INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM THE INDUSTRY

CYBER SECURITY AND THE SPACE RACE : NEW CHALLENGES

With the advent of Anti-Satellite Weapons (ASAT), the possibility of destroying satellites to disrupt the flow of information is posing to be a new challenge in the era of a global space race. The war between Russia and Ukraine has escalated the problem with Russia using various tactics of a hybrid war. This war has seen jamming, GPS spoofing, and other cyberattacks launched against ViaSat and Starlink Internet services in Ukraine.

The attackers have not been involved in damaging the satellite itself, instead, they targeted the services. However, it is noteworthy that countries like China and Russia have used ASATs to destroy their own satellites, drawing criticism from other countries over both security and the prospect of space debris that could damage other satellites in orbit. While no military has launched a missile at the satellite of another country, the way a number of different countries have demonstrated its potential including the USA, means that such attacks against satellites can't be discounted in a future conflict. Further, this warfare can prove to be a vital tool in the hands of the attackers.

IN THIS NEWSLETTER

GEOPOLITICAL TENSIONS AND ITS IMPACT ON CYBERSECURITY IN 2023

The impact of the ongoing conflict between Russia and Ukraine has brought the spotlight on cybersecurity threats to the Critical Infrastructure of nation-states. In this era of nation-state sponsored attacks, we could experience attacks for the sake of disrupting global economies evolving from cyber-attacks that encrypt data and ask for ransom. This poses a direct threat to specific sectors, including energy, shipping, financial services and chip manufacturing. These attacks won't stop at stealing IPs or asking for ransom. Instead, they will focus on proper disruption, compromising or shutting down critical operations on a national scale.

USA BRINGS QUANTUM COMPUTING SECURITY LAW

The Quantum Computing Cybersecurity Preparedness Act progressed through the Senate after companion legislation (a bill introduced in either the House or Senate with identical or similar language) passed the House in July. The legislation will encourage Federal Government agencies to adopt technology that is protected from decryption by quantum computing. The law requires the Office of Management and Budget to prioritize federal agencies' acquisition of and migration to IT systems with post-quantum cryptography. It also mandates that the White House create guidance for federal agencies to assess critical systems one year after the National Institute of Standards and Technology issues planned post-quantum cryptography standards.

Joe Biden, the USA President, also signed the SBA Cyber Awareness Act, which requires the Small Business Administration to submit an annual report regarding the cybersecurity of the agency.

UK'S DIGITAL REFORM BILL DRAWS CRITICISM FROM EXPERTS

The United Kingdom seeks to break away from the EU's General Data Protection Bill Regulation (GDPR). In May 2022, the UK Government proposed a new Bill to bring the 2018 Data Protection Act, UK GDPR, and the UK's application of the EU's ePrivacy directive, the Privacy and Electronic Communications Regulations (PECR) under one directive. The proposed bill has been officially named the Data Protection and Digital Information Bill, also known as the 'Data Reform Bill' (DRB).

The Bill proposes changes with regard to the following:

- Limitations on the types of personal data that can be collected, used, and shared.
- Changes to the rules around using personal data for legitimate interests aim to make it easier for scientific research and the public sector to access and use this data.
- A redefinition of Data Protection Impact Assessments (DPIAs) as "assessments of high-risk processing." This suggests that the scope of DPIAs may be narrowed to focus on specific types of data processing deemed high-risk.
- A change to the rules around subject access requests (SARs), which are requests made by individuals to access their personal data. The threshold for refusing or charging a fee for SARs may be changed from "manifestly unfounded or excessive" to "vexatious or excessive." This means that organizations may have more leeway to refuse or charge for SARs if they are deemed to be unreasonable.

The Bill has been criticized by experts especially considering that businesses will be forced to operate under two regimes. UK companies dealing with clients, partners, customers, etc., will have to comply with DPR on top of GDPR. The bill also reintroduces red tape that GDPR scrapped, such as the requirement for a business to register with the Information Commissioner's Office (ICO). These clauses can be restrictive for businesses who would only be willing to comply with the GDPR.

AUSTRALIA AIMS TO BE WORLD'S MOST CYBER SECURE NATION

Post a wave of data breaches in the country that resulted in data leaks of millions of its citizens, Australia has committed to becoming one of the most cyber-secure nations in the world by 2030. Australia faced back-to-back cyber incidents at private health insurer Medibank and telecommunications provider Optus. Home Affairs and Cyber Security Minister, Clare O'Neil, announced that the government is in the process of making a new cyber security strategy with the project to be led by former Telstra CEO, Andy Penn; Rachael Falk, CEO of the Cyber Security Cooperative Research Centre; and Mel Hupfeld, a recently-retired chief of Air Force. O'Neil also criticized the decision of the previous government to abolish the Ministry of Cybersecurity in 2018. O'Neil had announced the formation of a task force that would hunt down hackers and contemplated a ban on ransomware payments.

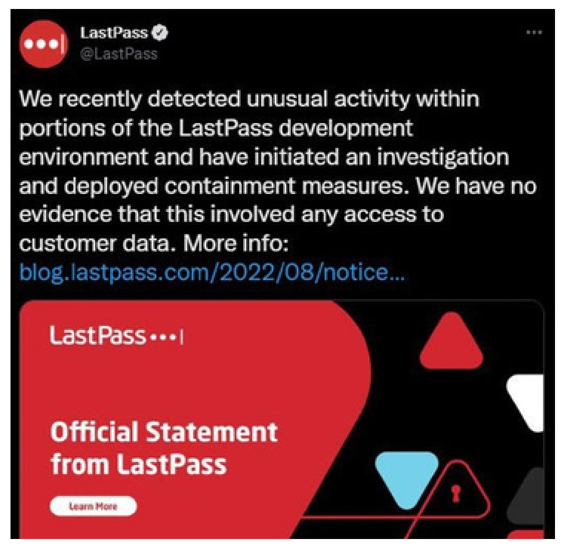
Further, it is to be noted that Australia will host a virtual international counter-ransomware task force early next year as a part of the 36-nation Counter-Ransomware Initiative.

PASSPORT DETAILS OF EXPATS LEAKED BY INDIA'S FOREIGN MINISTRY

The Global Pravasi Rishta Portal, the Government of India's platform for connecting with its overseas population, exposed the confidential data of its registered users. The portal did not have appropriate security measures. This was discovered by a research team that notified the Ministry of External Affairs. The data leak included usernames, passport numbers, country of residence, and email addresses in plaintext, as well as occupation status and phone among other details. According to media reports, the data was exposed via the website's edit function, where manipulating the URL allowed anyone to access the edit details of any user on the site.

DATA BREACHES

LASTPASS DATA BREACH, GOI ISSUES ADVISORY



LastPass
@LastPass

We recently detected unusual activity within portions of the LastPass development environment and have initiated an investigation and deployed containment measures. We have no evidence that this involved any access to customer data. More info: blog.lastpass.com/2022/08/notice...

LastPass, a password management company that enables users to store their passwords in a single application and reduces the usage of passwords for multiple platforms, has recently confirmed that its cloud-based software was under a phishing attack.

The Indian cyber agency Computer Emergency Response Team (CERT-In) issued an advisory for the app's Indian users. It warned about the accounts getting compromised due to phishing attacks on the app.

DATA OF 30 MILLION USERS OF INDIAN RAILWAYS LEAKED

In a recent development, the Indian Railways was under malware attack, which resulted in the information of approximately 30 million customers being leaked. Some of the details of the customer information that was leaked included information like usernames, emails, verified and unverified mobile numbers, gender details, language preferences and so on. That's not all, the data breach also resulted in information of important person and government personnel being leaked. Post the breach the data was posted online for sale. However, only 10 copies of the stolen data were sold. According to media reports customers travel and billing histories were also compromised. Shadow Hacker, a username on the Dark web Forum, took the responsibility of this attack.

DDOS ATTACKS INCREASED BY 81% IN 2022

There has been a significant increase in the volume and frequency of DDoS attacks, in 2022, compared to the previous year. According to the Imperva DDoS Threat Landscape report, there were an average of four large-volume DDoS attacks per month in 2022. These attacks were more widespread, targeting companies in the automotive, IT, and telecommunications sectors. This was followed by organizations in the finance, government, and education sectors. The rise in geopolitical conflict also led to an increase in hacktivism-based DDoS attacks owing to the Russia-Ukraine conflict.

Large-volume DDoS attacks were made through an army of botnets with thousands of infected devices. For instance, the attack scope of ZeroBot was expanded with new exploits and DDoS methods to target more devices. Further, the capabilities of the Fodcha botnet were also enhanced by adding an extortion feature to its arsenal, thus demanding a ransom from victims in return for stopping attacks.

CYBER ATTACKS

AN EAVESDROPPING SPYWARE NAMED EARSPY

A new spyware named EarSpy has been discovered that eavesdrop on phone calls using motion sensor data from the echo of ear speakers during any conversation. Its major targets are Android devices that enable it to detect the caller’s speech, gender, and identity.

The accuracy of the attack for identification of gender ranged between 77.7% to 98.7%, and speech recognition between 53.8% to 56.4%. The spyware was discovered by researchers from five American Universities, namely the New Jersey Institute of Technology, Texas A&M University, Temple University, Rutgers University, and the University of Dayton. To reduce the efficacy of EarSpy, it is advised to set the call volume low for ear speakers.

TOP EXECUTIVES MORE VULNERABLE TO CYBERCRIMES THAN EMPLOYEES IN MNCS

Ivanti, an IT software company, conducted a research study among 4,500 MNC top executives about the cyber security measures they adhere to within their company. The survey findings revealed that despite 97% of the respondents feeling confident about their preparedness against cyber security threats, cyber security measures in their companies were inadequate to protect them against a potential breach. The report also highlighted that while many respondents consider themselves "very prepared" for the threat landscape, key security measures such as deprovisioning credentials are often overlooked. Many suspect former employees or contractors still have access to company systems and files.

According to the report, leaders are also engaging in risky behavior. They are at a higher risk of falling for phishing attacks, as they are four times more likely to be targeted than regular office workers.

MALVERTISING CAMPAIGN THROUGH GOOGLE ADS

Cybercriminals are increasingly using Google ads to spread malware through deceptive advertising strategies. They create fake websites that impersonate popular software packages, such as MSI Afterburner, Slack, Dashlane, Malwarebytes, Grammarly, Audacity, OBS, Ring, AnyDesk, Libre Office, Thunderbird, Teamviewer, Brave, and more.

These websites distribute trojanized versions of the software, which can steal victims' crypto wallets and GPUs. One known threat group, Vermux, is using many masquerAds sites and domains, primarily from Russia, to target US residents.

To evade detection by Google and other security agencies, the attackers redirect victims to irrelevant yet genuine sites created by them before ultimately leading the potential victims to the malicious, impersonating site.

COVERT INFLUENCE OPERATION

META BANS 200 COVERT INFLUENCE OPERATIONS ACTIVE SINCE 2017

Global social media conglomerate Meta took down over 200 covert influence operations (Covert influence operations originate from foreign sources and undermine the legitimacy of liberal democracies) across its social media platforms. Meta disrupted these networks for violating its CIB (Coordinated Inauthentic Behaviour) policy.

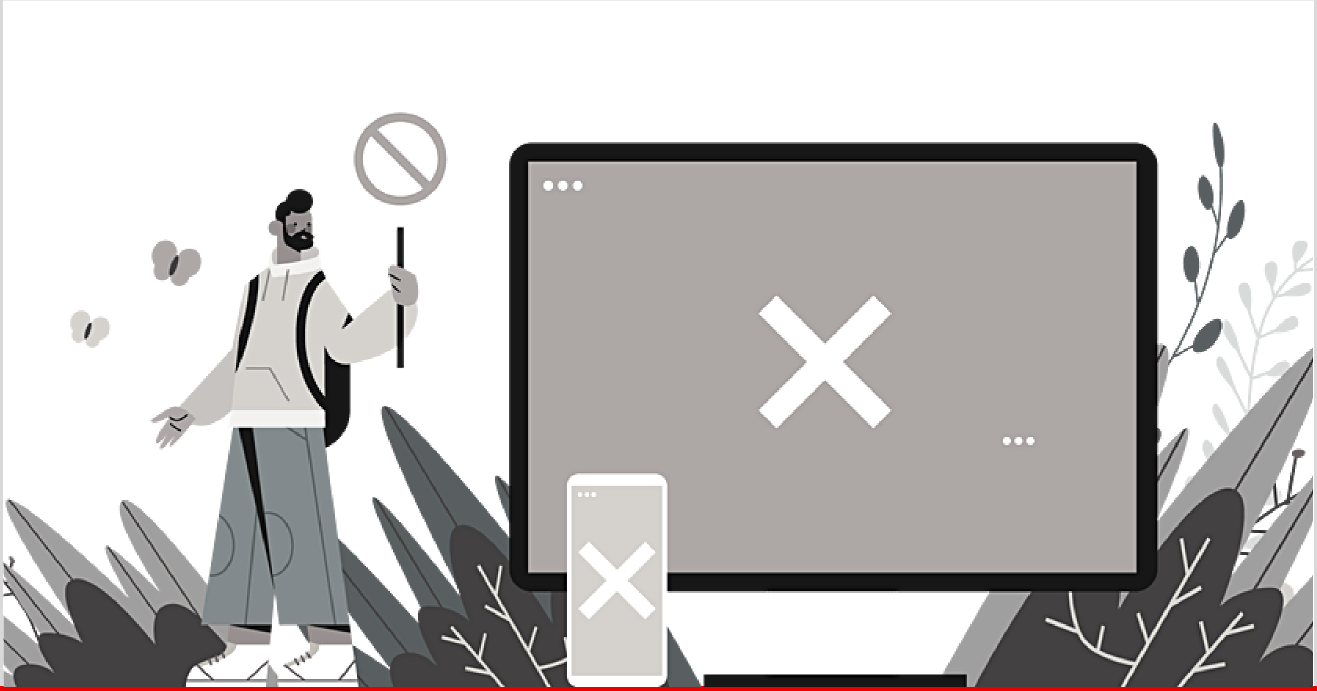
The company mentioned that these operations originated from various countries, and the content ran in several languages. Their content focussed primarily on local audiences and influenced local audiences.

These operations used various tactics, such as writing spammy comments to running fictitious cross-platform media entities that hired real journalists to write for them. Meta also highlighted the number of actions it took against spywares and its users.

This included removing over 350 accounts linked to Israeli spyware developer Candiru and Quadream. Both these companies were founded by former employees of NSO Group who developed the spyware Pegasus, linked with spying on influential people in various countries, including India.

These companies used persistent and adaptive tactics to avoid detection. Therefore, Meta emphasized a concerted regulatory response by democratic governments to tackle this issue.

According to Meta, “because surveillance-for-hire services cast their net so wide, no single company can tackle this alone.”



CONSULTATION ON THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

India Future Foundation (IFF) organized a consultation on "The Draft Digital Personal Data Protection Bill, 2022" (DPDP) at the United Service Institution of India. The DPDP draft was put out for comments from stakeholders by the Ministry of Electronics and Information Technology (MeitY). IFF put forward our views on aspects that should be taken into cognizance for necessary action before this Draft Bill takes the shape of a law.

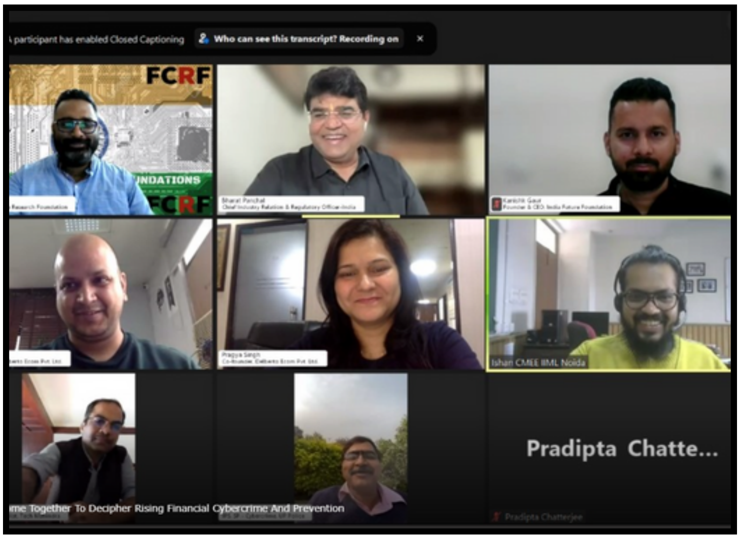
We provided our insights on topics including consent for the use of data; Data Fiduciary can use data of children only after the permission of children; threat to national security; transfer of personal data outside India, etc.

While the intention of coming up with The Draft Digital Personal Data Protection Bill 2022 is noble, some areas of concern and ambiguity require attention. More importantly, considering technology is continuously evolving, there should be a provision in the Draft Bill that speaks of regular updates if needed. It will help if the points mentioned get a relook for appropriate action.

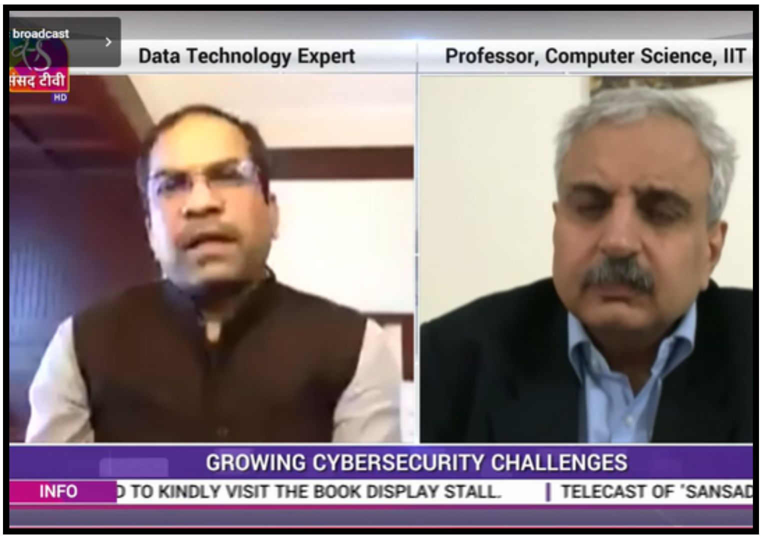
The consultation was held on December 13th, 2022, at the United Service Institution of India.

The speakers at the consultation were Gen. (Retd) Pawan Anand, Distinguished Fellow USI and Head USI-ANBI, Dr Pavan Duggal, Chairman, International Commission on Cyber Security Law, Col (Retd) Sanjeev Relia, Chief Strategy Officer, ThinkCyber, Mr Rahul Sharma, Founder, The Perspective, Mr Suhaan Mukherji, Partner, PLR Chambers, Col (Retd.) Sunil Kapila, Co-Founder & Chief Technology Officer, Athenian Tech, Mr Kanishk Gaur, Founder, IFF, Mr Amit Dubey, Co-Founder, IFF, Mrs Shonan Mahajan, Vice President - Training Development, ThinkCyber India.

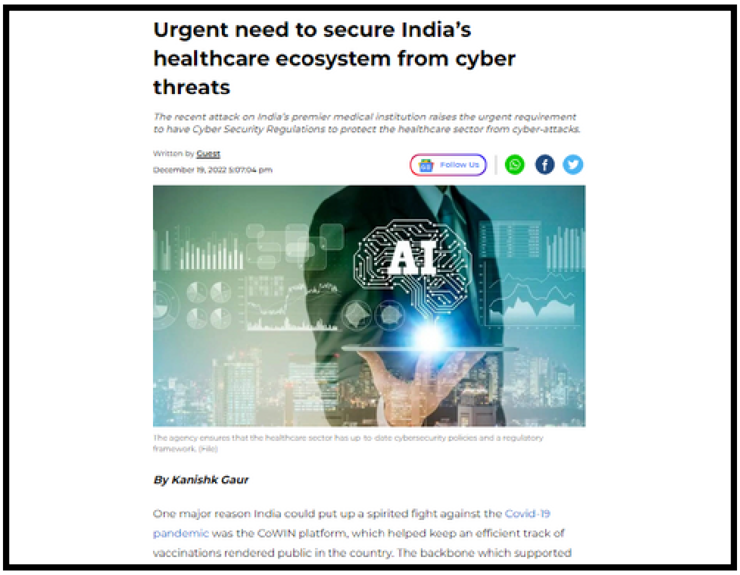
IFF IN THE MEDIA


A participant has enabled Closed Captioning
Who can see this transcript? Recording on
FCRF
INDATIONS
Ishan CMEE IIML Noida
Pradipta Chatte...
me Together To Decipher Rising Financial Cybercrime And Prevention

Kanishk Gaur, Founder, IFF, in a discussion about rising financial cybercrimes and prevention with the country's top cyber experts.


broadcast
संसद टीवी
HD
Data Technology Expert
Professor, Computer Science, IIT
GROWING CYBERSECURITY CHALLENGES
INFO
D TO KINDLY VISIT THE BOOK DISPLAY STALL.
TELECAST OF 'SANSAD

Amit Dubey, Co-Founder, IFF, talks about cybersecurity challenges on Sansad TV.



Urgent need to secure India's healthcare ecosystem from cyber threats

The recent attack on India's premier medical institution raises the urgent requirement to have Cyber Security Regulations to protect the healthcare sector from cyber-attacks.

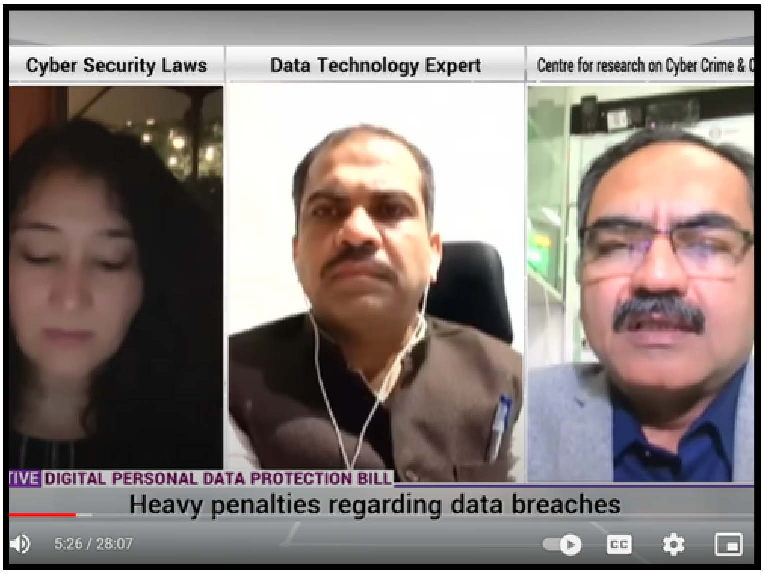
Written by Guest
December 19, 2022 5:07:04 pm

The agency ensures that the healthcare sector has up-to-date cybersecurity policies and a regulatory framework. (File)

By Kanishk Gaur

One major reason India could put up a spirited fight against the Covid-19 pandemic was the CoWIN platform, which helped keep an efficient track of vaccinations rendered public in the country. The backbone which supported

Kanishk Gaur, Founder, IFF shares his views on securing India's health ecosystem in The Financial Express.


Cyber Security Laws
Data Technology Expert
Centre for research on Cyber Crime & C
TIVE DIGITAL PERSONAL DATA PROTECTION BILL
Heavy penalties regarding data breaches
5:26 / 28:07

Amit Dubey, Co-Founder, IFF, in conversation with Sansad TV about The Digital Personal Data Protection Bill, 2022.

INDIA FUTURE
FOUNDATION

India Future Foundation

Phone: +91-1244045954, +91-9312580816
Email: helpline@indiafuturefoundation.com
Building no. 2731 EP, Sector 57, Golf Course Ext. Road, Gurugram,
Haryana, India – 122003
www.indiafuturefoundation.com