INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM AROUND THE WORLD

CLOP RANSOMWARE GANG ADOPTS NEW TACTIC TO PRESSURE VICTIMS

The notorious Clop ransomware gang, from Russia, is redefining its tactics by making use of an extortion strategy that is akin to the ALPHV ransomware gang, which involves deploying a website containing the leaked data of the victim on the clear web. This method aims to facilitate the leaking of stolen data, thereby intensifying pressure on the victims to meet their ransom demands.

Typically, gangs involved in ransomware activities pilfer data from compromised networks before encrypting those files. This stolen data then becomes a leverage for double-extortion attacks, warning victims that their data will be released unless a ransom is paid. Ordinarily, these data leak sites are hosted on the Tor network to evade takedown efforts and interference by law enforcement agencies. However, the Tor network has limitations in terms of accessibility, indexation by search engines and download speeds.

IN THIS NEWSLETTER

To overcome these challenges, the ALPHV ransomware operation, also known as the BlackCat, introduced a novel extortion technique last year by creating websites, on the clear web, to leak stolen data. Clear web sites are hosted on the standard Internet rather than anonymous networks like Tor, enabling easier access without specialized software. This approach also increases the likelihood of search engine indexing and widespread dissemination of the compromised information.

Recent reports reveal that the Clop ransomware gang has adopted a similar strategy. Security researcher Dominic Alvieri, a cyber security analyst and security researcher, informed BleepingComputer, an information security and technology news publication created in 2004 by Lawrence Abrams, that Clop has begun to deploy clear websites to expose data stolen during the MOVEit Transfer data theft attacks. The first victim to fall prey to this tactic was business consulting firm PWC. In this attack the threat actors created a website to leak the company's data in segmented ZIP archives.

Subsequently, the attackers launched websites of other organisation, whom they attacked, on the clear web. These included names like Aon, Ernst & Young (EY), Kirkland and TD Ameritrade. Unlike ALPHV's sophisticated sites, Clop's versions merely provide links to download the compromised data, lacking searchable databases.

While this method intends to intimidate employees, executives and business partners impacted by the data breach, it presents its own set of challenges. Hosting data on the clear web makes it more susceptible to takedown efforts. Currently, all known Clop clear web extortion sites have been taken down. The reason for their removal remains uncertain, but potential causes include enforcement by law enforcement agencies, DDoS attacks, or action by hosting providers and domain registrars.

Considering the ease with which these sites can be dismantled, the viability of this extortion technique is questionable.

CYBERCRIME FORUM DATA BREACH

The notorious Breached cybercrime forum has suffered a significant data breach, leading to the sale of its database. Breached was infamous for hosting, leaking and selling data stolen from hacked data from companies, governments and organizations worldwide. After the arrest of the site's administrator, in March 2023, the forum was shut down, and a new clone called BFv2 was launched by another data breach seller.

Contents of the Breach

The compromised database, which contained 212k records, was exposed, in November 2022. The breach exposed sensitive information or various degrees, including usernames, IP and email addresses, private messages between site members and passwords stored as argon2 hashes.

Sale and Sharing of the Database

As of early August 2023, the database was being sold by a threat actor named 'breached_db_person.' They have shared the database with the Have I Been Pwned data breach notification service to prove its authenticity to potential buyers. This actor claimed to be the only person, apart from the previous administrators, to be in possession of the database.

Impact and Implications

The Breached forum was a hub for cybercriminal activities, hosting a range of platform for a wide array of malicious activities such as hacking, data breaches and the illicit trade of sensitive information. The exposed private messages within the database could potentially reveal sensitive information about the forum members, their activities and previous attacks, they were involved in. The sale of the database presents the risk of exposing incriminating information and operational security lapses of threat actors. Furthermore, this breach highlights the potential vulnerabilities even within the criminal underbelly.

Interest and Potential Consequences

The Breached database holds interest not only for cybersecurity researchers but also for other threat actors and blockchain analytics companies. The private messages could provide valuable insights into various cybercriminal activities and give a peek into how cybercriminals think. The database also contains information about payments made using cryptocurrencies, potentially linking threat actors to criminal activities. Impact of the Breached's compromise on the cybercrime community remains uncertain, but it is possible that its database could be leaked for free in the future, as is common in data breach cases.

ROLE OF CYBERSECURITY IN DIGITAL BANKING

In today's increasingly digitized world, cybersecurity has emerged as a critical requirement across various sectors globally, with a special focus on data protection. Among those sectors, the importance of cybersecurity is paramount, especially in the banking sector. Banks engage in millions of transactions daily and store vast amounts of customer data. Consequently, robust proactive and protective security measures are essential to safeguard banks, against cyberattacks.

The primary goal of cybersecurity in digital banking is to secure customers' assets and confidential data. As the shift towards cashless transactions and digital dependence accelerates, the significance of data protection intensifies. Digital products such as credit and debit cards are extensively used for transactions, necessitating stringent cybersecurity measures.

Cybercrimes in digital banking not only impacts customers but also inflicts a substantial toll on the banks during data recovery efforts. Infrastructural, financial, reputational and data losses are some of the consequences banks face during recovery from disruptions. Financial institutions may also incur significant costs in the process of data recovery.

As the global economy transitions to digital platforms, cybersecurity in banking is gradually becoming a major concern. The unpredictable nature of data breaches and cyber incidents underscores the necessity of a robust cybersecurity culture. The risk landscape demands that banks remain compliant and resilient. Establishing a cybersecurity posture ensures data confidentiality, security and resilience.

The prevalence of cybercrime continues to rise in tandem with increasing digitalization. Banks, with their wealth of sensitive client data, remain prime targets of cyberattacks. As banks venture further into the digital domain to enhance customer service, the urgency of proactively addressing cybersecurity threats becomes paramount. This proactive stance starts with understanding the existing threats and implementing safeguards against them. Below are five of these threats, along with practical strategies financial institutions can adopt to mitigate them.

Phishing Attacks: One of the most common cybersecurity challenges, in the banking sector, are phishing attacks. Hackers employ this method to infiltrate networks/systems, often using malware-laden emails from trusted sources. Phishing attacks on financial institutions witnessed an uptick in the first quarter of 2023.

Trojans: Such attacks involve deceiving their way into secure data. A Banker Trojan appears legitimate until the hacker injects malicious code after the trojan is installed.

Ransomware: This attack mode is one of the most frequent attack modes employed by cyber criminals. Ransomware encrypts an organisation’s critical data, only releasing access upon payment of a ransom.

Spoofing: In this mode of cyberattack, hackers create clone sites mimicking financial websites to target end users.

Efforts to reduce cybersecurity threats in digital banking involves diligently investing in strengthening risk culture, so that it leads to adoption of a robust cybersecurity posture, by the particular institution. Compliance with standards and safeguarding IT infrastructure from internal and external threats becomes an integral part of such a plan.

Best practices and measures

Integrated Cybersecurity Model: Adapting an integrated cybersecurity model streamlines activities and communication across a centralized framework, fostering a holistic approach to governance and information safeguarding.

Data Privacy: Building a data privacy culture with well-defined privacy management and adherence to regulations.

Employment of Artificial Intelligence (AI)/Machine Learning (ML): Leveraging the power of AI and ML technologies for proactive analysis and real-time data security assessment.

Vulnerability Scans and Penetration Testing: Investing in technologies to identify and eliminate unknown vulnerabilities.

Risk Management: Identifying and managing potential risks to maintain business resilience.

Training and Awareness: Prioritizing employee awareness to prevent cyber incidents.
As cyber threats continue to evolve, safeguarding customer data and financial transactions is essential. Bolstering cybersecurity controls through a robust posture is critical for maintaining the integrity and security of banking operations.

CALL FOR GLOBAL COOPERATION TO COMBAT BORDERLESS ONLINE CRIMES

During his participation in the G20 meeting on security and AI, Union Home Minister Amit Shah issued a clarion call for international collaboration in the fight against "borderless" online crimes. Shah emphasized the urgent need for joint efforts to combat cyber-terrorism, online radicalization, illicit sale of personal data and the propagation of misinformation through 'toolkit-based' campaigns. He also underscored the growing trend of targeting critical information, digital public infrastructure, and financial systems. The G20 event witnessed the attendance of 900 delegates from member countries, nine guest nations, and organizations including Interpol.

Shah used the platform to advocate for standardized laws among G20 member nations to effectively counter digital crimes. Speaking at the summit he stated that an integrated and stable approach to cybersecurity policies will facilitate interoperability, increase trust in information sharing, and reduce the gaps in agency protocols and resources.

Drawing from India's proactive efforts to combat cyber threats and attacks, the Union Home Minister emphasized on the necessity for enhanced coordination among cyber agencies globally. He called for a unified reporting mechanism for cyber incidents and cross-border cybercrime investigations, thereby fostering a climate of cooperation to establish a secure and open information and communication technology landscape.

Highlighting India's digital transformation, Shah noted that the country's online user base had expanded to a staggering 840 million users. He pointed out the country's pioneering initiatives, including the 'open access digital public infrastructure' models such as Aadhaar for digital identity and the UPI interface for real-time payments, in fostering the growth of online users. Shah acknowledged the global trend of governments utilizing digital tools for governance and public welfare.

However, Shah acknowledged the dual nature of technology, which brings people closer but also exposes them to risks. He noted the misuse of technology by anti-social elements and global forces to inflict economic and social harm on individuals and governments alike.

Recalling Prime Minister Narendra Modi's assertion that cybersecurity transcends the digital realm to become a matter of national and global security, Shah highlighted the innovative tactics being employed by cyber criminals. He emphasized that terrorists were increasingly utilizing virtual assets for funding, employing darknet to obscure identities and to propagate radical content, by exploiting the metaverse for propaganda, recruitment and training. Shah also identified misinformation campaigns based on toolkits as a burgeoning concern in cyberspace.

The G20 meeting served as a critical platform for the international community to recognize the evolving landscape of digital threats and affirm the necessity for collaborative action to safeguard the integrity and security of the global digital ecosystem.

TECH AND FINANCE LEADERS COME TOGETHER TO TACKLE CYBERSECURITY CONCERNS

In an effort to confront the intensifying wave of cybercrime and white-collar offences, the esteemed Parliamentary Standing Committee on Finance summoned senior officials from tech giants like Google, Apple, Flipkart, Paytm and from financial institutions like Yes Bank, Punjab National Bank and Bank of India, along with officials from the Indian Computer Emergency Response Team (CERT-In).

This gathering was dedicated to dissecting the pressing issue of “Cybersecurity and the rising incidence of cyber/white collar crimes.” During the assembly, representatives from the organizations, that were called for the meeting, provided oral evidence, shedding light on their approaches to combat cyber threats and bolster the nation's cybersecurity infrastructure.

The high-stakes meeting underscored the paramount importance of cybersecurity, given the mounting incidents of cyber and white-collar crimes. In a previous session held earlier in July 2023, the Committee delved into the realm of cybersecurity with a comprehensive focus on industry experts. These experts were grilled by lawmakers on various dimensions of illicit activities, including the concerning trend of fraudulent loan applications.

Notable firms such as Chase India, Razorpay, PhonePe, CRED and QNu Labs were among the contributors in this crucial dialogue. Nasscom, the eminent trade body and chamber of commerce representing the tech industry in the country, also participated actively. The discussions revolved around addressing the worrisome proliferation of fraudulent lending apps.

The Chairman of the Standing Committee on Finance, Lok Sabha MP Jayant Sinha, was at the helm of this high-profile engagement. With a composition of 31 distinguished members, the committee drew on the expertise of 21 Lok Sabha representatives and 10 Rajya Sabha members to tackle these contemporary challenges head-on.

This proactive move resonated with the government's commitment to safeguarding national interests. Earlier in February, the administration took the decisive step of blocking 232 apps operated by foreign entities, notably Chinese, especially those that were implicated in activities such as betting, gambling and unauthorized loan services. The stringent measures included a ban on 138 apps entangled in money laundering, gambling and related misdeeds, as well as 94 apps engaged in unauthorized loan services. These actions were taken to mitigate threats to the country's economic stability.

INDIAN ORGANIZATIONS STRIVE TO BOLSTER CYBERSECURITY

Indian organizations, like their global counterparts, have witnessed the productivity dividends of digital transformation. However, the surge in cyber threats is posing a substantial risk to these digitization endeavours.

Research conducted by Check Point Software Technologies, an American-Israeli multinational provider of software and combined hardware and software products for IT security, revealed that Indian enterprises faced an average of 1,787 cyberattacks per week over the past six months, surpassing the global average of 983. Further a study by TeamLease, a technology professional services platform, pinpoints sectors such as healthcare, education, research and government as being particularly susceptible to cyberattacks.

Ransomware emerged as a common menace, impacting 73% of Indian businesses in 2022, a rate higher than the global average of 66%, according to a recent survey by Sophos, a Britain-based security software and hardware company. Government, education, financial services and manufacturing were identified as the industries most frequently targeted.

Yet, Indian enterprises are not conceding ground to malicious actors. Sakra World Hospital, Bengaluru for instance, has segregated networks, enforced role-based access, incorporated endpoint detection and response mechanisms and implemented zero-trust capabilities within their internal network. The hospital also conducts vulnerability assessments and penetration tests to safeguard its external assets.

In response to the mounting threats against critical infrastructure, the Government of India has undertaken robust initiatives to fortify the nation's cybersecurity posture. Measures include the National Critical Information Infrastructure Protection Centre (NCIIPC) and the National Cyber Coordination Centre, as well as formulation of the National Cyber Security Reference Framework, 2023. This policy empowers critical sectors with strategic guidance on cybersecurity concerns.

According to Cisco's Cybersecurity Readiness Index, approximately 24% of Indian organizations exhibit a "mature" level of readiness to counter cyber threats, surpassing the global average of 15%. With 90% of enterprises expecting security incidents to disrupt operations in the next 12 to 24 months, continued evolution in cybersecurity remains imperative.

ATTACK ON AIIMS DRIVES FORMULATION OF NATIONAL CYBERSECURITY RESPONSE FRAMEWORK

The ransomware assault on the All-India Institute of Medical Sciences (AIIMS), in November last year, has proved pivotal in the creation of a comprehensive national cybersecurity response framework (NCRF), according to insights shared by the former National Cyber Security Coordinator, Lt Gen. (Retd) Dr Rajesh Pant. The incident, which occurred on 23 November 2022, prompted a renewed focus on safeguarding critical infrastructure and paved the way for this strategic framework.

The NCRF delineates a comprehensive architecture for a cyber defence mechanism, complete with guidelines for trusted companies and supply chain mechanisms. In the aftermath of the AIIMS cyberattack, where the institution's systems were compromised resulting in the loss of outpatient and research data, the Delhi Police's Intelligence Fusion and Strategic Operations (IFSO) cell initiated an FIR under cyber terrorism sections. Simultaneously, the National Informatics Centre and the Indian Computer Emergency Response Team (CERT-In) launched investigations into the incident.

The NCRF, Lt Gen. (Retd) Dr Pant asserted, aims to address pivotal gaps in response mechanisms and establish standardized operating procedures for efficient mitigation. Additionally, he emphasized on the necessity of inter-ministerial cooperation and the establishment of a dedicated nodal ministry to effectively combat dynamic cybersecurity threats.

Lt Gen. (Retd) Dr Pant also shed light on the government's cybersecurity strategy, developed during his tenure as the national cybersecurity coordinator, which had been in development since 2020. The strategy proposes an array of mitigation measures to combat data breaches and aligns with the evolving cyber landscape.

As India strides forward in its cybersecurity initiatives, the AIIMS incident stands as a catalyst for reimagining response strategies and strengthening the nation's digital defences.

LT GEN. MU NAIR APPOINTED AS INDIA'S NATIONAL CYBER SECURITY COORDINATOR

In a significant development, Lt Gen. MU Nair, has been appointed as the new National Cyber Security Coordinator (NCSC) of India. He succeeds Lt Gen. (Retd) Dr Rajesh Pant, bringing his wealth of experience and expertise to bolster the country's cybersecurity efforts.

Lt Gen. MU Nair, an alumnus of the esteemed National Defence Academy, takes on the role as the head of the National Cyber Coordination Centre (NCCC). With his appointment, he becomes India’s third cyber security chief, succeeding Lt Gen. (Retd) Dr Rajesh Pant and the inaugural chief, Gulshan Rai.

Having held critical positions including that of the additional director general of signal intelligence, Lt Gen. MU Nair brings a deep understanding of cyber warfare, signal intelligence and communication & information technology, both within India and globally.

The NCCC operates under the National Security Council Secretariat (NSCS) and plays a pivotal role in coordinating cybersecurity-related matters at the national level. Among its functions, the NCCC generates situational awareness of existing and potential cybersecurity threats, issues alerts to relevant agencies during cyberattacks and facilitates enhanced cyber intelligence sharing.

One of the key responsibilities of the NCCC is to screen all forms of meta-data, fostering better coordination between various intelligence agencies and streamlining intelligence gathering processes. Its collaboration with the Indian Computer Emergency Response Team (CERT-In) further strengthens the country's cyber readiness across government, public-private and private sectors.

The appointment of Lt Gen. MU Nair comes at a time when India is witnessing an upsurge in cyber threats and attacks. The NCCC's role becomes pivotal in the face of an increasingly complex threat landscape. It is not only tasked with responding to cyber incidents but also with ensuring proactive measures to safeguard critical information infrastructure.

Under his leadership, Lt Gen. MU Nair is expected to continue driving forward India's cybersecurity capabilities and coordination efforts, working closely with various stakeholders to counter evolving cyber challenges. His expertise in cyber warfare and strategic understanding of cyber threats position him as a valuable asset in enhancing the nation's cyber resilience.

AKIRA RANSOMWARE EMERGES AS A THREAT

The Indian Computer Emergency Response Team (CERT-In) recently issued a warning about a novel ransomware called Akira. The Gurgaon police also raised an alert regarding this newly surfaced cyber threat.

Akira specifically targets computer systems powered by both Windows and Linux operating systems and is known for its capability to spread across networks. According to the government advisory, Akira not only steals personal data but also encrypts it, coercing victims into pay the ransom. In the event of refusal to comply, the ransomware actors threaten to publish the stolen data on the dark web.

WHAT IS AKIRA?

Akira represents a novel ransomware strain that was utilized in cyberattacks against targets in the United States and Canada earlier this year. Distinguishing itself from the Akira ransomware flagged by Microsoft Defender Antivirus in 2017, this iteration of Akira adopts a double-extortion technique to extract money from victims. The ransomware has gained notoriety due to its widespread impact in the US and hence the government's subsequent advisory.

UNIQUE CHARACTERISTICS AND TARGETS

Akira's operational method involves pilfering data from compromised networks, activating encryption, and issuing a ransom demand. It employs PowerShell commands to eliminate Windows Shadow Volume copies (backup copies), rendering data recovery more difficult. Following this, the ransomware encrypts a wide array of data file types and adds the 'Akira' extension to them.

RANSOM AND EXTORTION

Organizations lacking secure data backups are particularly vulnerable to Akira. The ransomware leaves a ransom note in each folder where files are encrypted, initiating a negotiation process for data restoration. The note includes a message outlining the victim's financial position and encourages communication if the organization has cyber insurance.

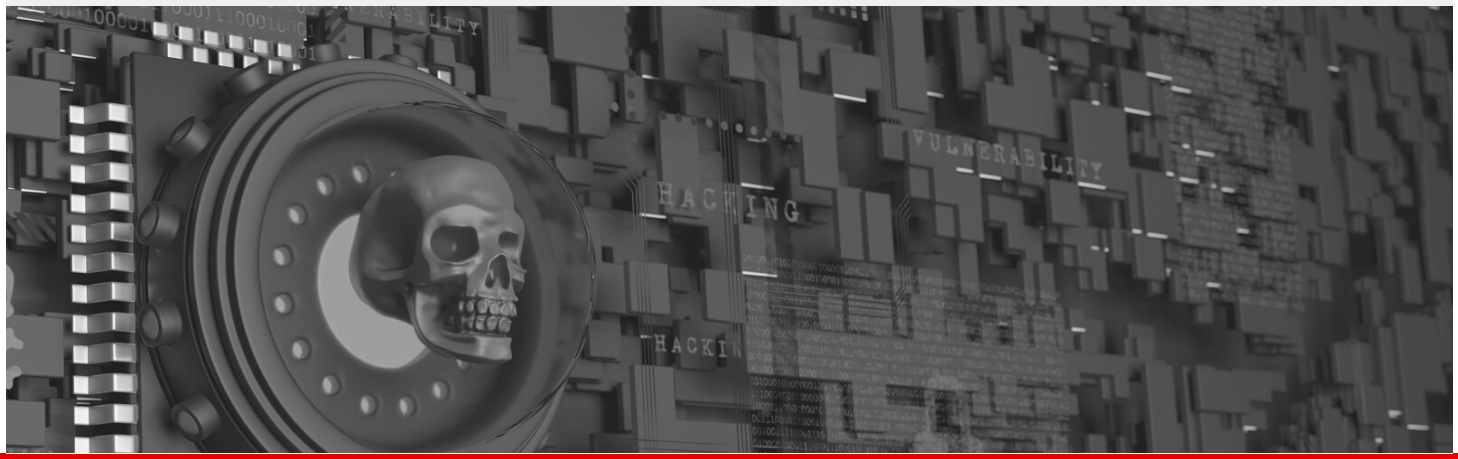
DISTINCTIVE AESTHETICS AND REPORTING

Interestingly, the ransomware's leak site possesses a distinct retro aesthetic, using neon green text on a black background. Rather than conventional dropdown menus, users are expected to input commands. The site also provides a 'news' command, listing victim organizations targeted by the ransomware group.

IMPLICATIONS AND SAFEGUARDS

Akira's effects are far-reaching, leading to data loss, reputation damage and operational disruption. To guard against this threat, organizations should prioritize cybersecurity practices, including regular backups stored offline, automatic software updates, and vigilant avoidance of suspicious links and email attachments.

Should an attack occur, immediate countermeasures involve disconnecting infected devices, isolating external storage and analyzing system logs for suspicious activities.



BLACKBERRY EXPANDS GLOBAL CYBERSECURITY SOFTWARE DEVELOPMENT TO INDIA

BlackBerry Limited has announced expansion of its global software development capabilities by establishing a state-of-the-art cybersecurity hub in India. The hub will be located across two prominent Indian cities, Bengaluru and Noida (Delhi NCR). Both these centres will contribute towards bolstering the company's cybersecurity efforts, in India, and the Asia Pacific (APAC) region.

This expansion follows BlackBerry's previous establishment of an 'IoT Centre of Excellence,' in Hyderabad, earlier this year, which focused on developing embedded software for critical IoT industries. The company is actively leveraging local expertise across various locations to enhance its global software and services teams, with a focus on countering cyberattacks using its cutting-edge Cylance AI technology.

Cylance AI is BlackBerry's advanced cybersecurity software, renowned for pioneering the AI-driven cybersecurity industry. With a seventh-generation iteration, it boasts of the industry's largest malware database, honed through years of real-world operation and trained on diverse threat data sets.

The company aims to onboard more than 100 specialized employees by the end of 2023, focusing on areas such as Generative AI, Machine Learning (ML), data science and analytics, threat intelligence, networks, Unified Endpoint Management (UEM), cloud and software development.

This expansion will complement BlackBerry's existing software and services teams situated in Canada, the United States of America and Europe. It further enhances regional access to BlackBerry's comprehensive suite of cybersecurity software and services, including Cylance AI, 24x7 cyber threat monitoring and mitigation, endpoint management, and real-time threat intelligence.

BlackBerry's decision to expand in India is driven by its data-driven threat intelligence, revealing India as one of the most targeted countries by cyber attackers. This expansion aligns with BlackBerry's strategy to amplify innovation and support for customers across the APAC region.

CYBERSECURITY THREATS SURGE IN INDIA DUE TO DIGITAL TRANSFORMATION

The rapid digital transformation sweeping through India's industries is coming with a significant rise in cyberattacks, posing a critical risk to the nation's economic ambitions. Sectors ranging from manufacturing to pharmaceuticals are facing increased vulnerabilities as they embrace digital operations, according to a subsidiary of Google.

Recent months have witnessed a notable spike in cyberattacks, with Mandiant (owned by Alphabet Inc.'s Google Cloud), reporting a surge in breaches. A breach at Suzuki Motorcycle India led to a production halt in May, while the country's largest drug manufacturer announced in March that a ransomware attack would impact its revenue.

These breaches underscore potential neglect of cybersecurity as India has swiftly built out its digital infrastructure. While the country is aggressively positioning itself as a global player in industries like electronics manufacturing, it is also aiming to provide an alternative to China's manufacturing prowess, which has faced challenges amid tensions with the US.

Ransomware attacks, wherein hackers encrypt files and demand ransoms, increased by 53% in India in 2022, according to a CERT-In report. These attacks have expanded their reach across critical sectors, the report revealed.

Such high-profile incidents have driven up the demand for security software.
The adoption of artificial intelligence (AI) presents both advantages and challenges in the realm of cybersecurity. While AI is being harnessed by security software companies to detect system weaknesses, hackers are also using AI-driven tools to craft more convincing phishing emails and malware code.

INDIA'S GROWING INVESTMENT IN CYBERSECURITY

India is poised to experience a significant surge in its cybersecurity spending, projected to increase by 18% between 2020 and 2025. This growth rate, as reported by Avendus Capital, outpaces other regions, making India a key player in the global cybersecurity landscape.

KEY CATEGORIES OF CYBERSECURITY

Identity and access management, network security and email security are identified as high-potential categories within the cybersecurity sector. The Government of India has established initiatives like Cyber Surakshit Bharat and the National Critical Information Infrastructure Protection Centre to coordinate cybersecurity efforts across the nation.

INDIA-US CORRIDOR: A HUB FOR CYBERSECURITY

India, along with the United States of America, contribute 16% of the world's talent pool in cybersecurity-trained resources, solidifying the India-US corridor as a cornerstone for international cybersecurity outsourcing services. This collaboration bolsters the global cybersecurity ecosystem.

MANAGED SECURITY SERVICES (MSS) AND IOT IMPACT

The report highlights that the managed security services (MSS) market is set to expand at a faster pace compared to the market for professional security services. The rise of IoT-based devices is also noted, with a projection that 75% of global devices by 2030 will be IoT-based.

COST OF DATA BREACHES AND TRENDS

The escalating complexity and frequency of attacks carried out by technologically advanced threat actors have driven up the cost of data breaches. As of 2022, the cost per breach had reached USD 4.4 million. The report also underscores the shift towards cloud-based solutions and the adoption of Zero Trust Architecture for data protection.

INNOVATION AND PARTNERSHIPS

Indian companies are actively engaged in enhancing cybersecurity education and training programmes. Infosys has partnered with Purdue University, USA to provide cybersecurity education to its employees. TCS Cyber Security Practice Unit organizes the 'HackQuest' event for new hires. Wipro is establishing an engineering and innovation hub focusing on engineering solutions, customer experience, and cybersecurity.

PROJECTED MARKET GROWTH

The report forecasts that the cybersecurity services market will reach a size of USD 191 billion by 2028. Global cybersecurity spending is expected to double between 2021 and 2028, reflecting the escalating emphasis on cybersecurity worldwide. As the digital landscape evolves, investments in cybersecurity are becoming a strategic imperative to safeguard digital assets and customer data.

GROWING DEMAND FOR CYBERSECURITY JOBS IN INDIA

The cybersecurity market in India is expected to reach USD3.5 billion by 2027, with an annual growth rate of 8.05%. A study conducted by TeamLease Digital indicates that as of May 2023, there were approximately 40,000 job openings in the cybersecurity industry in India. This demonstrates a substantial demand for skilled cybersecurity professionals. However, there is a notable skill gap of 30%, posing a challenge for the industry.

INCREASE IN CYBER ATTACKS

The study also highlights a rise in global weekly cyber attacks, surpassing 1,200 attacks per week. In Q1 2023, Indian organizations experienced over 2,000 weekly attacks, marking an 18% increase compared to the previous year. The healthcare sector was particularly targeted, accounting for 7.7% of such attacks.

SPECIALIZATIONS AND IN-DEMAND JOB ROLES

The study identifies specific areas of specialization within the cybersecurity field that are in high demand, including data privacy, cloud security, AI security, and network security. In addition to technical expertise, soft skills such as problem-solving, communication, teamwork and collaboration are also essential. The study lists top job roles in cybersecurity, such as IT auditor, Information Security analyst, Network/IT Security Engineer/Specialist, Security Testing/Penetration Tester and Computer Forensics analysts. Entry-level salaries range from INR 3 to 6 lakh per annum, while senior and mid-level professionals with over 12 years of experience can earn between INR 50 to 80 lakh annually.

IMPACT ON CRITICAL SECTORS

The study also underscores the impact of cyberattacks on critical sectors:

Healthcare: India ranks 11th in vulnerability to cyberattacks in the healthcare sector, with 1.9 million reported cyberattacks in 2022. The average data breach cost was 176 million.

Manufacturing: Ransomware accounted for 23% of cyberattacks on companies in the manufacturing sector.

Government: India's share in total cyberattacks on government agencies increased to 13.7% in 2022 from 6.3% in 2021.

Financial Services: Indian banks reported 248 successful data breaches, with public sector banks accounting for 41 cases, private sector banks for 205 cases and overseas banks for two cases.

Retail: 77% of retail organizations experienced ransomware attacks in 2021, higher than the global average of 37%. The ransomware recovery cost in the retail sector was $1.97 million, above the global average of $1.85 million.

INDIA FUTURE FOUNDATION (IFF) HOSTS VIRTUAL DISCUSSION ON BALANCING PRIVACY AND SECURITY IN REGULATING OTT SERVICES

In a bid to address the escalating demand for regulations in the ever-evolving realm of Over-The-Top (OTT) services, IFF organized a virtual discussion titled **"Regulating OTT Services: Balancing Privacy and Security."** The event, held on July 20, 2023, from 12:00 PM to 1:30 PM IST, which delved into the intricate confluence of privacy, security and regulatory requisites within the OTT landscape.

The crux of this discussion lay in the recently issued Consultation Paper by the Telecom Regulatory Authority of India (TRAI), released earlier in the same month. The paper titled **"Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services,"** signalled a critical juncture where the Indian regulatory framework seeks to grapple with the complex ecosystem of OTT platforms.

The consultation paper's fundamental motive was to strike an equilibrium between safeguarding user privacy and ensuring security, while also addressing the need for regulatory measures. With the proliferation of OTT services encompassing streaming platforms and communication apps, the discourse around regulating these services has assumed paramount significance.

This virtual event brought together a distinguished panel of experts who engaged in an in-depth dialogue on two pivotal aspects.

Regulation of OTT Platforms: The panelists delved into the multifaceted aspects of regulating OTT platforms. This aspect encompassed discussions around content censorship, licensing norms, ownership structure and the overarching regulatory mechanisms. Balancing the imperative to regulate content and upholding the fundamental freedom of expression posed a formidable challenge.

User Privacy and Encryption: The second facet revolved around safeguarding user privacy and ensuring end-to-end encryption on OTT platforms. The discourse recognized the pivotal role of end-to-end encryption in preserving communication privacy. However, the necessity to address concerns about potential misuse of encryption for illicit activities within the purview of regulatory requirements posed an intricate puzzle.

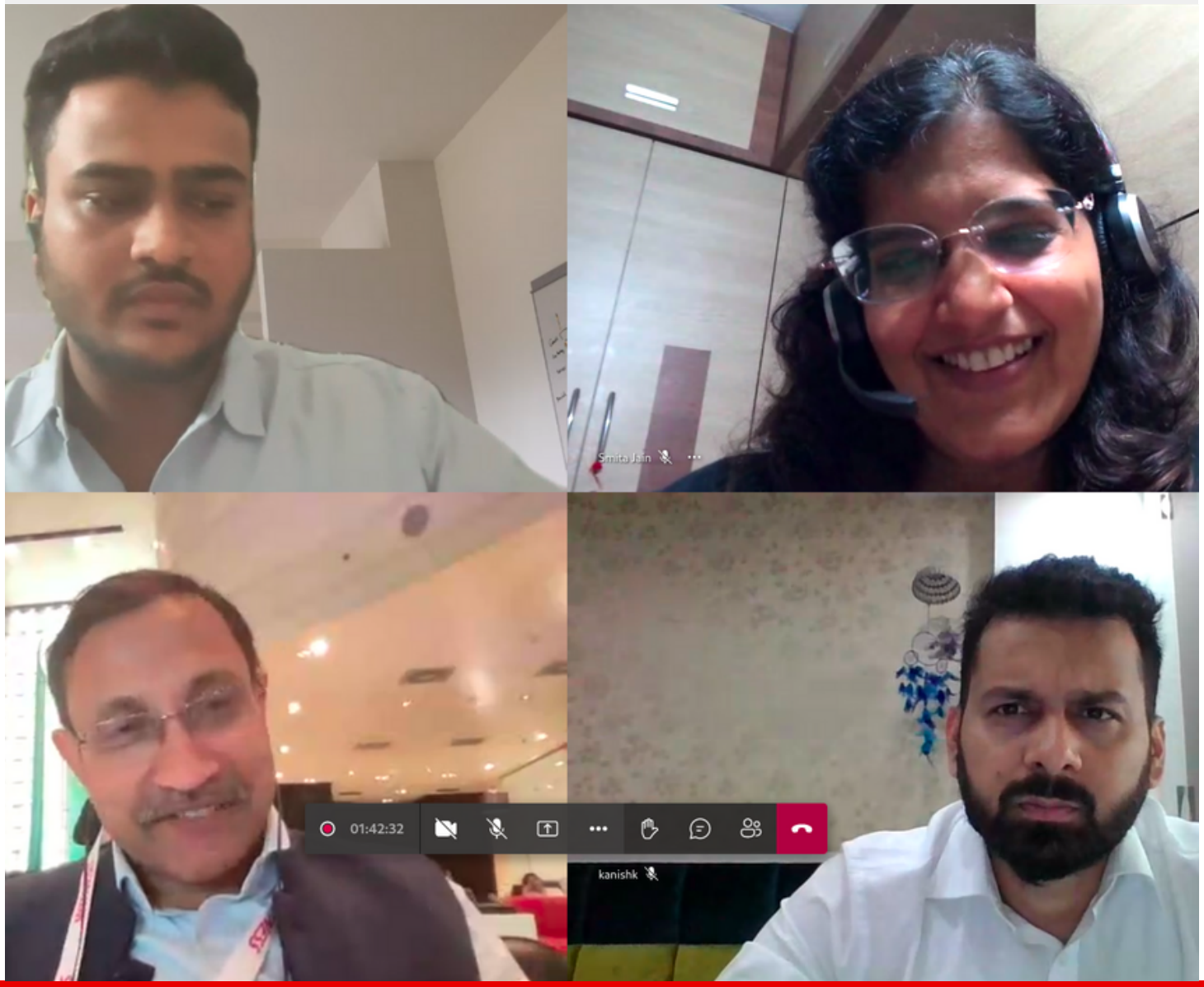
The esteemed panel, comprising industry luminaries and thought leaders, critically analyzed these dimensions, drawing from global regulatory paradigms and technical considerations. The insights shared during the discussion underscored the evolving nature of the OTT landscape and its profound impact on privacy, security and freedom of expression.

CONSULTATION OF THE MONTH

The outcome of this event is poised to influence the contours of regulatory discourse surrounding OTT services in India. As the nation navigates the intricate pathways of regulating the digital sphere, the IFF's initiative stands as a crucial milestone, reflecting a concerted effort to harmonize privacy, security and regulatory imperatives.

IFF's virtual discussion serves as a potent reminder of the intricate challenges posed by the rapid proliferation of OTT services. The insights gleaned from this event will invariably contribute to shaping the future of the regulatory landscape governing the dynamic realm of digital communication services not only in India but also in the broader global context.

This virtual session was attended by **Dr Debabrata Nayak, noted Cyber Security Expert; Dr Shruti Mantri, Associate Director at Indian School of Business, Mr Salil Mittal, Lead Cyber Security - Emerging Technologies at Jio; Anil Batra-Corporate Vice President-Technology at WNS; Kanishk Gaur- CEO, IFF, Rakesh Maheshwari- Member, Advisory Board at IFF; Pankaj Anup Toppo- Head-Policy Programmes & Research and Nikhil Bansal- Deputy Manager at IFF**



INDIA FUTURE FOUNDATION SIGNS MOU WITH ASSAM STATE POLICE

India Future Foundation (IFF), a leading tech think tank in the country, recently signed an MoU with the Assam Police to strengthen the realm of online security. This strategic partnership aims to bolster the cybersecurity capabilities of the state police, focusing on areas such as cybercrime investigation, information security management and cyber forensics.

The MoU was signed in the presence of the Assam Chief Minister, Hemanta Biswa Sarma. The MoU outlines IFF's pivotal role in enhancing Assam Police's adeptness in managing cyber threats. Notably, IFF's involvement will be contingent upon securing requisite approvals from the State Police.

One of the significant initiatives stemming from this collaboration is the establishment of a Digital Learning Lab. This specialized lab will play a dual role, acting as a training ground for cybersecurity skills and an avenue for raising awareness about online security. Mr Kanishk Gaur, Founder, India Future Foundation, expressed his enthusiasm for contributing to the enhancement of the cybersecurity capabilities of the state police and the establishment of the Digital Learning Lab. He emphasized on the positive impact of such endeavours on fostering a safer online environment.

Commenting on the MoU, Gaur stated, "It is indeed an honour to be partnering with the Assam Police for this initiative and contributing towards bolstering their cyber capabilities. We are equally delighted to collaborate with Assam Police in creating a Digital Lab. Educational centers of this nature play a pivotal role towards establishing a secure online space."

Mr Harmeet Singh, Special Director General of Police (Admn/Border), Assam, stressed on the significance of education in combatting cybercrimes and expressed confidence that educational labs, like the one being established, would significantly advance this endeavour.

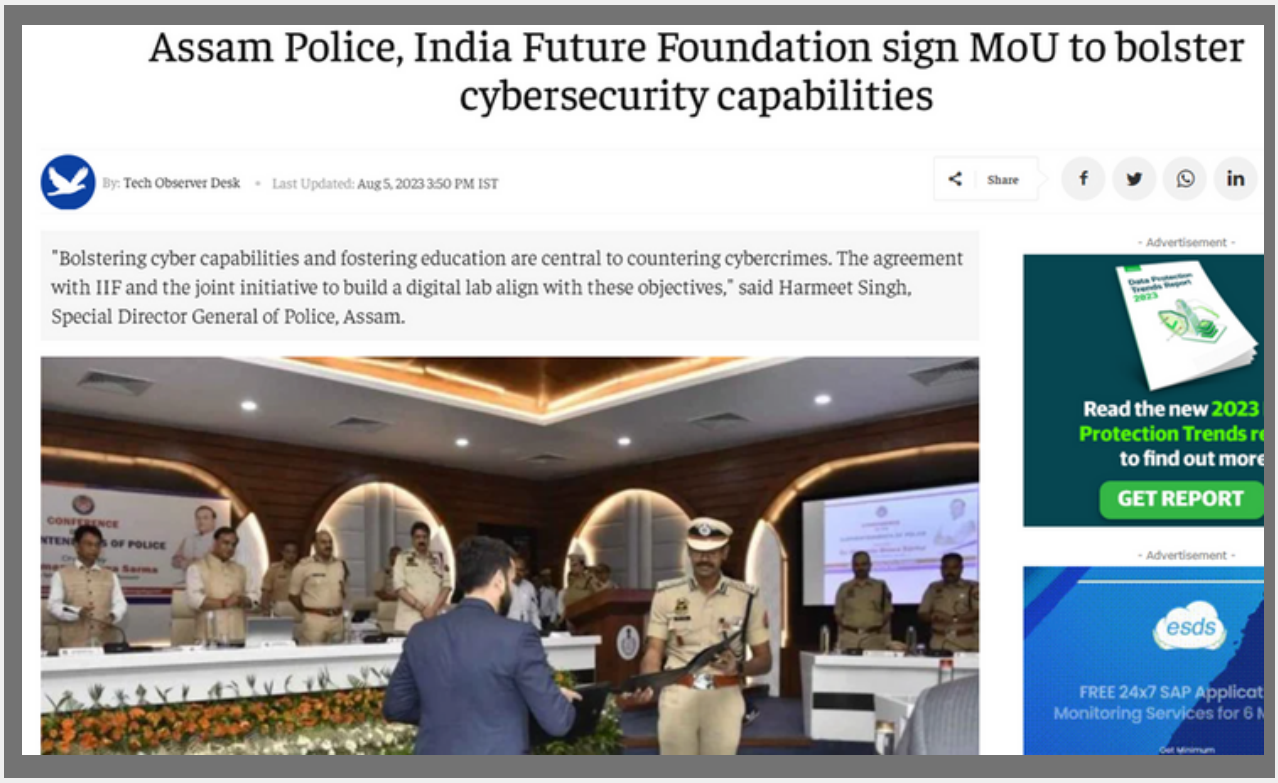
As IFF pioneers this collaborative effort, their commitment to elevating cybersecurity standards is evident. By assisting Assam Police in building a robust Digital Learning Lab, IFF furthers its mission to contribute towards establishing a secure digital landscape in India.

IFF IN THE MEDIA

Kanishk Gaur, CEO of IFF, shared his views on the Transformative Role of CIOs in India on ITNEXT

Insights by Kanishk Gaur, CEO of IFF on The changing face of CISOs in India's Digital Landscape In ITNEXT

Kanishk Gaur, CEO of IFF, shares the blueprint that the Government and Public Sector should adopt to align themselves with the Digital Personal Data Protection Bill, on TechObserver



Assam Police, India Future Foundation sign MoU to bolster cybersecurity capabilities

By: Tech Observer Desk • Last Updated: Aug 5, 2023 3:50 PM IST

Share

"Bolstering cyber capabilities and fostering education are central to countering cybercrimes. The agreement with IIF and the joint initiative to build a digital lab align with these objectives," said Harmeet Singh, Special Director General of Police, Assam.

Kanishk Gaur, CEO of IFF, shares the blueprint that the Government and Public Sector should adopt to align themselves with the Digital Personal Data Protection Bill, on TechObserver

INDIA FUTURE
FOUNDATION

Contact Us

+91-1244045954, +91-9312580816

Building no. 2731 EP, Sector 57, Golf Course Ext. Road, Gurugram, Haryana, India – 122003

helpline@indiafuturefoundation.com

www.indiafuturefoundation.com