examples highlight the severe consequences of cyberattacks on the wind sector, reinforcing the need for stringent cybersecurity measures to protect this critical infrastructure. Without adequate protection, the risks to operational continuity, financial stability, and human safety are immense.

Current Cybersecurity Measures in India's Wind Sector

India is stepping up its efforts to protect the wind energy sector against cyber threats with the introduction of the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2024. These new regulations aim to strengthen the cybersecurity framework for India's power sector, including wind energy, amidst rising global cyberattacks on critical infrastructure.

Developed under Section 177 of the Electricity Act of 2003, the regulations mandate comprehensive cybersecurity measures across the power sector. They outline stringent requirements for generating firms, transmission and distribution licensees, and other relevant entities to safeguard their operations from cyber threats. The regulations aim to enhance the resilience of India's energy systems, with a specific focus on wind energy infrastructure. Given the sector's rapid digitalization and automation, the new cybersecurity rules address vulnerabilities that could otherwise be exploited by hackers.

Key provisions of the proposed regulations include establishing a dedicated Computer Security Incident Response Team (CSIRT) for the power sector. This team will collaborate with national cybersecurity agencies like CERT-In and NCIIPC to develop security frameworks, incident response procedures, and crisis management plans. Additionally, the regulations require organizations to appoint Chief Information Security Officers (CISO) to oversee cybersecurity efforts, ensuring that key roles are filled by individuals with the expertise to protect critical national infrastructure.

Organizations will also be required to maintain Cyber Crisis Management Plans (CCMPs), which will be crucial for addressing cyber incidents. These plans will outline procedures for quick identification and remediation of potential threats, ensuring that wind energy operations remain secure. Furthermore, the draft introduces a 'Trusted Vendor System,' ensuring that all ICT equipment used in the sector is sourced from verified, secure suppliers, thus mitigating risks associated with supply chain vulnerabilities. The draft regulations have been made available for public consultation, with stakeholders invited to submit feedback by September 10, 2024. Once finalized, these regulations will take effect six months after their publication, marking a significant step towards strengthening India's cybersecurity posture in its renewable energy sector.

Recommendations for Enhancement

A recent report by Niti Aayog's has put forth several recommendations to enhance the cybersecurity of India's wind energy infrastructure, addressing vulnerabilities from data management to policy regulations.

Data Collection Servers Outside India: A Major Concern

One of the primary vulnerabilities lies in the location of Original Equipment Manufacturers' (OEMs) data collection servers, many of which are outside India. These external data centers create significant risks for power system networks, especially when OEMs update the operating software of wind plant devices without obtaining permission from the grid operators or the Ministry of New and Renewable Energy (MNRE). This practice opens up the possibility of unauthorized access, increasing the threat of malicious cyber activities.

Certification and Approval of Foreign-Origin Technology

To mitigate these risks, the report emphasizes the need for thorough certification and approval processes for all intellectual property rights (IPRs), software, and hardware from foreign-origin OEMs. It is recommended that the Central Electricity Authority of India (CEA), the Ministry of Electronics and Information Technology (MeitY), and the Standardization Testing and Quality Certification (STQC) take on the role of ensuring that all technology used in wind energy operations complies with national security standards.

Relocating Data Centers to India: A Critical Move

A major policy shift recommended in the report is the relocation of data and research centers of all wind sector OEMs to India. The establishment of local data centers would not only ensure greater control over sensitive data but also align the sector with India's data sovereignty goals. The MNRE has been urged to set strict timelines for this relocation, with non-compliance leading to the exclusion of such OEMs from participating in future tenders or supplying equipment within the country.

Appointment of CISOs: A Key to Ensuring Compliance

Another essential recommendation is the appointment of Chief Information Security Officers (CISOs) within every utility, specifically residing in India. These officers would be responsible for maintaining cybersecurity standards and reporting compliance to a proposed independent agency that would oversee cybersecurity for the entire power sector. This move is aimed at establishing a standardized security protocol across all wind energy operations.

Strengthening Cybersecurity Protocols and Industry Collaboration

The report also highlights the need for stronger cybersecurity protocols at wind farms, recommending the implementation of more stringent security measures for digital systems and networks. Industry collaboration and information sharing between stakeholders are vital to improving the sector's defenses against cyber threats. By working together, wind energy operators, regulators, and cybersecurity experts can create a more robust and unified approach to managing risks.

Training and Awareness: Building a Culture of Security

Finally, the report highlights the importance of regular cybersecurity training for personnel involved in wind energy operations. Raising awareness about potential threats and equipping staff with the knowledge to detect and respond to cyber incidents are crucial steps in reducing vulnerability. A proactive approach to training can ensure that employees are prepared to act swiftly in the event of an attack, minimizing damage and downtime.

The relocation of data centers, appointment of dedicated CISOs, and strengthened cybersecurity protocols aren't just policy suggestions—they are critical for the future of India's renewable energy ambitions. Now is the time for bold action, collaboration, and unwavering commitment to securing the lifeblood of India's clean energy revolution.

GOVERNANCE

Cyberattacks on Critical Infrastructure: A Ticking Time Bomb

- By Ashish Khaitan

In today's world, it's hard to miss the constant buzz about cyber threats, especially when they hit critical sectors like energy, healthcare, and transportation. These attacks are not just increasing in number; they're becoming more sophisticated, making it crystal clear that we need to step up our defenses.

Take recent events, for example. In February, the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and FBI teamed up with their partners to issue a serious warning. They alerted key infrastructure sectors about potential cyber threats, drawing attention to vulnerabilities that had already been exploited by cyber operations linked to the People's Republic of China (PRC).

And it's not just happening in the U.S. a cyberattack on a nuclear facility in the UK recently showed us how high the stakes can be when it comes to protecting our infrastructure. Yet, despite all the alarms and awareness, there's still a huge gap in both legislation and international cooperation on cybersecurity.

The Dire Need for a Better Global Cyber Treaty

The current state of cybersecurity for critical infrastructure is fragmented, with a patchwork of regulations and standards that often fail to address the complexities of modern threats. Although the United Nations adopted voluntary norms in 2015, their impact has been limited.

Cyber incidents targeting infrastructure have reportedly doubled between 2020 and 2022, according to the International Energy Agency, highlighting the inadequacy of the current response framework.

To address this pressing issue, the international community should consider establishing a global cyber treaty specifically focused on enhancing the protection of critical infrastructure. Such a treaty could build on existing frameworks, introducing binding measures that would elevate global cybersecurity standards.

Currently, the cybersecurity regulatory environment comprises a mix of federal laws, industry standards, and sector-specific guidelines. However, none of these regulations provide comprehensive coverage for all critical infrastructure sectors.

Health Insurance Portability and Accountability Act (HIPAA): This federal law is crucial for safeguarding medical information, requiring healthcare providers and their associates to implement security measures to protect patient data. Despite its importance, HIPAA's scope is limited to the healthcare sector and does not extend to other critical infrastructure areas.

Cybersecurity Maturity Model Certification (CMMC): Designed for defense contractors working with the Department of Defense (DoD), the CMMC ensures these entities adhere to specific cybersecurity standards. However, its applicability is restricted to defense-related contractors, leaving other sectors without comparable protections.

Payment Card Industry Data Security Standard (PCI DSS): This industry standard, adopted widely across states, sets security requirements for entities handling credit card data. Yet, PCI DSS does not encompass critical infrastructure sectors beyond financial transactions.

Communications Assistance for Law Enforcement Act (CALEA): Enforced by the Federal Communications Commission (FCC), CALEA mandates telecommunications companies to facilitate lawful interception of communications. However, CALEA's focus on law enforcement does not address broader cybersecurity concerns.

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP): NERC CIP guidelines are instrumental in securing the electric grid from cyber threats. Nonetheless, they are sector-specific and do not extend to other critical infrastructure areas such as transportation or manufacturing.

Despite these existing frameworks, there is no central, comprehensive approach to cybersecurity across all critical infrastructure sectors. This fragmented regulatory environment often results in gaps that cyber adversaries can exploit.

The Case for a Unified Cybersecurity Framework

The need for a more integrated regulatory approach is not only important but has become the need of the hour. Centralized regulations could establish a baseline for security practices, encouraging organizations to develop and refine their cybersecurity strategies.

This would address common vulnerabilities and foster innovation in security measures. For instance, the Zero Trust model, which manages interactions between people, data, and systems to mitigate security risks, has emerged in response to the need for better security in increasingly parameterless networks.

Centralized regulations could also standardize security practices across supply chains, reducing vulnerabilities that arise from interconnected business operations. By ensuring that all parties adhere to the same security protocols, organizations can better manage and mitigate risks. This approach would not only enhance security but also build trust among stakeholders, including consumers and supply chain partners.

The current threat system highlights the need for better regulatory frameworks. Online threats such as Advanced Persistent Threats (APTs) and the convergence of IT and Operational Technology (OT) systems pose significant challenges.

Convergence of IT and OT Systems: The integration of IT and OT systems has expanded the attack surface for critical infrastructure. Systems like industrial control systems (ICS) and supervisory control and data acquisition (SCADA) are now vulnerable to cyber threats that were previously limited to IT networks.

This convergence highlights the need for integrated cybersecurity frameworks that address both IT and OT environments.

Advanced Persistent Threats (APTs): APTs are sophisticated, often state-sponsored attacks aimed at high-value targets over extended periods. Addressing APTs requires advanced detection and response capabilities, as well as continuous monitoring and threat intelligence. Regulations that mandate these capabilities could help organizations better defend against such sophisticated attacks.

Internet of Things (IoT) and Legacy Systems: The proliferation of IoT devices introduces additional security challenges, as many are designed with minimal security controls. Moreover, critical infrastructure often relies on legacy systems that were not designed with modern cybersecurity threats in mind. Updated regulatory standards are needed to address these vulnerabilities.

Global Perspectives and Recommendations

Given the global nature of cyber threats, international cooperation is essential for protecting critical infrastructure. A global cybersecurity treaty focused on critical infrastructure could help establish universal standards and norms. Such a treaty would provide a framework for responding to cross-border cyber threats and build on existing frameworks, like the UN's guidelines on responsible state behavior in cyberspace.

Enhancing public-private partnerships is also crucial. Collaboration between government agencies, industry stakeholders, and cybersecurity experts can lead to more effective security measures and facilitate the sharing of threat intelligence. Initiatives such as the Cybersecurity and Infrastructure Security Agency (CISA) and Information Sharing and Analysis Centers (ISACs) play a vital role in fostering this collaboration.

Moreover, promoting innovation in cybersecurity is essential for staying ahead of emerging threats. Investing in research and development for new security technologies and fostering collaboration between researchers, developers, and industry practitioners can drive the development of advanced security solutions.

To Sum Up

As we navigate the complexities of our digital world, upgrading cybersecurity standards for critical infrastructure is more urgent than ever. The recent spike in cyberattacks on energy grids, healthcare systems, and transportation networks exposes a troubling stagnation and insufficiency in our current defenses.

While frameworks like HIPAA, CMMC, and PCI DSS exist, they fall short of covering all critical sectors comprehensively. The fragmented nature of today's cybersecurity landscape leaves dangerous gaps, especially as technology advances and threats become more sophisticated.

To truly tackle these challenges, the international community needs to push for a unified global cyber treaty. Such a treaty could bring a cohesive approach to protecting critical infrastructure, establish universal standards, and enhance global cooperation.

By aligning our efforts, standardizing practices, and encouraging innovation, we can build a stronger, more resilient cybersecurity strategy capable of standing up to the evolving threats of the digital age.

IT-OT Convergence: A Cybersecurity Double-Edged Sword

- By Krishna Murthy

In today's fast-paced industrial landscape, the lines between Information Technology (IT) and Operational Technology (OT) are blurring more than ever before. Companies are increasingly merging their IT and OT systems to boost efficiency, streamline operations, and harness the power of data for better decision-making. But while this integration offers numerous benefits, it also introduces a host of cybersecurity challenges, especially for critical infrastructure.

So, what exactly are IT and OT systems? Think of IT systems as the backbone of your business operations, handling everything from data security to network management and software applications. Meanwhile, OT systems are the unsung heroes of the industrial world, managing the physical processes and devices that keep things running smoothly.

Traditionally, these two worlds have operated separately, with OT systems often isolated from IT networks and requiring their own unique security measures. However, as they converge, safeguarding these systems becomes a critical priority.

The Growing Interconnectedness of IT and OT

The increasing adoption of technologies such as the Internet of Things (IoT), cloud computing, and big data analytics has blurred the lines between IT and OT systems. As these technologies are integrated into industrial operations, IT and OT systems become more interconnected, expanding the attack surface for potential cyber threats.

According to a report published by Virtue Market Research, the Global IT/OT Convergence Market was valued at $96.34 billion in 2022 and is projected to reach a market capitalization of $280.66 billion by 2030.

Cybersecurity Implications

The convergence of IT and OT systems presents several cybersecurity challenges:

- **Increased Attack Surface:** The interconnectedness of IT and OT systems creates a larger attack surface, making it easier for cybercriminals to gain access to critical infrastructure.
- **Vulnerabilities in OT Systems:** OT systems are often less secure than IT systems due to their focus on reliability and availability rather than security. They may have outdated software, lack of encryption, and limited visibility into network traffic.
- **Impact on Critical Operations:** A successful cyberattack on critical infrastructure can have devastating consequences, including service disruptions, financial losses, and threats to human safety.
- **Supply Chain Risks:** The convergence of IT and OT systems also introduces new supply chain risks. Vulnerabilities in third-party components or software can be exploited to compromise critical infrastructure.

Addressing the Cybersecurity Challenges

To mitigate the cybersecurity risks associated with the convergence of IT and OT, organizations must adopt a comprehensive approach that includes:

- Risk Assessment: Identify critical assets and vulnerabilities in the IT and OT environments.
- Segmentation: Isolate OT networks from IT networks to limit the spread of malware.
- Patch Management: Regularly update and patch both IT and OT systems to address known vulnerabilities.
- Access Controls: Implement strong access controls to restrict unauthorized access to critical systems.
- Monitoring and Detection: Use advanced security tools to monitor network traffic and detect suspicious activity.
- Incident Response Planning: Develop a comprehensive incident response plan to address cyberattacks effectively.
- Employee Training: Educate employees on cybersecurity best practices and the risks associated with the convergence of IT and OT.

The Role of Collaboration and Partnerships

Addressing the cybersecurity challenges of IT and OT convergence requires collaboration between different stakeholders. Governments, industry organizations, and technology providers must work together to develop best practices, share information, and foster a culture of cybersecurity awareness.

Case Studies

To illustrate the real-world impact of the convergence of IT and OT, let's examine a few case studies:

- Stuxnet Worm: This sophisticated malware targeted Iranian nuclear facilities in 2010, demonstrating the potential for cyberattacks to disrupt critical infrastructure.
- WannaCry Ransomware: This ransomware attack in 2017 affected numerous organizations worldwide, including hospitals and transportation systems, highlighting the vulnerability of interconnected systems.
- The Colonial Pipeline Attack: In 2021, a ransomware attack on the Colonial Pipeline, a major fuel supply line in the United States, caused widespread disruptions and fuel shortages.

The Future of IT and OT Convergence

The convergence of IT and OT systems is a trend that is likely to continue. As organizations seek to improve efficiency and gain competitive advantages, they will increasingly integrate these technologies. To ensure the security of critical infrastructure, it is essential to proactively address the cybersecurity challenges associated with this convergence. This includes:

- Cloud Adoption: The increasing adoption of cloud computing can introduce new cybersecurity risks if not properly managed.
- Industrial IoT (IIoT): The widespread deployment of IIoT devices can create a vast attack surface.
- Emerging Threats: Keep up-to-date with the latest cyber threats and vulnerabilities to stay ahead of potential attacks.

The convergence of IT and OT systems presents significant cybersecurity challenges for organizations. By understanding the risks and implementing appropriate security measures, organizations can mitigate the potential consequences of cyberattacks on critical infrastructure.

ROUND UP

A Month of Cyber Resilience: India's Top Cybersecurity Moves and Milestones

As the month wraps up, India's cyber landscape continues to evolve at a rapid pace. With Assam's new National Cyber Forensics Lab setting the stage for enhanced cybersecurity, the country's push to combat digital threats is evident in every corner—from the training of 5,000 cyber commandos to securing critical sectors like power and defense. As data breaches and cyberattacks persist, recent developments such as the new Digital Personal Data Protection Bill and the RBI's Unified Lending Interface show a forward-thinking approach to safeguarding both national infrastructure and individual rights.

Together, these efforts underline India's commitment to building a resilient and secure digital future, with a strong focus on proactive measures and innovation. Let's dive into the key highlights that shaped the country's cybersecurity efforts this month.

Assam Strengthens Cybersecurity with Launch of India's Second National Cyber Forensics Lab

Assam is set to enhance its cybersecurity measures with the launch of India's second National Cyber Forensics Lab (NCFL) at the Lachit Barphukan Police Academy in Dergaon. This new facility is part of a national strategy to strengthen defenses against the rising tide of cyber fraud and improve law enforcement's capabilities in tackling cyber threats. The establishment of the NCFL comes through a Memorandum of Understanding (MoU) between the Assam police and the Indian Cyber Crime Coordination Centre (I4C), which operates under the Ministry of Home Affairs.

Assam's Chief Minister, Dr. Himanta Biswa Sarma, has acknowledged the support from Union Home Minister Amit Shah and Minister of State for Home Affairs Nityanand Rai, highlighting the lab's critical role in enhancing the state's cybersecurity infrastructure. The NCFL will serve as a vital resource for investigating and prosecuting cybercrimes, thereby bolstering Assam's response to the increasing challenges in digital security.

Read More

India to Train 5,000 Cyber Commandos to Combat Rising Cyber Crimes

On September 10, 2024, India's Home Minister Amit Shah unveiled a major initiative to combat the country's rising cybercrime, announcing plans to train 5,000 cyber commandos over the next five years. This specialized force will be drawn from police units across states, Union Territories (UTs), and central police organizations.

The cyber commandos will be tasked with protecting IT networks, conducting investigations in cyberspace, and addressing cybersecurity needs within government and law enforcement agencies. Their role will extend beyond responding to cyberattacks, focusing on proactive threat identification and prevention to enhance India's overall digital security.
Read More

India Earns Tier-1 Rank in Global Cybersecurity Index 2024

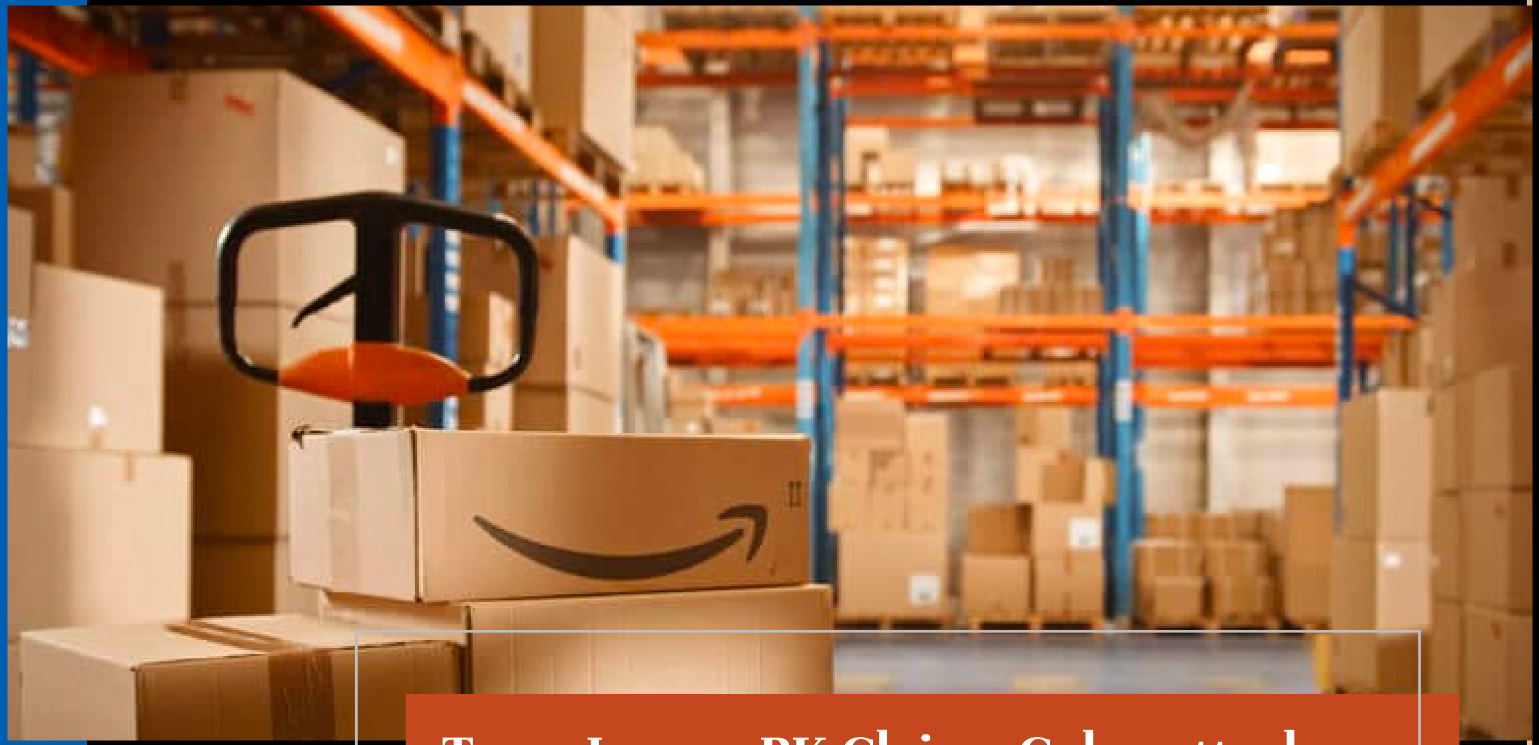
India has secured a place in the Tier-1 category of the Global Cybersecurity Index (GCI) 2024, marking its position among the 47 nations recognized for strong cybersecurity practices. With a score of 98.49, India's achievement reflects its comprehensive approach to cybersecurity, evaluated across five critical pillars: legal, technical, organizational, capacity development, and cooperation.

The GCI report highlights India's legal framework as a standout feature, with key laws like the Information Technology Act (2000) and its amendments, as well as the Digital Personal Data Protection Bill (2022), playing a pivotal role in combating cybercrime, protecting critical infrastructure, and ensuring data privacy. These measures underscore India's commitment to strengthening its cybersecurity landscape on a global scale. Read More

Alleged Durex India Data Breach Exposes Customer Details

Durex India, the Indian division of the renowned British condom and personal lubricants brand, has reportedly suffered a significant data breach, exposing sensitive customer information. The breach was discovered in late August 2024 and involved a flaw in the company's order confirmation page, allowing access to personal details such as full names, phone numbers, email addresses, shipping addresses, ordered items, and payment details.

Security researcher Sourajeet Majumder uncovered the issue, highlighting that hundreds of customers were potentially impacted due to the brand's inadequate security measures. The incident raises serious concerns about data privacy, particularly given the sensitive nature of the products purchased. While the extent of the breach remains unclear, it underscores the critical need for stronger cybersecurity practices in handling consumer data. Read More



Team Insane PK Claims Cyberattack on Amazon India

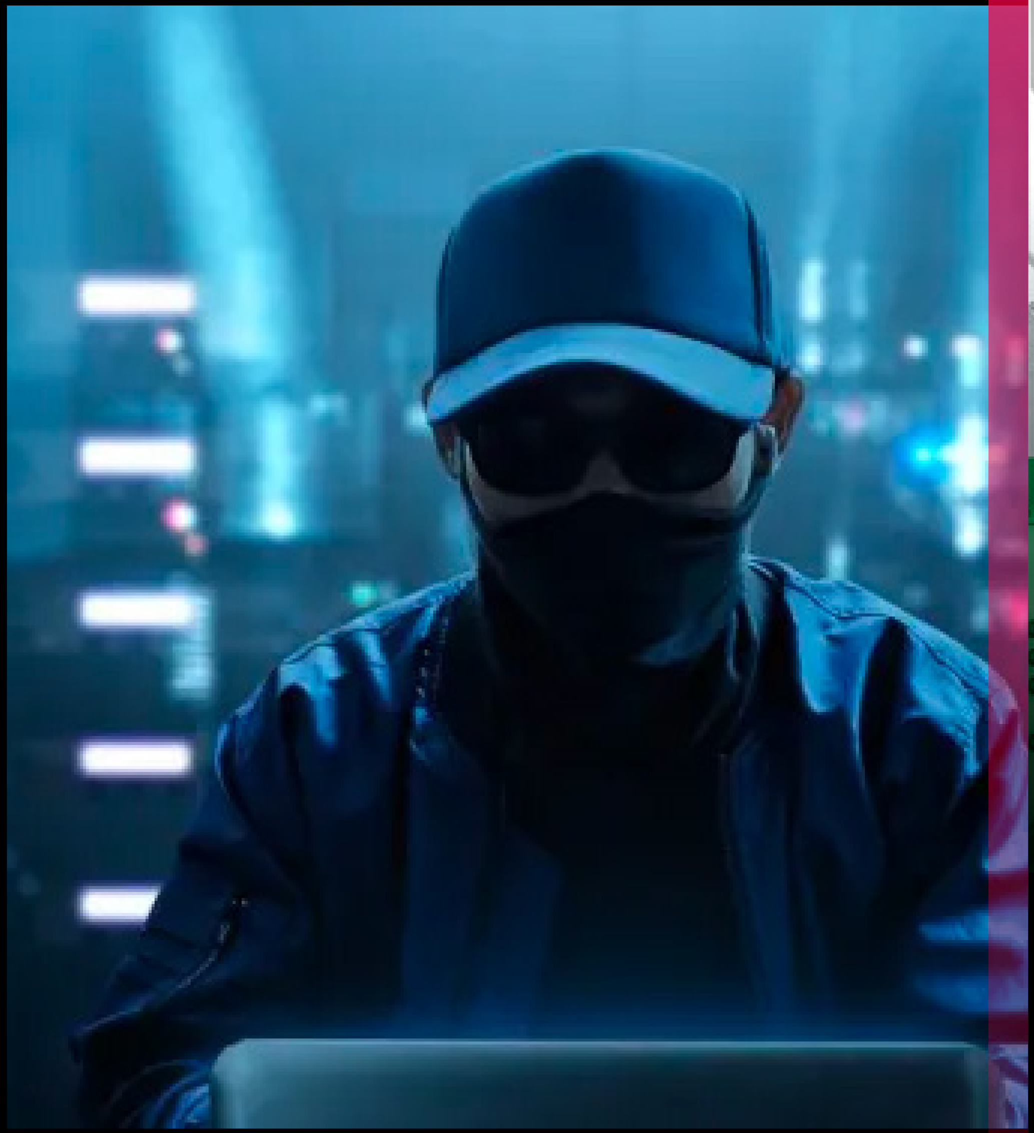
The hacker group "Team Insane PK" made headlines with claims of a successful cyberattack on Amazon India. Announcing their purported breach via Telegram, the group posted a message declaring they had taken down India's largest online shopping site, accompanied by a screenshot suggesting a disruption of the Amazon India website. Despite these bold assertions, both the Amazon India website and its shopping app remained fully operational throughout the period in question.

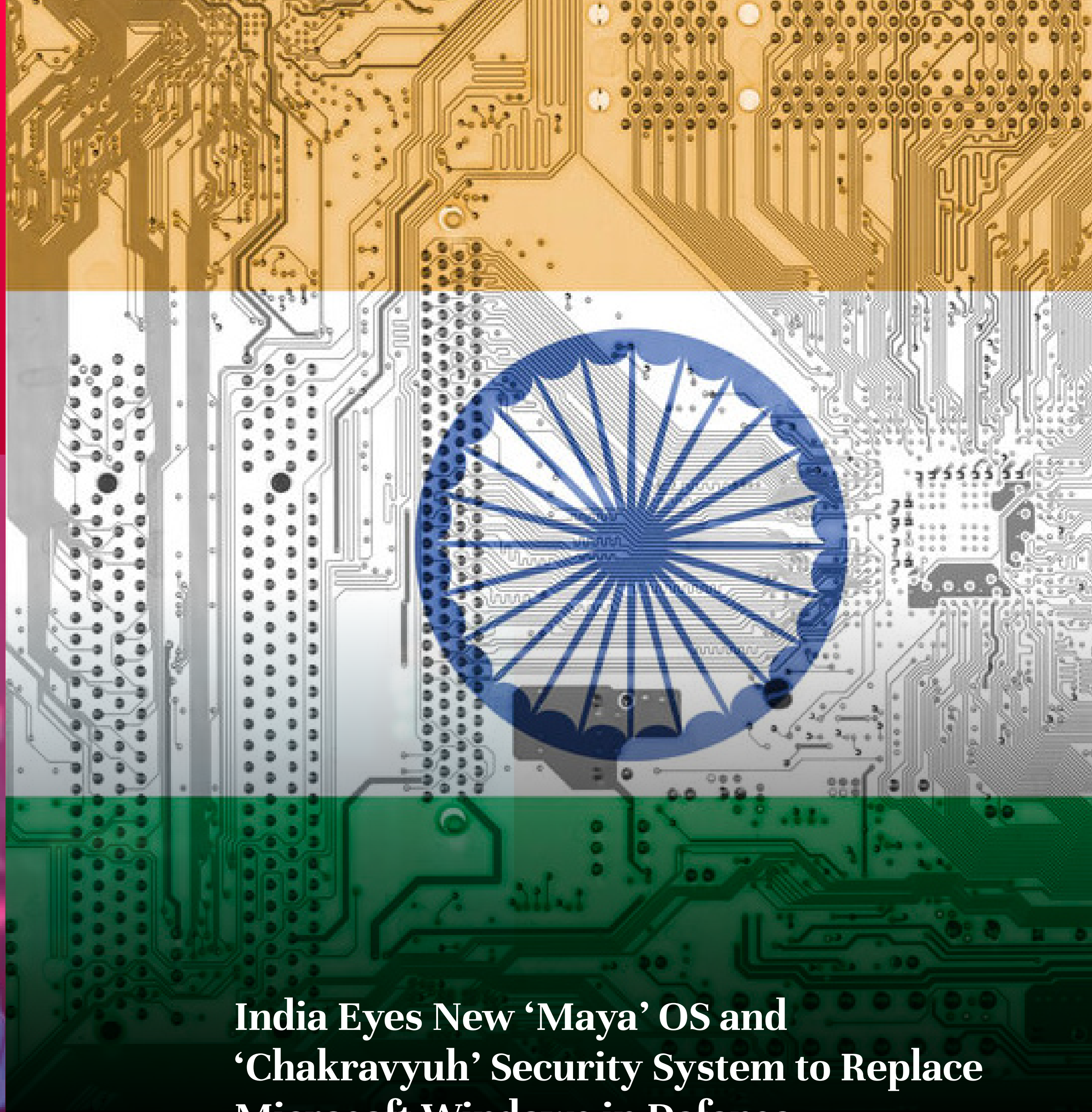
To enhance their claims, Team Insane PK included a "Check Host" link for users to verify the site's status. As of now, The Cyber Express has reached out to Amazon for confirmation but has yet to receive an official response, leaving the legitimacy of the attack claims unresolved. Read More

Telangana Cyber Police Refund ₹85 Crore to Fraud Victims

In a drive to support cybercrime victims, the Telangana Cyber Security Bureau (TGCSB) recovered and refunded ₹85.05 crore (approx. $10.13 billion) between March and July 2024. This initiative spanned across all commissionerates and districts in the state of Telangana, India. To facilitate these refunds, the TGCSB partnered with the Telangana State Legal Services Authority (TGLSA), addressing the growing number of cybercrimes that left citizens with significant financial losses.

A key factor in these recoveries was the quick response from victims, who reported fraud within the critical "golden hour," enabling authorities to act swiftly. Additionally, the Bureau faced challenges with registering cybercrime complaints through India's National Cyber Crime Reporting Portal (NCRP), further highlighting the need for streamlined processes. Read More





India Eyes New 'Maya' OS and 'Chakravyuh' Security System to Replace Microsoft Windows in Defense

India is reportedly making a significant move away from Microsoft Windows, with plans to adopt a new operating system called "Maya" for its Defense Ministry. This transition, aimed at bolstering digital security, also includes the integration of "Chakravyuh," an advanced endpoint detection and protection system designed to enhance malware and virus defenses. While these security upgrades are widely anticipated, The Hindu notes that the Indian Defense Ministry has yet to officially confirm the shift, leaving room for further developments before a formal announcement is made. Read More

India's Power Sector Gets New Cybersecurity Rules

In response to the growing threat of cyberattacks on critical infrastructure, the Central Electricity Authority (CEA) of India has introduced new regulations aimed at bolstering the cybersecurity of the country's power sector. The Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2024, set to be enforced six months after their publication, represent a significant step toward enhancing the cyber resilience of India's electricity infrastructure. Rooted in Section 177 of the Electricity Act of 2003, these regulations call for stringent cybersecurity measures across the entire electricity industry, including generating firms, transmission, and distribution licensees. This proactive approach addresses the escalating risks faced by essential services worldwide. **Read More**

RBI's Unified Lending Interface Promises Faster, Easier Credit Access Across India

The Reserve Bank of India (RBI) is set to introduce the Unified Lending Interface (ULI), aimed at streamlining credit access for small and rural borrowers across India. Announced by RBI Governor Shaktikanta Das on August 26, ULI is expected to enhance the credit appraisal process much like how the Unified Payments Interface (UPI) transformed digital payments. Currently in its pilot phase, ULI promises to facilitate a smooth, consent-based exchange of digital information between data providers and lenders, including essential data like land records, which often slow down credit approvals. The platform's standardized application programming interface (API) simplifies integration, enabling lenders to quickly access diverse data sources and expedite credit processing. **Read more**

India Advances Digital Rights with New Data Protection Legislation

As India approaches the 77th anniversary of its Independence, it has made a significant leap in digital rights and cybersecurity with the endorsement of the Digital Personal Data Protection Bill 2023 (DPDP Bill 2023). On August 9, President Droupadi Murmu approved the bill, which had already received strong backing from both houses of Parliament—the Lok Sabha on August 7 and the Rajya Sabha on August 9. This endorsement marks a pivotal moment in India's approach to data protection. The DPDP Bill 2023 aims to balance the protection of individual privacy with the need for lawful data processing in an increasingly connected world. It serves as both a shield for personal data and a guide for its necessary use, embodying the principles of safeguarding privacy while accommodating legitimate data needs.

Read More

CYBLE®

AI-POWERED

Comprehensive,
Contextual, and
Near real-time

Threat Alerts

5k+	Malware Operators Tracked
5k+	Threat Actors Monitored 24/7
15k+	Darknet Marketplaces & Apps Monitored
200+	Sensors Deployed Across 35 Countries
3Bn+	Digital Assets Monitored
15Bn+	Web Pages Analyzed Daily
100Mn+	Knowledge Graph of Entities Available & Growing

Combat Threats
Before They Strike

SCAN AND STAY UPDATED WITH
REAL TIME CYBERSECURITY NEWS

To advertise with us, write to: marketing@thecyberexpress.com