Security risks that lurk deep inside the Metaverse p28
Cyber Insurance: Who comes after the Spiderman takes off? p34
Intensification of cyber attacks over the last 35 years p52
AI & Ethics: 'The dog ate my homework' excuse won't work here p60

₹125
VOL. 35 | ISSUE 3 | March 2022
www.pcquest.com
PCQUEST
UNDERSTAND • CHOOSE • IMPLEMENT
CyberMedia
35 YEARS
1987 - 2022

Blended World, Blended Threats

It's time to revisit your security postures

Special Subscription offer on page 62
76 pages including cover

AMD

Power of Desire

INDIA'S
MOST DESIRED BRAND
TRA's Desired Brand Report - India Study 2021

HELP YOUR TEAM RISE

For next level productivity and performance, use Windows 11 Pro and AMD Ryzen™ PRO Mobile Processors.

AMD RYZEN PRO | Windows 11

APEEJAY EDUCATION

SOARING HIGH IS MY NATURE

Apeejay Stya Advantage (50+ Years of excellence in education)

Quality Education from pre–nursery to doctoral level	**2,500** Faculty	**65,000** Strong alumni network	**85+** Programmes to choose from	**40,000** Students	**24** Educational institutions across the country

Some of our Awards and Accolades

'Top Education Brands Award' (Academic Excellence in K–12) by Business World Education in 2020

Awarded as **'Best Education Society for promoting Social Cause in 2019'** by Centre for Education Growth and Research

Apeejay Schools

- Apeejay School, Mahavir Marg, Jalandhar, Punjab
- Apeejay School, Hoshiarpur Road, Jalandhar, Punjab
- Apeejay School, Tanda Road, Jalandhar, Punjab
- Apeejay School, Model Town, Jalandhar, Punjab
- Apeejay School, Panchsheel Park, New Delhi
- Apeejay School International (IB), Panchsheel Park, New Delhi
- Apeejay School, Saket, New Delhi
- Apeejay School, Pitampura, Delhi
- Apeejay School, Noida, U.P., Near Delhi
- Apeejay International School, Greater Noida, U.P.
- Apeejay School, Faridabad, Haryana
- Apeejay Svrán Global School, Faridabad
- Apeejay School, Charkhi Dadri, Haryana
- Apeejay School, Kharghar, Navi Mumbai
- Apeejay School, Nerul, Navi Mumbai
- Apeejay Rhythms Kinderworld, GK–2, New Delhi
- Apeejay Rhythms, Sector–15, Faridabad
- Apeejay Rhythms Kinderworld, Model Town, Jalandhar

W: www.apeejay.edu | E: aes@apeejay.edu

PCQUEST 35 YEARS 1987 - 2022
UNDERSTAND • CHOOSE • IMPLEMENT
www.pcquest.com

EDITORIAL
MANAGING EDITOR: Thomas George
EDITOR: Sunil Rajguru
ASSOCIATE EDITOR: Soma Tah
DESIGN MANAGER: Nadeem Anees

CYBERMEDIA LABS
MANAGER: Ashok Pandey

CONSULTING EDITOR: Pradeep Chakraborty

VICE PRESIDENT RESEARCH: Anil Chopra

BUSINESS
SR. VICE PRESIDENT & GROUP HEAD:
Rachna Garga (rachnag@cybermedia.co.in)

NORTH:
ASSOCIATE VICE PRESIDENT:
Harminder Singh
MANAGER: Sudhir Kumar Arora

SOUTH:
MANAGER: Shubhadeep Sen

WEST:
MANAGER: Shubhadeep Sen

EAST:
MANAGER: Sudhir Kumar Arora

MARKETING & ALLIANCES
(marketing@cybermedia.co.in)
SR. VP & GROUP HEAD: Rachna Garga
MANAGER MARKETING: Rajiv Pathak

OPERATIONS, EVENTS & COMMUNITIES
SR. VP & GROUP HEAD: Rachna Garga
GENERAL MANAGER: CP Kalra
MANAGER, MIS & DATABASE:
Ravi Kant Kumar
MANAGER: Ashok Kumar

CIRCULATION & SUBSCRIPTIONS
SR. VP & GROUP HEAD: Rachna Garga
SR. MANAGER: Sarita Shridhar
ASST. MANAGER: Alok Saxena
SR. PRESS CO-ORDINATOR:
Harak Singh Ramola
CHENNAI: C Ramachandran

For subscription queries contact:
rsepcq@cybermedia.co.in

Send all your tech questions to:
pcquest@cybermedia.co.in

http://twitter.com/pcquest
http://facebook.com/pcquest
http://linkd.in/pcquest
http://gplus.to/pcquest

EXPLORE


p10

COVER STORY
SECURITY

Evolving cyber threat tatics keeping businesses and individuals alike on their toes

CORPORATE OFFICE: **Cyber House, B-35, Sec-32, Gurugram (NCR Delhi) 122001. India**
email us pcquest@cybermedia.co.in
call us +91-124-482-2222, **fax us** +91-124-238-0694

OUR OFFICES

BENGALURU: **Address:** 205-207, Sree Complex (Opp. RBANMS Ground), # 73, St John's Road, Bangaluru - 560 042. Tel: +91 (80) 4341 2000, Fax: +91 (80) 2350 7971

MUMBAI: **Address:** 404 Trade Square, Mehra Industries Compound Safed Pool,, Sakinaka, Andheri East, Mumbai – 400072. Mobile: 9969424024

DELHI: **Address:** Cyber House, B-35, Sec 32, Gurugram, NCR Delhi-122001. Tel: 0124-4822222, Fax: 2380694

Printed and published by Pradeep Gupta on behalf of CyberMedia (India) Ltd, printed at printed at M/s Archna Printers, D-127, Okhla Industrial Area, Phase-1, New Delhi, published from D-74, Panchsheel Enclave, New Delhi-110017. Editor: Sunil Rajguru. Distributed in India by IBH Books & Magazines Dist. Pvt. Ltd, Mumbai.

NEW

#PCQuestTroubleShoot
p7

EXPLORE

Intensification of cyber attacks over the last 35 years
p52

COVER STORY
SECURITY

p16
Malicious actors on the prowl; Don't let your guard down, ever!

p28
Security risks that lurk deep inside the Metaverse

p32
How secure is your Smart Home?

p34
Who comes afer the Spiderman takes off?

p44
Combating HR Data Threats

p48
6 Best Practices to minimize the Cloud security risks and threats

AI
p60
AI & Ethics: 'The dog ate my homework' excuse won't work here

DEVELOPER
p64
Low-code may open AI doors for many businesses

METAVERSE
p66
What it takes to build a human-centric Metaverse

REVIEW
p71
AMD Radeon RX 6600 XT Graphics card

REVIEW
p72
Zunpulse Smart Bulb 12 W

REVIEW
p73
Zunpulse Smart Plug 16A

REVIEW
p74
Kent Cameye Homecam 360

FORM IV (See Rule)

Statement of ownership and other particulars about the Magazine PC Quest to be published in the first issue every year after the last day of February

1.	Place of Publication	: New Delhi
2.	Periodicity of Publication	: Monthly
3.	Printer's Name	: Pradeep Gupta
	Whether Citizen of India	: Yes
	Address	: D-74, Panchsheel Enclave, New Delhi – 110 017
4.	Publisher's Name	: Pradeep Gupta
	Whether Citizen of India	: Yes
	Address	: D-74, Panchsheel Enclave, New Delhi – 110 017
5.	Editor's Name	: Sunil Rajguru
	Whether Citizen of India	: Yes
	Address	: C,O, 302 Royal Avenue Apt, Kathriguppe Main Road, Near Big Bazar, Banashankari 3 Stage, Banglore South, Bengaluru, Karnataka - 560085
6.	Names & addresses of individuals who own the newspaper, and partners or shareholders holding more than one percent of the total paid-up capital	: Cyber Media (India) Limited D-74, Panchsheel Enclave, New Delhi – 110 017

List of shareholders holding more than 1% of the paid up capital of the company as on 15th February 2019: Pradeep Gupta, Sudha Bala Gupta, Dhaval Gupta, Kriti Gupta, Vimgi Investments Pvt. Ltd., SAL Advisors Pvt. Ltd., Mahesh Dinkar Vaze, Mahendra Girdharilal, Presan Consultants Pvt. Ltd., Hemali Prakash Mehta

I, Pradeep Gupta, hereby declare that the particulars given above are true to the best of my knowledge and belief.

Sd/-
Publisher

Sunil Rajguru
✉ sunilr@cybermedia.co.in

The importance of tech sovereignty

Your water, electricity and broadband are all given by Indian service providers. Your roads are built by Indian contractors. The offline world is by and large Indian. When it came to the Indian mainstream media, the government tried its best to keep foreign players out of the equation. In the online world all that has changed. Tech has opened the floodgates. America has taken over.

WhatsApp is India's largest player in that domain. Facebook is the largest Indian social media network. LinkedIn dominates social networking. Twitter, despite its small size, is India's most powerful political tool. We are dependent on Google Maps and American GPS. YouTube and Instagram are big and TikTok was growing at a rapid pace before the ban on Chinese apps. Amazon India is becoming a behemoth and Flipkart has been taken over by Walmart. The world's top three cloud service providers are American (AWS, Azure and Google Cloud).

Make in India has to succeed in the app world

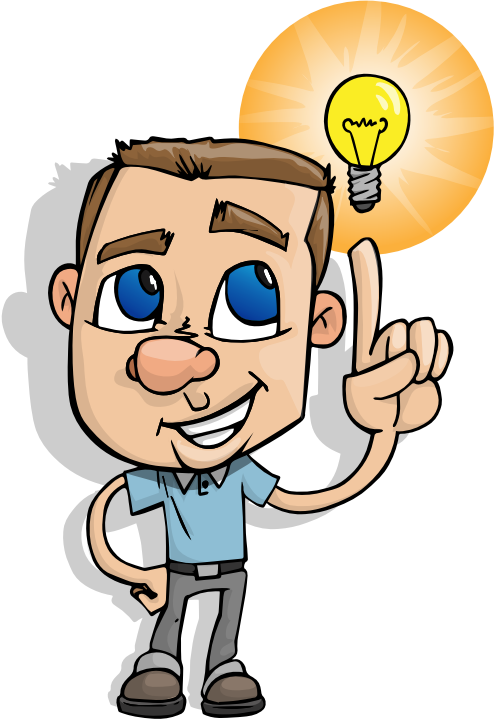
Russia's invasion of Ukraine is showing the dangers of being dependent on America. Google Pay went offline in Russia. YouTube has blocked Sputnik and Russia Today in Europe. Silicon Valley can declare war on any country it wants to. What happens if it decides to go after the Indian leadership in the future over some political disagreement? China was the first country to realize this and has its own Internet ecosystem. The Indian ecosystem is by and large American, and this does not bode well for its future political and strategic stability. Indian IT services giants are heavily dependent on America for business.

It's not all doom and gloom. India's UPI (United Payments Interface) has 150 million users and is operational in multiple countries. They are developing a voice command feature in regional languages that is sure to make it even more widespread. The Digital Rupee is being looked at. We will have an operational Indian GPS—The Indian Regional Navigation Satellite System (IRNSS) or NavIC (NAVigation with Indian Constellation). The satellite launches have begun.

Indian Production Linked Incentive Schemes cover everything from semiconductors to electronics to hardware to telecom. The Indian startup industry really took off in the pandemic era and if this pace of growth continues then soon it will challenge the likes of America and China. This is not enough. Key remain the apps. India cannot hope to achieve much unless it becomes an app superpower. We have always been an underperformer in software innovation never having say a Windows or a Google Search. Not much has changed in the social media era. The largest social media platforms are American and Chinese, with some European entries.

This is one area where Make in India has to succeed. India's future sovereignty may well depend on it.

Sunil Rajguru



#PCQuestTroubleShoot

Ashok Pandey
ashokpa@cybermedia.co.in

I am a web developer and looking for a laptop to start a web development bootcamp?

■ *Anand Arora*

You can get a laptop powered by an 11th Generation Intel Core i5 processor, 8 GB RAM, Intel Iris Xᵉ Graphics and 512 GB SSD. It would be better to get a business laptop as they comes with built-in security features. I would recommend the Dell Latitude series of laptop. Get a compact laptop with light Aluminum chassis, so you can carry the PC easily from one to another place.

What is the best laptop for trading in 2022?

■ *Ramesh Thapar*

It would be best if you had a decent and premium laptop with a good hardware configuration to match your trading style. The laptop must contain a very good display with a long-lasting battery, enabling you to trade on the go.

Trading might need you to run multiple tabs and windows on the screen simultaneously, so you need decent processing power backed up with ample RAM. You also need the laptop to be compatible with attaching multiple displays if you need them. Considering you are a professional trader, so, you should check out the HP Z Bookseries of laptop. depending on your budget you can get a laptop powered by an 11th Gen Intel i7 CPU, 16 GB RAM and 512GB SSD.

I am looking for a best laptop for gaming?

■ *Rajbir Sharma*

When looking for a gaming laptop, you should understand that a gaming laptop can not replace a gaming desktop. So, do not expect it to perform like one. But, gaming on the go is a common need these days; many laptops can provide you with a premium experience.

When buying a gaming laptop, you should consider the facts of CPU, RAM, GPU, and Display in mind. Most gaming laptops are very costly and do not feature a long-lasting battery backup. You can get a gaming laptop like Dell Alienware or HP OMEN powered by 11th gen Intel i7 CPU, 16GB DDR4 RAM, and Nvidia RTX 3050 GPU. You should also check for display minimum - 1080p FHD resolution and 144 Hz refresh rate for the best visual experience.

What is the best laptop for a student?

■ *Sanjeev Gupta*

It depends on what you are studying or planning to study in the future. A laptop is a necessary but expensive investment for a student. Your study needs will impact the decision to choose a laptop directly.

If you are looking for a laptop to learn basic coding, any laptop can do the job for you. But if you are planning to learn Graphics

Designing, Machine Learning, MatLab, etc., you may need a decently powerful laptop for that. If you have plans to do trading or crypto mining as a student, you need a very powerful laptop. If gaming on the go comes under the need of your hood, you probably need a gaming laptop. If your budget is very low, as a laptop is necessary to complete the assignments and attend classes, you should go with an entry-level laptop.

As a balanced choice, I recommend to get a laptop powered by 11th gen Intel Core i3 and 8GB RAM.

What's the best laptop I can buy as a CS student?

■ *Tarun Mahajan*

As a student of Computer Science, you might be learning coding on your pc for starters. Later on, you might move on to machine learning or full-stack development. You might also use the laptop to learn data analytics and data science in the future. So, it would help if you had a decent-level laptop powered with the latest gen CPU and a decent GPU. Mind that you need a laptop with good battery backup, as every day you will be spending a lot of time on the move.

You can get a laptop powered by 11th gen Intel Core i5 and 8GB RAM and Nvidia GTX 1650 GPU. You can also look at Ryzen CPU powered laptop as Ryzen'sconsume less power gives you better battery life.

In a general sense, which is better, a desktop or a laptop?

■ *Josh Brar*

Laptop and desktop both have their places in this cyber era. Only depending upon your needs and lifestyle it can be said which one is better. IF you are seeking the answer to which one is the most powerful, the answer is desktop. Even if you are asking which one is more affordable the answer is desktop.

Desktops are more powerful, affordable and have a low maintenance cost. Desktops are also compatible with multiple upgrades, unlike laptops. But still, laptops have their place in the computing ecosystem, which no desktop can take. If your job requires you to move or travel daily, a laptop can be your only option.

Students, office employees, travel vloggers, traders, on-field reporters, everybody need a laptop for their computing needs. These days laptops are extremely powerful and feature long batteries providing up to 8+ hours of backup.

My PC doesn't show my home WiFi in the available networks but connects with it using Ethernet. How should I resolve this?

■ *Ashish Khurana*

Please check and update your network adapter's drivers. For instance, if you have an HP laptop, then go to HP's website's drivers download page and using your laptop model number you can find the relevant software. Download the driver and install it on your PC. You should also check for the latest BIOS or UEFI firmware, Chipset, Display (Video), Sound, USB3, Bluetooth, Network and all other drivers, or else download and install the latest one.

If still, you are unable to connect, then go to Device Manager > Network Adapters, select Wi-Fi adapter, then Power Management tab, clear the check box to ""Allow the computer to turn off the device to save energy."" Then on the Advanced tab disable any energy-saving options. Enable IPv6 in the network adapter settings and try to connect.

I hope this will help.

How do I fix my laptop after the BIOS update? The screen is black, but I can hear it running and everything.

■ *Rahul Rai*

If the screen is blank and you can hear it running, it could mean that the BIOS has changed the screen resolution. Try to get hold of an external display and connect it to the laptop. If it works, then change the screen resolution and restart the system. If that doesn't work, then you will have to restore the BIOS to the previous version. For this, I suggest you visit your nearest service center and ask them to do it for you.

Evolving cyber threat tactics keeping businesses and individuals alike on their toes

Soma Tah & Ashok Pandey
somat@cybermedia.co.in
ashokpa@cybermedia.co.in

The burgeoning cybercrime marketplace offering Cybercrime-as-a-Service has not only made it easier for even less technically-minded criminals to engage with cybercrimes, it created a perfect breeding ground too for malicious actors and organized cybercrime groups to exploit unsuspecting businesses and individuals

From 2020 onwards, when the lines between digital and physical worlds started blurring increasingly by the growing adoption of digital during the pandemic, cyberattacks on critical infrastructure and cyber security failure have also started emerging as top risks globally.

The expanded attack surface caused a massive increase in cyber threats. New industries, platforms, and processes have been targeted by the miscreants leaving consumers as well as businesses alike at risks of being held hostage.

The growing business model of Cybercrime-as-a-Service makes malicious activities more affordable and easily accessible for anyone, while the increasing sophistication of tools makes detection and prosecution of cybercrimes even more difficult.

Surfshark's study revealed that 4 in 1M Indian internet users have been a victim of cybercrimes in 2020, ranking India 10th in the world in terms of cybercrime density. The FBI received almost 3,000 complaints during the year from India, ranging from romance scams to ransomware attacks.

In its global incident response analysis for the first half of 2021, Accenture Security found that there's a triple digit increase in intrusion volume driven by three trends- 1) global uptick in web shell activity by way of nation-state and cybercrime actors alike, 2) targeted ransomware and extortion operations and 3) supply chain intrusions.

▾ How threat actors and the expanded attack surfaces are likely to hurt us in 2022?

Although Financial services, Government, ICT, Manufacturing, Healthcare, and Education have been the most targeted industries during the pandemic, but as the pandemic starts to subside and the world returns to normal, it can turn the spotlight again on 'dormant' industries such as Consumer Goods & Services, Industrials, Travel & Hospitality and Retail– already reeling from lockdowns and staff shortages.

The continuing work from home trend with an unprecedented number of people working remotely, will also leave the company's doors exposed to cybercriminals. Nathan Wenzler, Chief Security Strategist, Tenable said, "Remote work has become the perfect ongoing distraction for attackers to build social engineering attack campaigns around. After all, only one-third of remote workers strictly follow their organization's security guidelines, and they have an average of eight devices connecting to their home network, creating plenty of targets of opportunity for attackers to take advantage of. All it takes is one employee falling victim to a single, well-crafted social engineering stunt, which makes end users the perfect target for today's adversaries who are aiming for access to corporate networks, databases, and other valuable assets."

▾ **Ransomware:** Despite the global pandemic, cybercrimes continued to thrive. Ransomware wreaked havoc in 2021- not only by increasing the frequency of assaults, but by increasing the amount of ransom demands also. CrowdStrike's 2021 Global Security Attitude Survey revealed that Indian firms suffered more ransomware attacks than any other country in 2021, and accounted for the

highest average extortion fee payment ($1.128 million) on top of ransom.

It is likely that instances of worldwide ransomware attacks will continue to increase in 2022 targeting crucial data/infrastructures. Mandiant forecast says that In 2022, threat actors are likely to ramp up new tactics, such as trying to recruit insiders within their victims or targets. We can also expect to see more cybercriminals punishing victims that hire professional negotiation firms to help reduce the final amount of the extortion payment.

Jakub Kroustek, Malware Research Director, Avast said, "Cybercriminals delivering Ransomware-as-a-Service (RaaS) will strengthen affiliate models to better target enterprises, including adding Linux-specific ransomware, greater rewards and extending extortion layers."

An entire underground economy being built around the business of data exfiltration and extortion. Mike Sentonas, CTO, CrowdStrike said, "We're seeingData-shaming websites popping up like street-corner storefronts, providing a hub for ransomware groups to post and auction stolen data that's being held ransom. These ransomware groups are revamping their entire infrastructure of tactics, techniques and procedures to hone in on more effectively exfiltrating and selling stolen data. Even if the threat actors can't get their ransomware to execute past the encryption stage, they'll pivot and find other ways to gain access to the data to sell for a profit anyway. This year we spoke about the rise of the double extortion ransomware model where adversaries demand one ransom for the return of data and another to ensure that data is not leaked or sold. This double extortion ransom model will grow in sophistication in 2022."

10 most common Cyber Threats and Attack Vectors

An attack vector is a way by which an attacker can breach or infiltrate a system or an entire network. It enables the attackers to exploit system vulnerabilities and gain access to sensitive data, personally identifiable information (PII), and other critical information. Some of the common cyber threat vectors today are:

1. Weak/Compromised credentials
2. Poor System/Security configurations
3. Insider threats/Third-party breach
4. Malware/Ransomware
5. Phishing
6. Social engineering
7. DDoS attacks
8. Zero-day attacks
9. Brute force attacks
10. Cryptojacking

▼ **Phishing:** Alongside Ransomware, Phishing also continues to be one of the most common cybercrimes globally. According to the Verizon 2021 Data Breach Investigations Report, phishing attacks were connected to

36pc of breaches, and increased by 11 percent which in part could be attributed to the COVID-19 pandemic. Threat actors have been observed tweaking their phishing campaigns based on what's making the news at any moment in time.

▼ **Social Engineering- Deepfakes and Romance Scams:** Researchers say that audio deepfakes will be increasingly utilized in spear-phishing attacks, such as impersonating a senior executive or other employee/trusted contacts to persuade someone to allow them access to sensitive data or a company network. Deepfake identity thefts are more difficult to detect as fraudsters falsify identity documents and/or imitate a victim's voice on the phone to get around verification steps. They can gain access to devices that collect data using biometrics, especially facial recognition. They collect audio, video, and photo samples from social media/mobile phones to feed into the AI.

While we are talking about complex threat vectors, it might sound surprising that

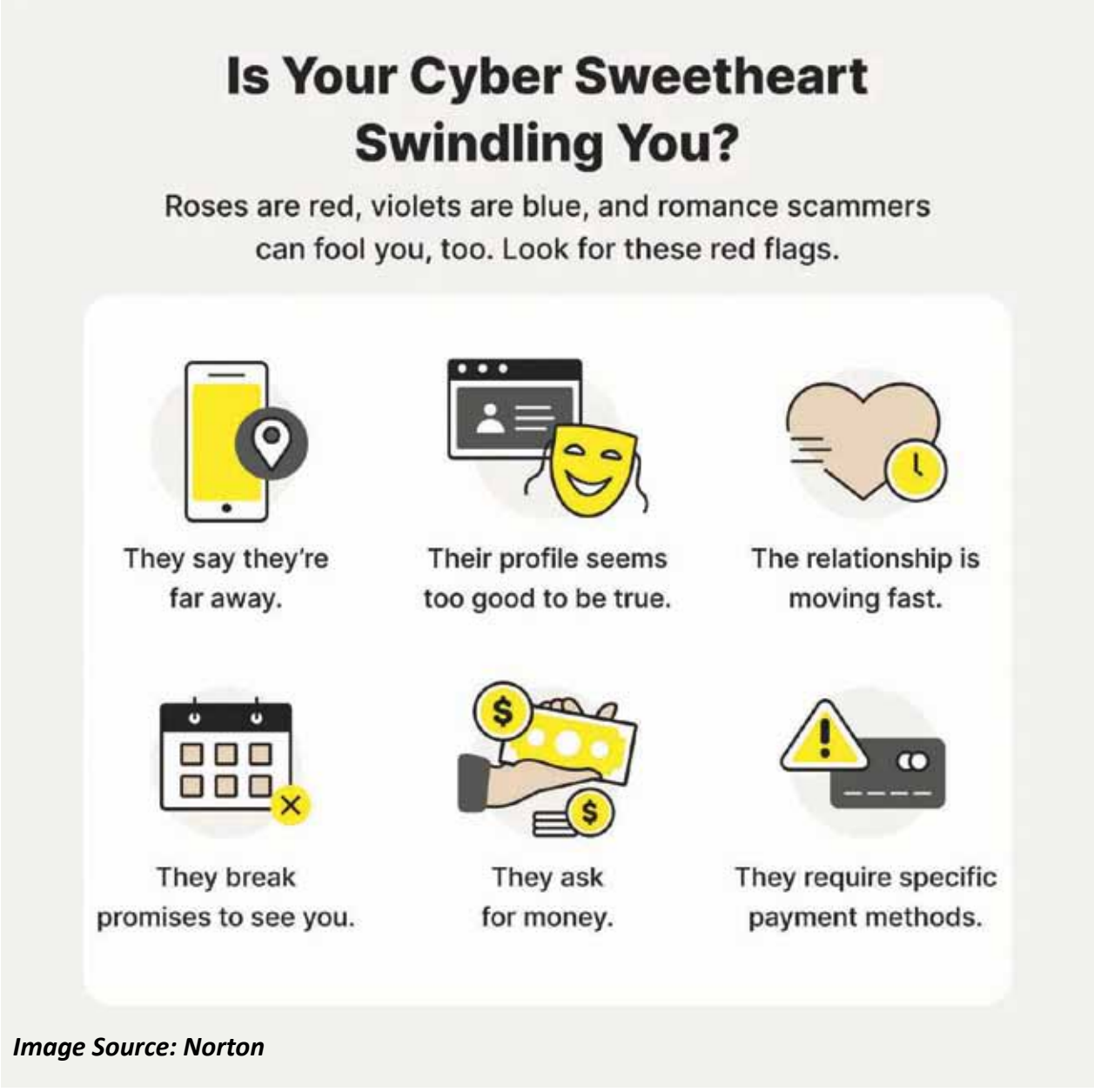


Image Source: Norton

many cyberattacks rely on less technically demanding techniques. Romance scams, for example, have boomed during the COVID-19 pandemic, when many people felt lonely and isolated and looked for love online. A romance scam, also known as an online dating scam, is when a person gets tricked into believing they're in a romantic relationship with someone they met online, while their cyber sweetheart is a cybercriminal using a fake identity to gain enough of their victim's trust to ask them for money. According to the FTC, the reports of the online dating scams have nearly tripled in the past years. In 2020 alone victims lost around $304 million from being swindled by their cyber sweetheart.

▼ **Exploiting Open Source vulnerabilities:** Rohan Vaidya, Regional Director- India, CyberArk said, "In 2022 we can expect attackers to continue looking for new ways to compromise open source libraries. Digital economy runs on open source software (OSS) - it's flexible, scalable and harnesses collective community power to spark new innovations. But countless open and free OSS libraries also mean a dramatically expanded attack surface and a way for threat actors to automate their efforts, sidestep detection and do more harm."

Log4j exploits, of late, have become a security concern already by impacting almost half of all companies worldwide. The humble open source Apache Java logging library is used in many Internet services and apps with over 400,000 downloads from its GitHub project. Attackers are able to exploit vulnerable apps to execute cryptojackers and other malware on compromised servers. Until now, most of the attacks have focused on the use of cryptocurrency mining at the expense of the victims. However, advanced attackers have started to act aggressively and take advantage of the breach on high-quality targets, warns Check Point Research.

▼ **Cryptojacking:** Since cryptocurrencies have garnered a lot of interest from the retail investors, researchers also foresee continued use of crypto-mining malware, cryptocurrency wallets/exchange-related frauds in 2022. For

example, researchers at the Lookout Threat Lab have identified over 170 Android apps, including 25 on Google Play, scamming people interested in cryptocurrencies by offering cloud-based mining services. They scammed more than 93,000 people and stole at least $350,000 between users paying for apps and buying additional fake upgrades and services.

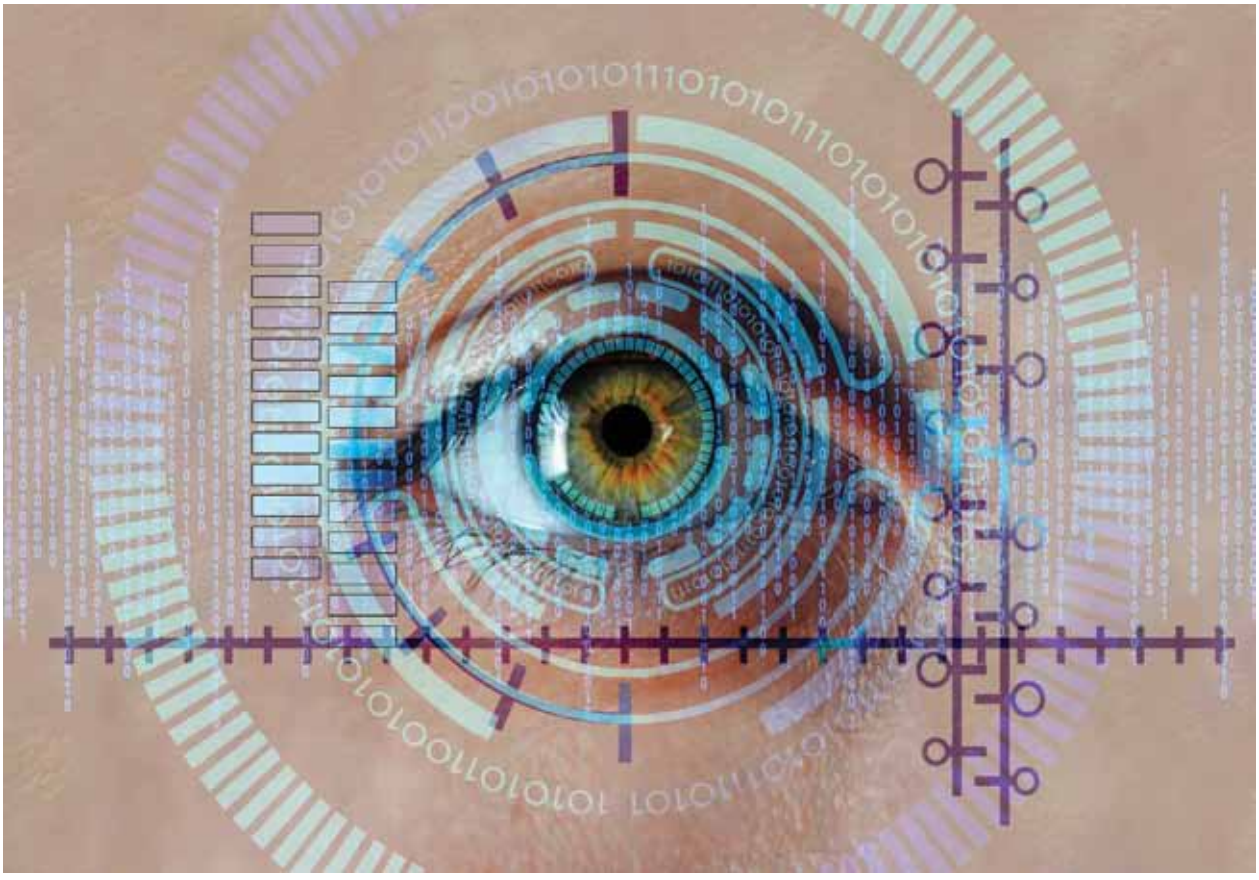
▼ Cyber Espionage and Cyber Warfare: Cyber spying and attacks are part of modern warfare.

As the geopolitical tensions grow due to the Russia-Ukraine crisis, we might see more cyber espionage, warfare, and zero-day attack tactics globally. Securonix Threat Labs has seen a significant increase in cyberthreats- MuddyWater, HermeticWiper and SandWorm are actively being used to launch cyberattacks, including DDoS attacks targeting financial institutions, cyber espionage campaigns and infrastructure. Coming to cyber espionage, India, in fact, is among the top 5 targets for cyberattacks in the APAC region, particularly security breaches that involve cyber espionage, revealed Kaspersky's findings. Its bustling economy and expected growth are among the key reasons for the elevated level of threat it faces.

Concerns are reasonable and valid, according to Sandra Joyce, EVP, Head of Mandiant Intelligence. "Russia has twice turned off power to Kyiv in the middle of winter, they have carried out a global destructive attack that froze global shipping and vaccine production, and they have even fielded tools to target critical infrastructure technology that could have fatal consequences," wrote Joyce in an official blog post. "This isn't just a Ukraine problem. In fact, we believe that after attacking US and French elections, Western media, the Olympics, and many other targets with limited repercussions, Russia is emboldened to use their most aggressive cyber capabilities throughout the West. While they are unlikely to engage the West in combat, these tools give Russia the means to aggressively compete with others without risking open armed conflict. Should US and allies deploy sanctions in the event of a full invasion, the risk of this only increases," wrote Joyce. ■

Malicious actors on the prowl; Don't let your guard down, ever!

Soma Tah & Ashok Pandey
somat@cybermedia.co.in
ashokpa@cybermedia.co.in



The enterprise attack surface has grown exponentially during the New Normal of Work. Remote work, virtual meetings along with digitalization and cloudization at a rapid pace, proliferation of IoT unleashed a whole new set of cyber attack tactics, but many organizations have been slow to adapt to the new security climate

Over the last few years, Cloud and Datacenters, in particular, have grown in importance, ensuring that shared access to applications for companies and their distributed workforce remains seamless. More broadly, the pandemic has accelerated the adoption of hybrid cloud, microapps, and hybrid work models, forcing enterprises to rethink their security postures.

Network deployments in Indian enterprises have changed dramatically. For example, in the manufacturing sector, the Internet of Things (IoT) and IT-OT convergence have had an impact on how networks and data center architectures are designed to keep up with the influx of data from applications and devices.

The growing affinity to digital, cloud, IoT, and the rise of shadow IT have added new levels of risk, complexity and cost to securing an organization's data and intellectual property. Organizations of every size must nowadays fight a wide range of increasingly sophisticated threats, including advanced persistent threats (APTs), cybercriminal activity, spam and malware. At the same time, many are also grappling with tighter budgets and don't have the resources to easily address this.

However, despite having safeguards in place, cybersecurity breaches, particularly those caused by human error, continue to be a problem for business continuity plans. The industry is still seeing phishing and ransomware attacks, in which confidential records and customer information are stolen and sold to the highest bidder, causing irreparable damage to corporate reputations. This begs the question - are these companies overlooking something fundamental in their approach to cyber security?

Harshil Doshi, Director- Sales, India & SAARC, Securonix said, "Security teams are no strangers to an ever-changing threat landscape. However, the challenges brought in by the pandemic have overwhelmed SOC teams and significantly compromised businesses. New-age threat vectors have majorly risen from the accelerated adoption of cloud by companies working remotely. As a result, the traditional solutions

MICHAEL MONTOYA, CISO, Equinix

Security will become everyone's responsibility in this new era, with CISOs leading the charge. Establishing convergent cybersecurity environments will be a primary responsibility for CISOs as enterprises expand their digital footprints. DevSecOps models and secure software development life cycles (SSDLC) will assure automated security throughout the development process, given that every organization is now a software corporation.

PIYUSH SOMANI, MD & Chairman, ESDS Software Solution

The increased growth of businesses to a digital base may also contribute to the rising concerns for data security, due to which, it may be required to add more security layers to businesses. With the spread of malware from IT to OT, it may be better for enterprises to pay more attention to asset-focused cyber-physical systems and have a proper system in place to tackle them.

VENKAT KRISHNAPUR, VP & MD, Trellix

Today's digital architectures need to be open (allow data to and from multiple sources – internally and externally), have the technology to farm vast amounts of data, mine them using state of the art techniques such as AI and ML in a cloud environment, perform the analytics in almost real time and identify the needle in the haystack that would result in the most positive outcomes from a protection standpoint for customers and Enterprises.

used for threat detection and response have become obsolete."

Akarsh Singh, CEO and Co-Founder, TSAARO said, "competitors may hire hackers to conduct corporate espionage or overwhelm your data centers with a Distributed Denial of Service (DDoS) attack to disrupt operations, impair sales, and drive consumers away. Hence, it has become necessary to safeguard your organization's systems from such threats."

▾ Enterprises need to revisit their security postures in 2022

The threat landscape continues to evolve at a frightening pace. Hence, businesses need to remain vigilant and implement innovative technology to amplify their overall security posture. Cyber perils are one of the biggest concerns for enterprises in 2022. "In order to curb cyber risks, it is imperative that every enterprise invests in educating their employees about their role towards becoming Cybersmart. A vigilant security posture calls for a unified cloud security platform, performing a thorough security review on every existing tool/solution across the enterprise and the adoption of new ones while being onboarded," said Satya Machiraju, VP, Information Security, Whatfix.

"Organizations are evolving and rethinking their approach to security to ensure resilience. They are realizing that as they may move to embrace hybrid work, their security posture needs to evolve as well," said Rashmi Chandrashekar, Director- DXC Security, GIDC, DXC Technology.

An enterprise's security posture refers to a comprehensive cybersecurity readiness status of an organization. There are several challenges in terms of threat analysis, managing identity and access, endpoint security, application security, cloud security, data security, etc. to name a few.

MANIKANDAN THANGARAJ, VP, ManageEngine

Compliance towards regulations can be improved by establishing centralized IAM solutions with built-in features like MFA, privileged access management and central access policies. Organizations must now shift their focus to incorporating IAM capabilities driven by microsegmentation of the network followed by implementation of risk-based authentication to address threats and secure the surface.

AKSHAT JAIN, Co-founder & CTO, Cyware

While there is an abundance of threat information available today from threat intel providers, OSINT, dark web, and other sources, security teams find it difficult to correlate and analyze the data they collect about security weaknesses and threat campaigns with the existing gaps in their security capabilities.

▾ Endpoint Security:

The combination of the work from anywhere and the growing sophisticated threat landscape underscores exactly how important endpoint security is for organizations to secure their infrastructure and users. However, managing endpoints and securing them across various environments is a well-known challenge for enterprises. If you do not have a solution that provides visibility and reduces your response time during an outage or business disruption, you'll spend a good chunk of your day in troubleshooting and mitigating.

Anthony Di Bello, VP, Strategic Development, OpenText said, "It's more important than ever to ensure security operations have visibility into endpoint and network activity occurring across the enterprise. Attackers are well funded and motivated to keep up the relentless pace of attacks. Adoption of Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) technology that empowers analysts to detect and hunt for threats across the enterprise is more critical than ever."

However, a patchwork approach of

EDR bolted on to traditional Endpoint Protection Platforms (EPP) is simply no longer sufficient for today's digital organizations and work from anywhere approach. EDR has now evolved to eXtended Detection and Response (XDR), and is increasingly being identified as the technology required to safeguard a company's endpoints. While EDR focuses on endpoint security, XDR takes a more holistic approach to security – and works across endpoints, cloud infrastructure, mobile devices, among others. It also helps in easier monitoring by utilizing new-age tools such as artificial intelligence and machine learning to provide accurate analysis and reporting of threats.

A unified endpoint security solution must be designed from the beginning to take a behavior-based approach to pre-infection and post-infection protection as well as detection and response. This unique combination is more effective at stopping breaches and preventing ransomware encryption attacks because it blocks, detects, and defuses threats automatically.

SIDHARTH PISHAROTI, Regional VP- India, SEA & APJ Carrier, Akamai Technologies

> Enterprises need to put into place a strategy that minimizes the risk of cybercriminals reaching critical assets once defenses are breached. This is where micro-segmentation technology comes in. It acts like a waterproof bulkhead, containing the 'blast radius' from a malware attack, by enabling businesses to define security controls down to the individual software and workload level – enabling deep visibility into, and control of data movements.

▾ Application Security

While applications are the backbone of today's modern organizations, they are also the focal point for data breaches. Cyber threats disrupt customer experience and cost businesses more than $100 billion a year. So regardless of industry and business size, protecting apps, wherever they reside, is critical to an organization's security.

88pc of organizations operate both legacy and modern application architectures, while 70pc operate in multiple clouds. This expands the threat surface area as companies are forced to deploy separate, and often inconsistent, security controls across different environments. Also, as apps evolve and API deployments increase, selective coverage is no longer enough.

DHANANJAY GANJOO, MD- India & SAARC, F5

Applications require highly accurate protection for web application firewall (WAF) and API security against DDoS and malicious bots. To dramatically simplify operations, businesses must reduce the number of point solutions and enforce a centralized security policy across the entire estate of apps.

ANAND NAIK, Co-founder & CEO, Sequretek

Application security considerations bring a fundamental change in approach for how new applications are written and consumed by enterprises. Reducing the attack surface by identifying and fixing security flaws (e.g. open port communications, non-encrypted data flows etc) helps organizations achieve better security posture.

▾ Cloud Security

Cloud environments are becoming increasingly popular as a target and effective cloud security management is essential to ensure business continuity, protect revenue and confidential data. Mandiant predicts that cloud compromise and abuse will continue to grow in tandem with enterprise cloud adoption throughout 2022.

Cloud Security Posture Management (CSPM) can help to adequately address security risks across various cloud environments. Also, cybersecurity concerns can be dealt with programmatically, with solutions and approaches like the 'Security as Code (SaC)'.

SANJAY MANOHAR, MD, McAfee Enterprise India

As organizations build cyber resilience in an increasingly sophisticated threat landscape, cloud compliance and security will rise in prominence. Having said that, the coming year will still remain challenging in terms of cloud security. According to recent research by McAfee Enterprise and FireEye, the top three cyber risks of 2022 that are the most threatening to businesses in India will continue to be malware attacks, data breaches, and cloud jacking.

BALAJI RAO, Country Manager- India & SAARC, Mandiant

We suspect that organizations using cloud and cloud-hosted providers may become more vulnerable to compromises, as well as errors, vulnerabilities, misconfigurations or outages affecting cloud resources.

SAURABH SETH, VP, eSec Forte Technologies

Businesses also create siloes between cloud and on-prem and between different teams that have shared responsibilities. Besides, there are a few loopholes in terms of Data classification, Access controls, technology silos, Insecure APIs, misconfiguration, lack of visibility that make Cloud even more vulnerable.

ARUN BALASUBRAMANIAN, MD- India & SAARC, ServiceNow

In a hybrid work environment, a single data model and integrated cloud platform capabilities are essential for productive business. Centralized traffic analysis, network monitoring, and web filtering require fewer policy and software updates, freeing up time for more technical work rather than monitoring multiple systems. Governments and businesses realize the benefits of linking digital foundations to cyber security strategy. Boards understand cyber security risks are a business risk and that if you don't have the right visibility of your cloud environment it is difficult to monitor, protect and respond to incidents and potential breaches.

VISHAK RAMAN, Director, Security Business, Cisco India & SAARC

As more companies move their workloads to the cloud, the traditional way of protecting digital assets is no longer enough. Today's cloud requires security that is easy to deploy, use and maintain and builds intelligence into every control point. It requires a zero trust framework, cloud-based security technology, and intelligent security automation to brace the emerging cyberattacks. According to a Cisco study, nearly 60pc of organizations in India are expanding their investments in cloud-based security technology plans.

▼ Data Security

Data Security continues to be a challenge as there has been a shift of the business networks to the Internet. As businesses are expected to adopt a data-driven approach from system-based forecasting and automation driven by AI, data is now likely completely embedded within every process, from decision-making to end-to-end interaction. Amidst all this, managing data effectively and ensuring data security is anticipated to be critical for every organization.

Also as remote work models shift to 'hybrid work' models, organizations have stepped up

the use of cloud-based collaborative tools for enhanced flexibility, but often with inadequate protection measures. This has vastly increased the risk of sensitive data getting compromised,

It is important to understand that security isn't the only team responsible for data security. They may have a specific data security solution for which they have the approved budget, but that does not make them solely responsible.

▾ Network Security

Organizations are developing hybrid IT architectures, comprising data centers, campuses, interconnecting branches, home offices, and multi-cloud deployments. This has led to an expanded attack surface while the intensity and sophistication of cybercriminals continues to increase.

To address this challenge, organizations need to adopt a security-driven networking approach that weaves core security capabilities combined with actionable threat intelligence deep into every environment of their network.

RAJESH MAURYA, Regional VP, India & SAARC, Fortinet

A security-driven networking strategy enables organizations to have complete visibility across their entire network—from the core, out to the branch, the cloud, the home office, and the emerging edge—helping them to keep relevant, competitive, and resilient. With security woven into their core, networks can also evolve, expand, and adapt to the next generation of digital innovation, including hyperscale, hyperconnectivity, and 5G+ environments.

RAJESH KUMAR S, Head- Systems Engineering Enterprise & Govt., Juniper Networks

As attack surfaces grow because of a distributed workforce, companies must consider how AI and automation can fundamentally shift network operations from reactive troubleshooting to proactive remediation, minimizing the risk and impact of cyberattacks."

DEBASISH MUKHERJEE, VP- Regional Sales, APAC, SonicWall

To combat growing security challenges, more organizations are migrating away from traditional firewalls that focus only on stateful packet inspection (SPI) and access control rules to next-generation firewalls. New Gen Firewall's (NGFW) have transformed network security by providing more robust protection against emerging threats. In addition to traditional firewall features, NGFWs feature a tightly integrated intrusion prevention system (IPS), real-time decryption and inspection of TLS/SSL sessions and full control and visualization of application traffic as it crosses the network."

▾ Embracing Zero-Trust

To effectively combat cybersecurity threats in the coming year, organizations must make cybersecurity a business priority. However, many enterprises are still approaching security with the outdated notion of a protected, firewalled corporate network. The first step businesses can take to strengthen their cybersecurity posture is to reframe their security strategy to focus on both external and internal attacks. This means moving away from the old perimeter-centric approach to security, towards a Zero Trust model that focuses on granting the right people the right access at any time, regardless of location.

One of the key shifts that we are witnessing is that organizations are accelerating the switch from VPNs to Zero Trust Network Access (ZTNA) to increase business resiliency and

foster end-user productivity. Fundamentally, ZTNA runs on the principle of "trust no one" and determines if a user or device is suspicious by looking at several factors, including the user, device, network, and access request at a particular moment in time. In fact, as reported by Gartner, 60pc of businesses will phase out their VPN and replace them with ZTNA by 2023.

Prakash Maharaj, Regional Sales Manager, Jamf, India said, "As work landscapes continue to evolve, organizations have internalized the importance of building an infrastructure that is not just result-focused and collaborative, but also offers uncompromising security. With hybrid work becoming the new norm, we will see a lot more organizations, hospitals, schools, etc. adopt advanced security models like ZTNA in order to create a robust data protection strategy.

Alok Khandelwal, MD, Accenture Security Lead- Advanced Technology Centers, India Implementing offensive security frameworks and Zero Trust with a strong focus on digital identity will also be crucial towards building a strong enterprise security architecture.

VISHAL SALVI, CISO & Head- Cyber Security Practice, Infosys

Built on the least privilege access policy, zero trust security is the need of the hour for enterprises looking to securely fasten their pace of digitization. With identity becoming the new perimeter, zero trust is the only way forward to maintain a strong security posture.

HUZEFA MOTIWALA, Director- Systems Engineering, India & SAARC, Palo Alto Networks

To deploy Zero Trust effectively, companies must adopt a platform approach that leverages next-gen, cloud-delivered tools for better visibility, continuous validation, and automated protection. Relying on such tools is especially important given the lack of cybersecurity staffing and expertise in SMEs.

NITIN VARMA, MD- India & SAARC, CrowdStrike

Modern organizations need a cloud-native, holistic end-to-end platform approach to tackle and remediate threats quickly. Effective counter measures that CISOs can initiate today include integrating a managed threat hunting program to help stop the most sophisticated threats before they turn into breaches and establishing an identity-centric Zero Trust architecture.

SUMIT SRIVASTAVA, Solutions Engineering Manager- India, CyberArk

With endpoints having migrated outside of the perimeter, security has not necessarily kept up with these altered circumstances, while the need to access corporate data and assets has not changed, even while working remotely. This is why a Zero Trust approach, allied with least privilege principles, is essential to secure the identities and access on endpoints to address the risks associated with these assets. Failure to implement this approach will significantly ease an attacker's job.

"Embarking on a least privilege strategy and the adoption of zero trust tactics requires a platform approach with products that are integrated by design. In practice, traditional multi-vendor strategies are simply too complex and incapable of addressing the volume, variety, and velocity of data and threats found in today's networks. ZTNA solutions need to be tightly integrated. You can then implement least privilege strategies by identifying and classifying all the users and devices that seek network and application access, assessing their state of compliance with internal security policies, automatically assigning them to zones of control, and continuously monitor them, both on and off the network, said Rajesh Maurya of Fortinet.

Focused Digital Campaigns...

PCQUEST

VOICE&DATA

DATAQUEST

DQ Channels

CIOL

"IN THE MIDDLE OF DIFFICULTY LIES OPPORTUNITY"

Enable your business in this challenging time with CyberMedia digital offering...

We ENGAGE with your AUDIENCE

Large Enterprise / Medium Enterprise / Small And Medium / Channel Eco-System / Start-up / Developer / End Cosumers / Gaming Community

HOW TO BETTER A DIGITAL BRAND STRATEGY

- Branding
- Response Generation
- Webinar
- Virtual Round Table
- Custom Program
- Virtual Event

Create a successful brand focused campaigns with :

Harminder Singh, Associate Vice President - Online Expert, harminders@cybermedia.co.in

Tips to create a secure ‘Work from Home’ culture and practices

The future of work is remote and hybrid and there is no way organizations can afford to ignore this trend. A recent Gartner survey shows that 76pc of employees have an expectation for continued flexibility, and a growing majority of organizations are ready to support them with hybrid work.

The pandemic has significantly forced organizations throughout industries to become more digital. The growing dependency on technology to enable remote work and online collaboration has become the new normal. This transformative change also implies that new cyber-attacks can surface and threaten the data security of an organization.

According to Mercer Study carried out in 2021, 70pc of organizations have shifted to a hybrid model of working post the pandemic. In a study conducted by HP's Wolf Security division, 83pc of respondents opined that work from home has become a 'ticking time bomb' resulting in a breach of their organization's networks. So, thwarting security risks while working from home needs a disciplined approach to handling digital assets.

While employees working within the confines of the corporate network will have the security and privileges inside the firewall, organizations find it difficult to manage employees accessing data and applications from outside of their network.

Organizations working with remote connectivity solutions must be mindful to keep their communications, data, and infrastructure secure and private. It is important to remember that, in doing so, employees are using their home networks to connect to global servers. Using solutions like VPN while working from home on your devices can go a long way. It was initially meant only for enterprises and is now also available in security solutions for consumers too. VPN can help protect your connected devices against rouge Wi-Fi attacks, evil twin attacks, DNS spoofing, ARP spoofing, HTTPs vulnerabilities, and other such online threats.

Primarily, Identity is a security perimeter, so securing the identity should be the focus for everyone. Keep updating the security credentials of all online accounts and

RITESH CHOPRA, Director- Sales & Field Marketing, India & SAARC, NortonLifeLock

> Consumers should also be aware that if you check your emails on your phone or access your bank account or even shop online, apps tend to target communication networks when users log into an unsecure or faulty network to gain access to this data. To help them keep their passwords unique and not lose track of new passwords.

utilize two-step authentication steps. To ensure the protection of identity, modify (login credentials, device you use to log in, application you are trying to access) using an additional layer of authentication i.e., MFA (Multi-Factor Authentication). Enabling MFA is an effective way to protect yourself while interacting with the digital world, via OTP, authenticator app, Fast Identity Online (FIDO2) key authentication, etc. Interestingly, Microsoft is focusing a lot on password-less authentication. Moreover, the Microsoft Authenticator app, Windows Hello for Business is providing higher security and higher usability in terms of MFA.

Here are some of the best remote working security recommendations to keep you and your employees safe while working from home.

▾ At home, install antivirus and internet security software

Investing in a complete antivirus package for you and your staff is one of the most effective security advice for working from home. Emails are necessary for communication among coworkers. They are also one of the most easily exploited and compromised modes of communication. Keep an eye out for email frauds and make sure your email security is up to date.

▾ Ensure that your passwords are both strong and secure

Strengthening your passwords and

ensuring that you have optimum password protection across all of your devices is one of the simplest yet frequently ignored ways to secure yourself when working from home. Passwords should be used on all of your devices and apps. Using a password manager to help you keep track of all your passwords.

▾ Ensure that all the software are updated

When you get reminders that software updates are available for your computer, laptop, tablet, or mobile device. Don't wait. Update. You can configure your devices to update automatically also. Encourage your teams to upgrade their software to the latest version supported under the company's security policy. Updates help patch security flaws and help protect your data. Updates can also add new security features to your devices and remove outdated ones.

▾ Use a virtual private network (VPN)

Companies should seek measures to improve the security of their VPN. Using the most secure authentication method feasible helps improve VPN security. Many VPNs employ usernames and passwords, but you might want to consider switching to smart cards. For VPN access, you can additionally improve your encryption strategy.

▾ Protect your Wi-Fi network at home

Strengthening the security of your home Wi-Fi network is one of the simplest ways to assure cybersecurity for remote workers. You may accomplish this by following a few simple steps. Rather than depending on the router's default password, create a strong, unique password. Make sure network encryption is turned on. Make sure you're using the most recent firmware version.

▾ Make use of a centralized storage system

If you suspect that your employees are unaware of or unfamiliar with your storage service, or that they are still storing files locally, ensure that they are aware of the centralized service. If your firm is hacked and local data is lost, destroyed, or compromised, you'll be more likely to have a backup of critical information. Important documents will also be safer with this strategy, as they will be safeguarded by the firewall tied to your centralized storage system.

> Security features like end-to-end encryption or multi-factor authentication for accounts and individual incoming connections to strengthen the secure usage of its connectivity solutions. Companies can keep their critical systems and infrastructure safe while benefiting from the advantages of remote connectivity.

KRUNAL PATEL,
Director & Head-Business, India & South Asia, TeamViewer

▾ Safeguard your online banking

If you're in charge of a company's finances, you need to make sure that money is stored and transferred in the safest possible method. It's critical to only use certified software and services when dealing with money. Make sure you're using a Secure Hypertext Transfer Protocol to access a banking website. Passwords can be tightened to improve the security of your corporate and personal bank accounts.

▾ Keep online meetings safe

Working from home means taking part in virtual meetings, which require the use of your webcam. Unfortunately, savvy hackers can easily access your webcam without permission, compromising your privacy. Invest in a sliding webcam cover. During video calls, use the "blur background" feature if your platform has it. This can prevent people in your conferences from spying on objects in the background of your home, which can often include sensitive data about you or your clients.

Avoid oversharing your screen during online meetings. Try not to leave any windows open that you don't want to share. It's also a privacy issue. You might accidentally share content that is not meant to be viewed by others. ■

DATAQUEST

Research Partner
CMR

UNVEILING DATAQUEST 17TH EDITION RANKING OF TOP 100 ENGINEERING COLLEGES MARCH 2022

The value that academic research, reskilling and lifelong learning bring to the space of talent transformation - Prof. Debabrata Das, Director, IIIT Bangalore

Several jobs will be created due to demand spurred by new tech.
- Richard Lobo, executive vice president, & head HR, Infosys

GRAB YOUR COPY TODAY

Form Link
https://bit.ly/3J1e0nE

FOLLOW US TO GET THE LATEST UPDATES ON TECH, TRENDS & TECHNOLOGY:

Dataquest_India | Dataquest | dqindiadotcom

Leverage Dataquest platform & network.
Write to Rajiv Pathak I Manager, Marketing I rajivp@cybermedia.co.in I +91 8010757100

A CyberMedia publication

Security risks that lurk deep inside the Metaverse

Soma Tah & Ashok Pandey
somat@cybermedia.co.in
ashokpa@cybermedia.co.in

As the world of Metaverse is still unfolding before us in layers, we don't know about the potential risks or security loopholes yet. Although we can use existing techniques to protect ourselves in the Metaverse, it may not be sufficient to thwart attacks that have never been seen before

The growing dependence on advanced digital technologies to transform work and leisure have expanded the cyber attack surfaces leaving individuals and organizations exposed to greater cyber risks and many expressed concerns that the situation is likely to get out of hand as people and businesses start discovering new ways to collaborate, interact, trade, buy, and work in the metaverse world.

Digital world has internet-based applications to make our life easier and the metaverse has potential to become a transformative medium for human engagement. It can enhance our digital experience and engagement further by bringing virtual, 3D environments and immersive technologies together. Users can navigate this online world similar to the way we traverse the real world but with digital avatars. With the concept of metaverse becoming a reality, the lines between digital and physical spaces will become even more blurry. But what could be the downsides?

▾ Vulnerabilities and security loopholes that are likely to plague the Metaverse

Because of its infrastructure, the metaverse is expected to bring totally new cybercrimes, in addition to the usual phishing, malware, and hacking. First, cybercriminals will have plenty of possibilities thanks to the metaverse's personal nature and the data it generates. VR headsets and digital avatars provide a more intimate look into users' real life than anything that could be shared on social media. Second, the AR/VR devices that power the metaverse collect a huge amount of personal user data such as biometric information, which opens a window for potential cyber hacks/attacks. As the metaverse evolves. the risks to the user data will also increase manifold. Third, technologies that are powering the metaverse will require robust IT devices and their firmware, and hence, these are the most critical areas for cybersecurity.

Cryptocurrencies and non-fungible tokens (NFT) are widely used in the metaverse, and they might be appealing targets for cybercriminals for a variety of reasons. Pramod Sharda, CEO, IceWarp India & Middle East said, "Monitoring and defending attacks in the metaverse will not be simple. Cryptos/Virtual currencies and NFTs will be used largely leading up to crypto phishing attacks, crypto jacking for fraud, thefts, as attackers' identity can no longer be traced for such transactions." Vulnerable VR headsets causing privacy issues for metaverse users is another concern, he said.

Vivek Sharma, MD- India, Lenovo Infrastructure Solutions Group (ISG) explained the issue in detail. "Metaverse

relies on IT infrastructure along with external devices such as VR headsets to allow virtual access. While organizations are continuing to strengthen the end-point security, the challenge of securing IoT-based devices is an added pressure on the IT and requires a security best practices overhaul. Unprotected devices can compromise not just individual identity; but also lead to ransomware, business data breach, and in some cases physical threats."

Researchers have indicated some potential malicious cyber activity that's only possible in an immersive virtual setting such as eavesdropping or complex social engineering attacks. "AI-based synthetic content such as Deepfake and social engineering threats are among the biggest risks posed by the digital world and metaverse as of now. Exploitation of Metaverse environments by hackers, companies and in some cases adversary states pose a big threat to individual privacy, corporate information and intellectual property espionage," said Anand Naik, Co-founder and CEO, Sequretek.

Experts even warned that disruption in digital security owing to innovations in the Metaverse could have far-reaching consequences due to the multisensory nature of the environment. According to Rahul Mahajan, CTO, Nagarro, "Metaverse experiences are designed to be immersive and close to reality, the digital security risks that occur in such an environment are a real threat as well. Security incidents in the Metaverse hence are exacerbated, leading to extreme human responses."

PROF. MOHAN RAM C, Adjunct faculty, IIIT Bangalore

As it stands currently, new technologies like VR, AR, etc., come with security as an afterthought, not built by design. This needs to change.

ANAND NAIK, Co-founder & CEO, Sequretek

AI-based synthetic content such as Deepfake and social engineering threats are among the biggest risks posed by the digital world and metaverse as of now.

> Cybercriminals will have plenty of possibilities thanks to the Metaverse's personal nature and the data it generates. VR headsets and digital avatars provide a more intimate look into users' real life than anything that could be shared on social media.

How do you protect yourself in the relatively unknown world of Metaverse?

So, is there a way to keep cybercriminals out of the metaverse? Well, the answer is 'No'. In fact, in a digital realm, it will be more difficult to identify bad actors, thus making the legal recourse even more difficult for victims.

"For the Metaverse, the security challenges are heightened due to the level of valuable personal data that users might potentially share digitally. These can include biometrics and personal and financial data to create a 'digital self' within the Metaverse. At the same time, the data will be shared in real-time, making it difficult to determine exactly what personal data is shared, with whom, for what purpose and when it is destroyed. This makes it difficult for users to exercise control over their data," explained Sidharth Pisharoti, Regional VP, India, SEA & APJ Carrier, Akamai Technologies.

Piyush Jha, SVP, Strategy & Technology APAC, GlobalLogic said, "The traditional approach towards security cannot work in the new digital world. Understanding the risks inherent in online activity and deploying the right

cybersecurity resources to protect yourself and your organization is key to remaining cyber resilient in this new age. Security should be an integral part of the business requirements rather than technical and compliance requirements only." Organizations must take a security-and-privacy-by-design approach when building products for the Metaverse.

Serge Gianchandani, CEO & CPO, MetaMall said, "We feel that Metaverse can be made very secure with the right choice on tech and protocols. It is important to secure both platform and user data security. Following both privacy by design and privacy by default methodology are a must. Wherever it is not necessary, default is masking the user details and allowing the user to configure his privacy settings. Strictly maintaining protection and testing against all top 10 OWASP vulnerabilities, following encryption of all information at rest and transit, and strict data access and password policy between servers and for clients are some of the things businesses should keep in mind, while embracing the metaverse world."

Prof. Mohan Ram C, Adjunct faculty, IIIT Bangalore said, "As it stands currently, new technologies like VR, AR, etc., come with security as an afterthought, not built by design. This needs to change as security must be considered as part of the coding stage itself. Our application and software developers must also remain cognizant of the importance of cybersecurity measures as they create new applications in the Digital world and Metaverse. Companies developing the applications for Digital World and Metaverse must invest in training their staff in development, with a 360-degree cyber threat perspective as well as methods/tools to avoid the common pitfalls in the coding."

"The Metaverse heralds the beginning of a new era in technology. While the notion is laudable and has found applications in IT, gaming, and fashion, it is built on disputed AI technology, the authenticity of which is dependent on the designer. Consumers are silently voicing their concerns about cryptocurrency's fragility, the insecurity of IoTs and wearables, and the transparency and ethics of AI," cautioned Apu Pavithran, Founder & CEO, Hexnode and Mitsogo. Time will tell how far we have progressed in preparing for the metaverse, said he.

Sooner or later, the need to construct a secure and trusted technology ecosystem for the metaverse is going to be a critical consideration for the metaverse early-movers, which will also help in building structures, algorithms, frameworks, regulations, and policies within hardware and software development cycles to address the elements of safety, privacy, and security within the DNA of the technology, suggested experts. Importantly, government, academia, industry, and civil society decision-makers all must collaborate and deliberate on the various issues concerned with security in this emerging technology. ■

How secure is your Smart Home?

Marthesh Nagendra
pcquest@cybermedia.co.in

Connected home networks present numerous cyber security risks as vulnerable connected devices could compromise the security of your privacy and safety of your data

Cyber-attacks are on the rise and are becoming highly sophisticated. With the fast proliferation of smart home devices, end users are becoming increasingly more vulnerable to potential security breaches. In just a few clicks, one could unwittingly download malware to a smart device, falling prey to a hacker's malicious intent.

TVs and entertainment systems, smart speakers, lights, cameras, outlets, thermostats, home appliances, security alarms, locks, doorbells– these are all products that have added 'connectivity' to their list of features over the past few years. Using WiFi to become accessible over the internet for a whole host of features, each of these products could become a potential entry to your home network.

The lack of sufficient protection when setting up an 'Internet of Things' device coupled with not keeping up with current updates from the manufacturer are two of the primary reasons why hackers are able to gain access to IoT devices. It does not require much time or a very sophisticated method to accomplish this either.

For example, a digital video recorder with factory configurations that are public is a sure target, discoverable by the bad guys in minutes.

Manufacturers of IoT devices do their best to strike a balance between security and practicality in the configuration of their products. But the final word on how well protected the smart device is from cyber-attacks belongs to the end-user, who enables options that agree with their needs and makes the conscious decision to install updates or to ignore them.

Intrusion Alert: Security Threats to Smart Devices

The typical IoT device does not come equipped with a way to inform who has access to it and from where, which makes it difficult for the average consumer to spot an intrusion. What's more, a gadget that is part of a botnet often performs the same, without any visible or straightforward indicators that it has been compromised.

Connection logs and router management interface typically include data to signal potential security incidents, but such critical data is not very user friendly.

By the time the obvious signs of an intrusion appear – for example, abnormal activity due to setup modification change, denied access to the configuration page because of changed credentials, it may already be too late.

Ignoring firmware updates from IoT makers leads to the same fate, as hackers customize the reach of their scanning tools to identify gadgets with documented vulnerabilities, and then attack them with the appropriate code. Cyber assaults such as these are deemed successful as long as the product is accessible directly over the web, even against a custom setup.

If you do choose to take advantage of the benefits a connected smart home provides, you will want to outsmart potential intruders to ensure you are the one in control of your data and devices. You might want to consider a level of network protection that can inform you of the health of your network and can provide you with the information and the tools to stay on top of things.

Detect and Protect: Block the Hidden Backdoors into your Home

In addition to manufacturers enhancing the security of their products, end users will benefit most if they have access to an efficient and intuitive application that can accurately identify and address any malicious activity on their network and smart devices.

MARTHESH NAGENDRA, Country Manager- India, ME & SAARC, NETGEAR

Companies should look for complete security solutions for the connected home that can protect all Internet-connected devices present from malware, stolen passwords, identity theft, spying, and more. A solution that runs a Vulnerability Assessment engine weekly on devices connected to your network to identify any possible misconfiguration or flaws. Some of the checks performed look at open services (SSH, Telnet) that may inadvertently expose the device to the outside world, or for default credentials known to ship with the device. Weak passwords set by the owner are also identified and reported. This is done by running dictionary attacks that go through a specified set of words and assess their strength as a password.

Making your home network safe should be a priority if you want to avoid the security risks that smart home devices pose. Since all IoT products connect to the wider web through the network, it is logical to enforce protection at that gate to detect and protect you from the risks of an Internet of Things connected world. ■

The author is Country Manager- India, ME & SAARC, NETGEAR

Who comes after the Spiderman takes off?

Pratima H
pcquest@cybermedia.co.in

Cyber insurance is no more a footnote in the backyard of any enterprise's IT strategy. It is the turnstile now. But is it helping enough to let the right future arrive in time?

Insuring an ice-cream taster, a wine connoisseur, a food critic, a footballer's leg, a guitarist's hands, a beautiful smile! That could have sounded outrageous some years back. But John Harrison, Angela Mount, Egon Ronay, David Beckham, Keith Richards and Julia Roberts, indeed, turned out names to be said in the same breath as the word 'insurance'.

Some years back all this would have been implausible. But people and companies, paranoid hearts and cautious minds, do prepare for all kinds of contingencies. That's why we have heard of a Derbyshire Whiskers Club which insured their beards against fire and theft. That's why, apparently, there are policies taken to be well-equipped for all shades of disaster-days- from kidnapping, alien abduction, a no-girlfriend Valentine day, a cancelled wedding and even the possibility of turning into a vampire or werewolf!

It may sound funny but definitely not in the insurer's mind. So if cyber-insurance still sounded funny and unnecessary to an enterprise, all that anyone needed was a blow-after-blow knock-out of the last two years. From supply-chain attacks like Solar winds to out-of-the-blue cloud outages, to sudden-but-merciless ransomware attacks, to open software cracks and zero-day wounds like ProxyLogon and like Log4j, to data dents at major tech giants, oil pipelines, automotive majors – the average CIO, CXO and CISO had many a sleepless nights in the last few months.

And all this costs the CXOs more than mere stress or embarrassment. It translates into money, pretty soon, and pretty huge. As per an IBM-Ponemon Institute reckoning, the average cost of data breach is past $4 million as seen in 2021. Not just that, lost Business aspect contributed as much as 38 per cent to Data Breach costs. Turns out that Customer personal data was part of 44 per cent of breaches, while compromised credentials facilitated 20 per cent of data breaches.And the global average cost of cybercrime was estimated to touch $6 trillion annually by 2021's end.

According to IBM, the average cost of a data breach has now reached over $4 million, while Mimecast estimates that the average ransomware demand levied against US companies is well over $6 million. The world record for the largest payout, made by an insurance company this year, now stands at $40 million.

What also comes up worth noting (in the 2021 Cost of a Data Breach Report or CODBR) is that even if the most common threat vector was compromised credentials, cloud misconfiguration did emerge as the third most-common threat. It accounted for 15 per cent of breaches.

Does that mean that insuring against cyber-risk and IT mishaps is no different than driving a car or taking a house or guarding your valued possessions? Looks like everything has to be accounted for – even third-party risks? And the higher the risk, the higher the cost of insurance- in all insurance-logic. Is that something enterprises are willing to consider?

Financial Impact-Calculations

- Business Email Compromise (BEC) - $5.01 million
- Phishing - $4.65 million
- Malicious insiders - $ 4.61 million
- Social engineering - $4.47 million
- Public cloud-based breaches - $4.80 million (average)
- hybrid cloud-based breaches - $3.61 million

Source: IBM-Ponemon study (Global)

TRISHNEET ARORA, Founder, Director & CEO, TAC Security

While cyber insurance may generally be under the purview of CIO or CISO team, there is a gradual shift happening with other CXOs particularly CFOs and even CEOs too being actively involved in the deliberation.

How much would they cough up for that not-so-one-in-a-million-chance anymore of 'when the lightning strikes'? And how much would insurers help here in a constructive and deep-rooted way that builds an enterprise's clarity and posture on cyber-security instead of just lining their pockets with heavy premiums and exclusions?

These are questions that cannot come with an assurance of right or ready answers. But asking them early would be the first premium to pay on this path. Let's confront these unpleasant, but crucial, what-ifs.

▾ Mr. Butterfingers, please stand up

Have enterprises become extra cognizant and candid about facing the gaps, mistakes and vulnerabilities they have from a cyber-risk angle? More so after the pandemic year?

Daniel Garcia-Diaz, Managing Director, Financial Markets & Community Investment, U.S. Government Accountability Office gives a snapshot at how the area of cyber-insurance has changed in the last two or three years.

"In our May 2021 report (GAO-21-477), we noted that take-up rates of cyber insurance have risen over the last 5 years, from about 26 percent to about 47 percent. However, take-up rates of small and mid-size entities lagged those of larger entities. They also varied by industry, with, at the time, sectors such as hospitality, manufacturing, education, and health care showing the highest take-up of cyber insurance. Also of note, industry sources told us there has been an increase in cyber-specific policies, compared with packaged policies. This may reflect a desire for more clarity about what is covered and higher cyber-specific limits."

Cyber risk now tops boardroom agendas as most companies have accelerated their digital agenda due to the pandemic and the bad actors have an increased surface area to attack, reveals Anup Dhingra, MD, FINPRO, Private Equity and M&A, Marsh India Insurance Brokers Pvt Ltd. "Average cost of a data breach in India is now $2.21mn, up from $2mn, based on IBM cost of a data breach report. There has been a slew of many high profile data breaches that have been recently reported not just in ecommerce or banking, the sectors that were most affected in the past, but also in pharma companies, pizza makers and many other companies in traditional sectors that were largely believed to be safe from such cyber events."

JITENDRA MOHAN BHARDWAJ, CIO & CISO, Coforge

The average cost of recovering from a cyberattack, especially ransomware, is 10 times the size of the ransom payment as it includes remediation costs, business downtime, lost orders, and operational costs.

He interprets the implications on investments and adds that from just a conversation item cyber risks and their mitigation strategies are now the most important and resource intensive investment area for companies. "Gartner estimates that spend on cybersecurity will cross $172bn in 2022, up from $155bn in 2021. However, these investments very soon reach marginal utility thresholds. The bad actors have to get lucky only once and the security has to work perfect all the time. On top of the weakest link is usually people (in the form of a careless employee) and not systems usually."

So - many firms have consciously chosen risk transfer through insurance as a balance sheet protection mechanism, he explains. "Early adopters and the biggest buyers of insurance still remain IT/ITeS, BFSI, and ecommerce giants, who usually buy limits of tens or hundreds of million dollars; but lately many manufacturing firms from pharma, auto, industrials as well as even power & energy firms as well as telco and consumer firms have started showing interest made purchases. Public sector enterprises (outside of PSU banks) continue to have least coverage, as well as construction firms."

There's a fundamental question that organizations need to address when they think of cyber-insurance, suggests Dr. Lawrence A. Gordon, the EY Alumni Professor of Managerial

Accounting and Information Assurance at the University of Maryland (UMD), Robert H. Smith School of Business.

"How much should we invest in cybersecurity? In addressing this issue, organizations need to consider the following three items. First- the probability of a cyber-breach (derived from the combination of the threat and vulnerability of a cyber-breach), Second- the potential loss from a cyber-breach, and third- the productivity (in terms of reducing the probability of a cyber-breach) of investments in cybersecurity. The Gordon-Loeb Model provides a framework for integrating the above three items so as to derive the optimal amount for an organization to invest in cybersecurity."

Cyber Insurance pricing has increased on an average of 96 per cent, year-over-year, in the third quarter of 2021 as organizations faced a daily onslaught of cyberattacks. The third quarter increase was a 40-percentage point rise over the prior quarter, and the largest since 2015. No wonder, the multi-fold increase of cyberattacks called upon a variety of changes in regulations and introduction of best practices for mitigating the risk, underlines Jitendra Mohan Bhardwaj, CIO & CISO, Coforge (erstwhile NIIT Technologies). "In the cyber insurance market, insurers usually require insured to take on higher retentions (similar to deductibles), and others to apply co-insurance on some or all elements of coverage, particularly for ransomware. Reinsurance policies are also experiencing an increase in demand and are actively shaping the market via treaty terms and modelling. With their potential insurability on the line, CISO's need to emphasize on cybersecurity controls now more than ever. They must look towards in-depth defense by analyzing the root cause and by continuous evaluation of other relevant data points. At Coforge, we focus on 'Engage with the Emerging'; offering solutions that safeguard our customers from cyber risks and data privacy breaches and therefore help in instituting a robust risk management strategy for our customers."

Ram Movva, Chairman and Co-founder, CSW (Cyber Security Works) echoes that the Cyber Insurance sector is growing rapidly in India. "According to a Forbes Report, Indian organizations are going to spend $3 Billion on Cybersecurity in 2002. Indian organizations and firms top the list of most vulnerable entities for ransomware attacks, therefore, it is not surprising that many enterprises have started buying cyber insurance."

RAM MOVVA, Chairman & Co-founder, CSW

Today, most of the spending by enterprises is for post-incident analysis and recovery, while they should be using AI and ML models to predict what vulnerabilities within their network could be weaponized and turned against them.

Strikingly enough, insurance is becoming an integral part of a CIO's budget, Movva avers. "It's hardly surprising given the fact that organizations are experiencing data breaches left, right, and center, and each incident is costing them in terms of money and reputation. No one wants to be in the news for the wrong reasons. I believe, in the future, underwriters may not issue policies, if they think it is too risky."

The view is the same on the global tree-tops. According to the Global Risks Report 2022, while the top long-term risks relate to climate, the top shorter-term global concerns include societal divides, livelihood crises and mental health deterioration.

The report also explores four areas of emerging risk and one of which is cybersecurity with experts underlining that as cyber threats are now growing faster than our ability to eradicate them permanently, it is clear that neither resilience nor governance are possible without credible and sophisticated cyber risk management plans.

Trishneet Arora, Founder, Director & CEO at TAC Security seconds that with cyber breaches being reported on a frequent basis, the sense of realization with enterprise community to avail cyber insurance services is indeed on a rise. "A pertinent dampener however is in

the tendency of corporates to refrain from reporting such incidents and instead paying ransomware to hackers. This directly impacts the cyber insurance considerations. In India too this trend is prevalent."

OK, so insurance is becoming a staple feature. But who is laughing all the way to the bank – the victim, the bad actor or the insurance company?

All fires covered, except from the kitchen

What do enterprises do when they are faced with exclusions from the insurer's side? And especially those that are buried way deep into the fine-print?

Like any insurance policy, cyber insurance, too, has certain exclusions that limit the scope of coverage, avers Dhingra. "There are ranges of items that may affect the actual coverage of a claim, and while this list is not intended to be exhaustive, here are a few to keep in mind: Prior acts / knowledge by C-suite or board; Bodily injury/property damage; Governmental acts, seizure, confiscation and Transfer of funds or loss/theft of money."

He explains that there are certain exclusions that can be removed by way of filling up questionnaires or carved back through negotiation. "For example, some insurers are willing to remove Covid-19/ Pandemic exclusion if the insured fills up Covid-19 questionnaire. Similarly, there is a carve-back for cyber terrorism while war and terrorism are standard exclusion in most cyber insurance policies."

Garcia-Diaz reminds how (as per industry participants told) insurers have been tightening policy terms and conditions for cyber policies, including by adding exclusions to traditional lines of coverage and package policies to avoid the issue of "silent cyber" coverage.

Garcia-Diaz also spells out some fine-print that a CISO has to be careful about. "Because cyber insurance is not yet a standardized product, issues with terminology and definitions can be challenges. Language in policies with more than $5 million in coverage can vary greatly, and others, including the Geneva Association have raised concerns about a lack of standard definitions for terms such as 'cyber war' and 'cyberterrorism'. Insurers may also define terms such as ransomware attacks differently."

DR. LAWRENCE A. GORDON, EY Alumni Professor, Managerial Accounting & Information Assurance, University of Maryland, Robert H. Smith School of Business

How much should we invest in cybersecurity? In addressing this issue, organizations need to consider the following three items. First- the probability of a cyber-breach, Second- the potential loss from a cyber-breach, and third- the productivity of investments in cybersecurity.

Movva brings up the need for underwriters and brokers to understand how vulnerable the organizations are before they book the insurance. "Most are merely reviewing process-related policies to fix a premium. That said, even the Enterprises are not aware of what coverage they need when it comes to insurance. They go only by regulatory requirements."

Also when we look at the nature and rise of security attacks – especially ransomware, data-theft, DOS, and outages in the last two years, there is a conspicuous need for new segments or products. Something that has not happened enough as Movva agrees. "Even today, most enterprises and firms in India look at security as a 'point in time exercise' whereas it has to be continuous. Attack Surface Management (ASM) is actively being used in the western world to understand the external exposures of an enterprise. Apache Log4J exposure is a classic example here. Many companies are still not aware of how exposed they are to these vulnerabilities and by the time they know, they become victims of a crippling cyberattack. Indian organizations are still catching up with this trend. They need to wake up and smell the coffee."

Who bells the cat

But smelling the coffee can be tricky on a

Data from a global insurance broker show that its clients' take-up rate (proportion of existing clients electing coverage) for cyber insurance rose from 26 percent in 2016 to 47 percent in 2020.

Higher prices have coincided with increased demand and higher insurer costs from more frequent and severe cyberattacks, as per industry sources.

In a recent survey of insurance brokers, more than half of respondents' clients saw prices go up 10–30 percent in late 2020 alone.

Also, a growing number of cyberattacks led insurers to reduce coverage limits for some industry sectors, such as healthcare and education.

There are policies being offered specific to cyber risk, rather than including that risk in packages with other coverage. This shift reflects a desire for more clarity on what is covered and for higher cyber-specific coverage limits.

The growing frequency and severity of cyberattacks have led more insurance clients to opt for cyber coverage—up from 26% in 2016 to 47% in 2020.

Data Source: US GAO Report

bad-nose day. Which can be almost every day when enterprises are fogged with confusion and complacence. Specially with questions like- Should SLAs or penalty-clauses accommodate and anticipate downtime from the vendor's end? Or should these outage-costs be borne by the enterprise?

There is a lot that can be done, and done better, when it comes to having the right foot forward on security – whether with or without insurance. Movva opines that enterprises must spend money on definitive and predictive technologies that would empower them to patch those vulnerabilities that would be weaponized in the near future. "That would allow them to defend themselves against evolving and adaptive threats. That's the only way to avoid breaches and limit their exposure."

He also seconds that the issue of fine-print cannot be ignored. "Firstly, there are too many fine prints that need to be reviewed and the responsibility doesn't lie only with the CISO. This should be reviewed by their legal team as well so that they understand the risks and know what kind of coverage is needed. The eligibility review process that Policy underwriters' follow for an Enterprise is inadequate. They check if an enterprise has information security policies/procedures or if they have internal audits or third-party audits or pentesting processes and they get their policy. This kind of process is insufficient and flawed."

▾ Umm, what are the damages please?

The cost of insurance and the size of premiums get determined by a lot of factors- the scale of company, the industry's and company's risk profile, its security strategy, its security readiness investments, its cost for third-party liabilities and regulatory fines etc.

The average cost of cyber liability insurance in the United States was $1,501 per year for $1 million in liability coverage, with a $10,000 deductible, if we look at a study from AdvisorSmith Solutions Inc. What is interesting to observe here is that there are a lot of drivers for cost calculation- ranging from location, the type of business, the number of credit/debit card transactions performed, and the storage of sensitive personal information such as date of birth and Social Security numbers.

As to the average cyber policy, it costs $1,485 per year, according to AdvisorSmith Solutions and insurers price products based on risk. This where they rely on historical data, Business size, level of liability coverage,

In India, the Cyber and Data Security Insurance covers:

Cyber, data security & Multimedia cover (Which includes court attendance costs and defense costs, losses arising out of employee dishonesty, loss arising out of hacker financial crime, any loss arising due to loss/damage to document(s))
Data breach notification costs cover
Information and communication asset rectification costs cover
Regulatory defense and penalty costs cover
Public relations costs cover
Forensic costs cover
Credit monitoring costs cover
Cyber extortion cover
Theft of funds cover: In case of cyber incidents or hacking of insured's Bank account, Credit/Debit card and/ or Mobile wallets by a Third Party
Identity Theft cover: Defense cost for claims made against insured by third/ affected party due to identity theft fraud and also provides expense to prosecute offenders and other transportation costs
Social Media cover/ Cyber Stalking / Bullying/ Phishing/ Privacy Breach cover: Provides Defense cost for hacked social media account of insured, bullying and stalking on social media platforms. Also provides expense for prosecution and other transportation costs.
Malware cover/ Phishing cover/ Cyber Extortion cover: Data restoration cost, financial losses and prosecution cost
Unauthorized Online Transaction/ Email Spoofing cover: Financial losses and provides protection against fraudulent use of bank account, credit/debit card, e-wallet by the third party
Media Liability Claims cover: Defense costs against defamation or invasion of privacy due to Insured's publication or broadcasting of any digital media content.

Source: People interviewed for the story

choice of deductible, and security measures at a company. As per the study, hacking, ransomware, phishing and employee negligence were some of the most frequent claims. And risk mitigation does play a role in the calculus, according to the report.

Industry players have often pointed out that the more security measures a company has in place, the lower the insurance premiums for cyber insurance.

Also note that insurers have to watch for their profitability and sustenance. If, as per an April estimate from credit-rating agency Fitch, for every dollar an insurance company made in cyber premiums, it paid out 73 cents last year, compared to 47 cents in claims two years ago – then it's no surprise that cyber insurance policies are shaping into costly iron gloves instead of velvet gloves that they used to be. The attack of ransomware and frequent-plus-

hard-to-guess cyber threat vectors add to the panic.

Insurers also have the pet peeve that organizations lack comprehensive, high-quality data on cyber losses, and cyber policies are devoid of common definitions – all of this makes it hard to estimate potential losses from cyberattacks and price policies in a prudent and win-win way. Some industry participants said federal and state governments and industry could collaborate to collect and share incident data to assess risk and develop cyber insurance products.

The cyber insurance industry faces the challenge of limited loss and event data, reflects Garcia-Diaz. "The changing nature of cyber risk and the lack of a comprehensive, centralized source of information about cyber events for insurers has led to concerns that current prices for cyber policies may not accurately reflect risk. The U.S. Cyberspace Solarium Commission recommended that an entity be created to collect data that would help insurers better understand cyber risk and create better risk models."

Bhardwaj calculates the cost math with a different formula. "According to the 2021 Sophos state of ransomware report, two-third (68 per cent) of Indian organizations have been attacked by ransomware in 2021, with 66 percent of organizations paying an average of $76,619. The average cost of recovering from a cyberattack, especially ransomware, is 10 times the size of the ransom payment as it includes remediation costs, business downtime, lost orders, and operational costs."

Cyber is not just an IT issue; it is an enterprise risk that affects many key stakeholders within the organization, says Dhingra in the same vein. According to recent reports, worldwide security spending is set to breach the $174.7 billion mark, and cyber insurance will account for a certain portion of that.

He indicates that Cyber insurance market is currently a 'seller's market'. "There has been a steady increase in claims in the last couple of years, leading to correction in the premium of cyber insurance. The market is currently going through a hardening phase, which is expected to last beyond 2025. There has been an increase in premium across sectors and

ANUP DHINGRA, MD, FINPRO, Private Equity and M&A, Marsh India

There has also been an increase in demand for retail/personal cyber insurance, which offers protection to individual against identity theft, cyber-bullying, cyber extortion, malware intrusion, and financial loss due to unauthorized and fraudulent use of bank account, credit card, coverage against reputation injury and mobile wallets and legal expenses arising out of any covered risk.

risk profiles with further increase anticipated in this year."

And Bhardwaj explains why the bills get higher. "Just as other parts of the insurance market have undergone significant shifts, hackers are also carrying out sophisticated attacks i.e. Gen 5 or Gen 6 attacks. Insurers are increasingly tightening underwriting requirements and stipulating organizations to adopt security controls that can make a measurable positive impact on their cyber risk exposure. With the cut-throat competition on premium amounts and evolution of cyber crimes, the insurances are also constantly getting expensive."

"While cyber insurance may generally be under the purview of CIO or CISO team, there is a gradual shift happening with other CXOs particularly CFOs and even CEOs too being actively involved in the deliberation, highlights Arora. "As conveyed, cyber insurance premium being expensive or economical is a direct function on the level of vulnerability ₹ risk management preparedness of enterprises- the higher the mechanisms and cyber score, the lower the premium."

Dr. Gordon dissects that Investments in cybersecurity are directed at reducing the probability of a breach (i.e., spending on such activities as encryption, access controls, firewalls, intrusion prevention and detection systems, employee training, etc.) and strategies for transferring the risk

associated with incurring a cyber-breach. "Most people think of the expected loss (i.e., 1 multiplied by 2, in the above paragraph) as the risk of a cyber-breach. An important part of an organization's strategy for transferring the risk associated with incurring a cyber-breach is to invest in cyber-insurance. Thus, purchasing cyber-insurance is (at least from my perspective) best thought of as part of the decision to derive the optimal amount to invest in cybersecurity within the framework of the Gordon-Loeb Model."

But even if you can afford it, and even if it is practical, is buying insurance dotted with some ethical dilemma?

Are we feeding the monster here?

There is an emerging school of thought that peels away some latent dangers of cyber insurance. Buying risk-covers can make enterprises complacent – but that's just a small minefield. The bigger one is that the entire business of cyber-crime thrives on ransomware and victim-compliance. Is it not possible that cyber insurance creates enough cushion here and allows enterprises to pay ransom easily- thus, adding to the vicious loop of cyber-crime and ransomware?

Can we afford to get laid-back or bend over backwards – now in the post-pandemic world where digital is not a suffix but a prefix for everything we do, buy, sell, use, share and work on? Cybersecurity threats are growing–in 2020, malware and ransomware attacks increased by 358 per cent and 435 per cent respectively–and are outpacing societies' ability to effectively prevent or respond to them, captured the Global Risks Report 2022. Lower barriers to entry for cyber threat actors, more aggressive attack methods, a dearth of cybersecurity professionals, and patchwork governance mechanisms are all aggravating the risk. The report also talked about how attacks on large and strategic systems will carry cascading physical consequences across societies, while prevention will inevitably entail higher costs. Intangible risks–such as disinformation, fraud, and lack of digital safety–will also impact public trust in digital systems. Greater cyberthreats will also hamper cooperation between states if governments continue to follow unilateral paths to control risks.

DANIEL GARCIA-DIAZ, MD, Financial Markets & Community Investment, U.S. Government Accountability Office

After holding relatively steady in 2017 and 2018, cyber insurance premiums rose markedly in 2020. In a survey of insurance brokers, more than half of respondents' clients saw prices go up 10-30 percent in late 2020 alone.

"GRPS respondents believe 'cybersecurity failure' will continue to test the world's digital systems over the next two years and, to a lesser extent, in three to five years. No technological risk appears among the most potentially severe for the next decade. This suggests lower relevance to respondents–or a blind spot in perceptions given the potential damage of cyber-risks–compared to economic, societal and environmental concerns." The report cautioned.

On that note

Both enterprises and insurance providers have to take a brave look at what has been going wrong and what can be improved upon in a major way. As Movva recommends, Insurance companies must look at what technologies enterprises are using to continuously learn about their exposures to avoid breaches and what kind of cyber incidents they have been victims of and how they are managing their vulnerabilities post that. "The only way for enterprises to avoid business interruptions and cloud-related outages is to invest in a continuous process of internal vulnerability management and stay on top of their external attack surface to learn about their exposures. Today, most of the spending by enterprises is for post-incident analysis and recovery, while they should be using AI and ML models to predict what vulnerabilities within their network could be weaponized and turned against them."

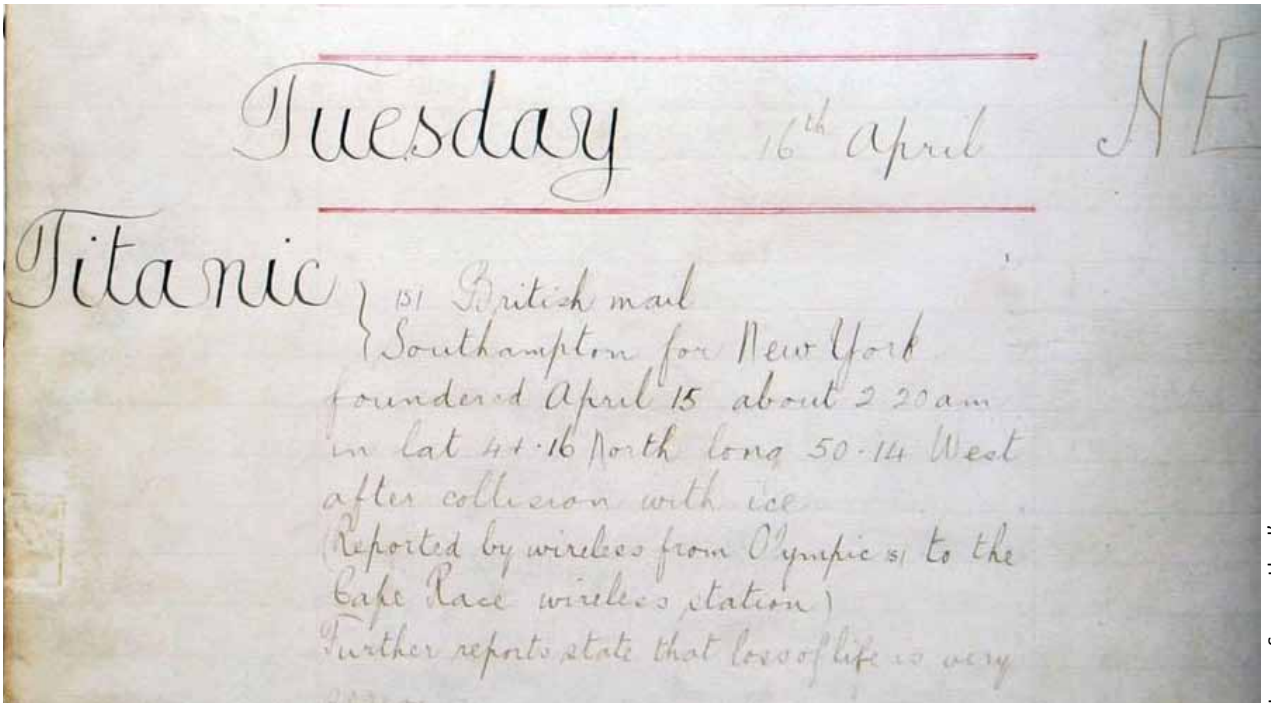


Image Source: Lloyd's

Cyber-risk is hard to wipe away completely. Organizations should strive to manage it to an acceptable level of residual risk, advises Bhardwaj. The most important point to bear, as Dhingra rightly reminds, is that while procuring cyber insurance, CISOs need to be mindful of the fact that it is not a replacement for cybersecurity. "Cybersecurity is the first line of defense and cyber insurance is complementary to good cybersecurity practices. Certain aspects of cyber insurance like adequate deductibles (monitory and hourly), non-cancellation clause, extended reporting period, etc. need to be looked at during policy placement."

An interesting chapter from Lloyd's chronicles is the one where one day in January, broker Willis Faber & Co came to Lloyd's underwriting room to insure the Titanic and her sister ship, the Olympic, on behalf of the White Star Line. That time, this was considered a prestigious risk, with cover for the hull alone standing at £1m – a back-of-the-envelope number in today's sense of £95m. It has been believed that many Lloyd's syndicates put their names on the slip, covering amounts ranging from £10,000 to £75,000. That proudly 'unsinkable' vessel was okayed with a premium of just £7,500.

But Titanic- the unsinkable ship- went down in the freezing waters of the North Atlantic, 375 miles from Newfoundland, in just two hours and 40 minutes. Of the 2,224 passengers and crew, only a few could be saved with lifeboats that were only for 1,178 people – and 1,514 people died.

Yet the ship was insured for over £1m and despite the high levels of claims arising from the tragedy, insurers paid out in full within 30 days. Lloyd's perspective counts the Titanic as one of the market's biggest losses alongside major natural and man made catastrophes like the loss of HMS Lutine in 1799, the 1906 San Francisco Earthquake and the tragic 9/11, Hurricane Katrina and the Japanese earthquake and tsunami of 2011.

From the perspective of a ship's captain, if there were enough lifeboats around, neither the insurer nor people would have suffered a loss that was too hard to replace.

For the captains of today's enterprises- small or big- the lesson rings loud like a SOS – cyber-risk is neither as funny as the risk of losing a taste bud or the risk of a run-in with an alien abduction; nor is it as impossible-sounding as the Titanic's wreck was. The aliens, the vampires, the storms, the ice-bergs and cyber-attacks – are getting eerily real. Let's not be shy to shout and act - Mayday! Mayday! ■

Combating HR Data Threats

Vicky Jain
pcquest@cybermedia.co.in

HR teams need to be equipped with cutting-edge digital tools and an HRMS with advanced security features to make sure that the employee data stays secure, both on-premise and cloud

Whilst innovative, smart technologies have certainly made life convenient and easier for us, it has also paved the way for multiple threats like hacking, security breach and data theft. As per reports, losses from cybercrime skyrocketed to almost $1 trillion in 2020. Cyber security violations are a big threat to organizations and can incur big losses for businesses.

How secure are HRM solutions in the era of cybercrime and data frauds?

The HR department is entrusted with some of the most sensitive data and key details related to employees. Therefore, to mitigate the risk of any threats, HR teams need to be equipped with some of the best applications and tools to treat employee data with the care it deserves. That's where HRM solutions can play a big part. With up-to-the-minute intelligence and hi-tech security, today's HRMS tools are equipped to secure private employee data and ensure global regulatory compliance.

Recent research has shown that HR leaders are putting in more time and resources towards data security. According to the Sierra-Cedar HR Systems survey 2019-2020, there has been a 17 per cent increase in the number of respondents utilizing cybersecurity strategies as compared to the previous year.

Any loss or threat to sensitive employee data such as payroll information, healthcare details, home address, contact information or date of birth has implications well beyond the HR department. It's not just the personal employee data, the entire enterprise faces risk from data breaches or cyber threats, since human resources are central to different processes throughout the organization.

HR leaders keen to invest on new tools

However, thanks to the inception of AI-powered tools, HR departments are now able to protect private organizational and employee data to a big extent. Some of these technologies have the ability to protect against automated malware attacks

VICKY JAIN, Founder, uKnowva

by recognising patterns that can identify doubtful behavior and block threatening online traffic or potential problems in real-time.

Companies are also embracing 'zero trust' policies that use multifactor authentication for identity authentication or network access. Multi-factor Authentication (MFA) confirms user identities with at least two different factors.

With many organizations supporting a hybrid model of work after the pandemic, HR leaders are also investing in digitized experience monitoring tools to gather operational data from the device of a user and proactively come up with an alert to indicate performance bottlenecks as well as identify the gap between perceived and expected user experience.

Keeping data secure with Digital HRMS

Cutting-edge HRMS provides advanced security features to make sure user data stays secure, both on-premise and cloud. HRMS security features cover nearly every aspect of sensitive data security including physical security, encryption of data, controlled access, internal security controls, etc.

Here are some of the key features of

digital HRMS which ensures proper use and protection of data without any privacy or data security risks:

- For high-level data protection, HRMS hosts information on the cloud that helps in the management of critical data in the event of any disaster. Even in the face of any real catastrophe, businesses can expect continued information flow as data is never lost.
- For next-level data protection, HRMS tools employ IP and port-based restrictions along with communication using SSL protocol.
- Systematic data backups across different places and backup upgrades throughout the entire day ensure that confidential and critical data is never lost and can be accessed from anywhere, at any time. Also, periodic automatic data checks allow HRs to assess outdated data and decide whether or not it should be kept.
- Automated data checks are also performed by HRMS tools to discover potential vulnerabilities and reduce the risk of data breaches.

Compared to on-premise HRMS software, the cloud-based HRMS is quite easier to integrate with the existing system. On top of that, it is user-friendly and requires less effort and time to train people to use it. With on-premise HRMS, significant effort is required for maintenance and upgrades.

Data is one of the crucial assets of an organization and to keep HR data safe and secure, it is not only enough to invest in a modern HRMS but ensure constructive collaboration between business owners and HRMS vendors to achieve the desired results. During the implementation of HRMS, every concerned party like employers, vendors, and managers should work together to tackle the security parameters efficiently. ■

The author is Founder, uKnowva

VOICE&DATA

CyberMedia

Hewlett Packard Enterprise | AMD

Presents

TELECOM LEADERSHIP FORUM

21st ANNUAL MEETING OF THE TELECOM ECOSYSTEM

EMPOWERING LEADERS IN TELECOMMUNICATIONS

Era of Convergence

From 5G to GenZ

22 March 2022 | 09:30 - 5:30 PM

Partners

Gold	Digital Transformation	Gold	Connectivity	Telecom	Internet Service	Academia
comviva	accenture	ciena	AT&T	VI	one	APEEJAY EDUCATION

Follow us: @VnDIndia

#TLFIndia | #TLFAwards | tlfindia.in

21st edition of Telecom Leadership Forum will focus on the game changing & key trends in telecommunications industry.

Voice&Data Jury Awards

- Telecom Person of the Year
- Lifetime Achievement Award
- Pathbreaker of the Year Award

Voice&Data Awards for Excellence in Various Categories

KEY DISCUSSION POINTS

Rapid technological change	AtmaNirbhar India	New semiconductor policy
Powering 5G - Next Gen Telecom	Network architecture	Datacentre & Cloud Infrastructure
OTT for profits	AI & Cybersecurity in the network	Make in India
Industry 4.0	Open RAN	Future of 5G
Wifi -6 and Internet of things	Voice, Data & Meta - the next decade	Satcom

SESSIONS CURATED FOR

Policy Makers, Regulators/ Govt. Bodies	CEO'/CTO's/CXO's of Service Providers
CIO/IT Heads of Enterprise Users	Academia/R&D Experts
VAS/Cloud/Content/Application Service Providers	CXO's of Defence/Citizen Networks
Start-ups & Investors	Influencers and Consultants

Acquaint with the quality content and, viewpoints and insights from the experts. Leverage Voice&Data TLF platform and network.

Marketing & Alliances: Rajiv Pathak
rajivp@cybermedia.co.in, +91 80107 57100

For Registrations: Ravi Kant
ravik@cybermedia.co.in, +91 98104 81484

6 Best Practices to minimize the Cloud security risks and threats

Bhavesh Goswami
pcquest@cybermedia.co.in

It's important for organizations to understand that cloud infrastructure itself cannot insulate organizational IT resources from security threats. They need strong security tools to neutralize cloud-security threats

The past decade has witnessed many organizations embracing cloud adoption and this makes cloud security a prominent player for them to thrive in the business game. According to IDC in 2021 the manufacturing industry spent $20 billion, professional services spent $18 billion and the banking sector spent $16 billion for cloud adoption. Also, research says on an average an employee uses 30 plus cloud services at the workplace.

With the ongoing cloud adoption spree, the cloud-security threats are also becoming rampant. The worldwide statistics say that the average cost of data compromise sums up to $3.86 million. Research also says if an organization can fix data breach issues within 30 days of occurrence, they tend to save $1 million. Moreover, if an organization can ensure a complete fool-proof system against security compromise millions of dollars are saved. It is important for organizations to understand that cloud infrastructure itself cannot insulate organizational IT resources from security threats. They need strong security tools to neutralize cloud-security threats.

A wide range of cloud-security challenges like data breaches, compliance with regular mandates, cloud migration challenges, insider threats, lack of IT expertise, and managing unsecured APIs are to be addressed while devising cloud security practices. Organizations must ensure better Cloud Security Posture Management (CSPM) and use of Cloud Workload Protection (CWP). While the CSPM tools help organizations to quickly identify risks by monitoring multi-cloud environments, workloads, teams and to produce useful insights the CWP assists to ensure server workload protection in modern day hybrid data center architectures. Here we have identified 6 best practices to be religiously put into action to build a robust cloud security system.

1. Maintain comprehensive inventory of Cloud-native applications and services

As Cloud adoption has gained momentum across big, small, and medium-sized organizations, the demand for cloud-native application development and container services has soared. Organizations continuously deploy applications and services to the cloud and these newly deployed cloud-native apps and services are vulnerable to security threats. So, from a cloud-security perspective organizations need to have a comprehensive inventory of all their cloud-native services and applications. Importantly, they can employ various CSPM tools to monitor the assets and applications in real-time. Thus, having a comprehensive inventory of newly deployed applications and services help organizations to nullify cloud security threats.

BHAVESH GOSWAMI, Founder & CEO, CloudThat

2. Well-defined Access Management, Data Protection and Monitoring

Granting 'Read, Write, and Execute' access for all members of an organization on IT resources is not a wise move, isn't it? Often mismanaged access-grants prove costly for organizations from the security perspective. So, having a robust access management policy is a key ingredient of a good cloud security practice. The access management policy should ensure proper identification and authentication of users, wisely granting

access rights to users, and systematic enforcement of resource access policy.

The next step is ensuring a reliable data protection mechanism. Implementing Data Loss Prevention (DLP) policies helps to detect, monitor, and prevent accidental or intentional sharing of sensitive data. DLP policies are applicable when data is in following states:

1) Data at rest
2) Data in transit
3) Data in motion

In addition, employing data classification techniques is vital to understand which type of data needs protection and prevention.

Continuous Monitoring and Analysis of IT resources are vital for every organization. An organization cannot show complacency just because they have hired a best-in-industry Cloud Service Provider (CSP). It is important to understand that a CSP monitors only the infrastructure and services they offer and will not monitor the on-premises applications and services developed by your organization. Also, it is important to employ Security Information and Event Management (SIEM) tools to continuously monitor the behavior of IT infrastructure. SIEM tools help to analyze threats and set the automated response to remediate.

3. Rope in encryption and security measures at development stage

Often the misconception amongst many organizations is that implementation of cloud security measures happens only after the resources are deployed to the cloud. But best practice is to prepare a pre-deployment, on-deployment, and post-deployment checklist to assess the types of encryptions and security measures that must be implemented during the design, development, and deployment stages of a software application. So, it becomes mandatory to ensure the security measures are taken during the early development stage of applications by roping in encryption and security features throughout the software development life cycle.

4. Ensure multi-cloud security coverage

Multi-cloud strategy means using services of more than one CSP to leverage the best cutting edge technology features for various needs. As organizations of modern days prefer to use multiple clouds for different services, ensuring that all assets across the clouds are secured becomes important. So, while devising multi-cloud security coverage emphasis should be laid upon: Consistent security policies, automation of security tasks, minimized point security solutions, and single point of control across the multiple CSPs.

5. Timely security review through external audits

We all get our automobiles serviced at regular intervals to ensure no sudden breakdowns are faced, isn't it? Similarly, it is vital for all organizations to get their cloud assets audited at regular periods by an external agency who offers audits to get IT-assets auditing to fix vulnerabilities in your IT resources. As the adage goes, prevention is always better than cure. Getting periodic security reviews is one of the best practices to thwart security risks.

6. Upskill employees and create awareness across the organization

Creating general awareness amongst all employees on the importance of IT security, encouraging them to upskill on security skills earn certifications from prominent cloud providers like Azure and AWS through trainings offered by authorized training partners helps to reinforce awareness amongst employees that the cloud-security is not the sole responsibility of one single department, and it demands collective responsibility of development, operations, and senior management teams.

To conclude, organizations adopting cloud should first choose the right CSP and understand the security tools provided by them in depth. They can easily avoid major security risks by employing the security tools with the right access control configuration, proper encryption methods, and multifactor authentication features offered by the CSPs. ■

The author is Founder & CEO, CloudThat

PCQUEST 35

CyberMedia

35 YEARS OF TECHNOLOGY

APRIL 2022 - COLLECTOR'S EDITION

#PCQ35Years Follow us: @pcquest

Visionaries, Industry leaders & influencers coming together to write about the nostalgic view & expert's insights of 35 years of IT landscape in India

RS PAWAR
Founder
NIIT

VEER SAGAR
Chairman
Selectronic

RAJESH JAIN
Founder and MD
Netcore Cloud

R RAMARAJ
Founder
Satyam Infoway (Sify)

BIKRAM DASGUPTA
Founder &
Executive Chairman
Globsyn Group of Companies

ARVIND GUPTA
Co-Founder and Head.
Digital India Foundation

SANDIP DAS
Independent Board
Director & Advisor
Sterlite Technologies Limited

VINEET TANEJA
Corporate Advisor
Angel Investor

RAHUL AGARWAL
Investor
Advisor & Entrepreneur

AJAI CHOWDHRY
Founder
HCL

PUNIT MODHGIL
Co-Founder
Octane Research

TEJAS GOENKA
MD
Tally Solutions

MARSHAL CORREIA
Vice President and
General Manager, India
South Asia at Red Hat

SRAVANTH ALURU
Founder & CEO
Avataar.Me

SOM MITTAL
Former President
& Chairman
NASSCOM

To be a part of this wonderful journey of 35 Years of Technology, write to
Rajiv Pathak | rajivp@cybermedia.co.in | +91 8010757100

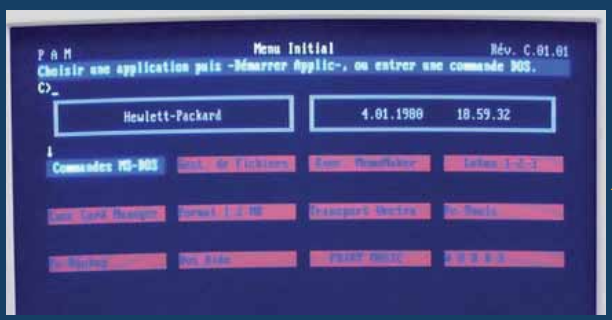
35 YEARS 1987 - 2022

Intensification of cyber attacks over the last 35 years

Ashok Pandey
ashokpa@cybermedia.co.in

Computers and the internet revolutionized the world of communication like never before, but they came under attack soon. The first worm was 'Creeper'. In 1971, Bob Thomas, a developer working on ARPANET, wrote a program that traveled from PC to PC on its own to the network to print the message: "I'm the creeper; catch me if you can". It was actually designed as a security test. In the year 1973, Thomas' colleague, Ray Tomlinson developed 'Reaper' to find and delete the Creeper worm. Therefore, if the Creeper was the world's first computer virus, the Reaper is understandably the first antivirus program. In 1986, two brothers named Basit and Amjad Farooq Alvi wrote 'Brain', which is considered to be the first virus for Windows based PCs.

1987



In 1983, ARPANET began requiring its users to conduct all network communications via a set of TCP/IP (transmission control protocol/internet protocol) conventions. While in 1987 a simple virus 'Vienna' destroyed random files on computers it infected.

Soon, German computer researcher Bernd Robert Fix wrote a program to neutralize the virus.

DID YOU KNOW ?

- Every 39 seconds, there is a new attack somewhere on the web
- 95pc of cybersecurity breaches happen due to human error
- Most companies take nearly 6-7 months to detect a data breach
- Six in every 10 attacks in 2020 intended to extort money from companies and individuals

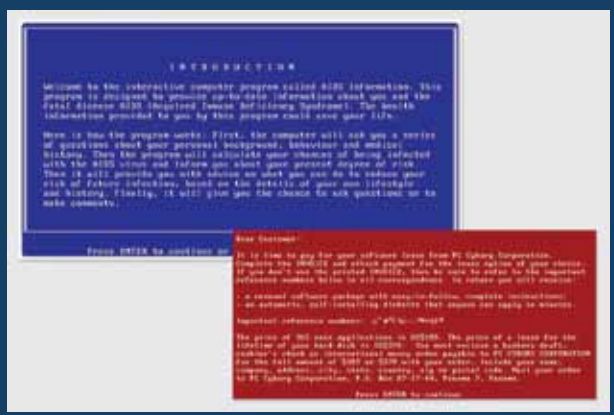
(Source: Reports from University of Maryland, IBM Security, Ponemon Institute, Verizon)

1988

Vienna was a simple virus that wasn't able to damage much. While the next and maybe the first internet worm infected and crashed about 10pc of the 60,000 internet connected PCs causing millions of dollars in damage. This worm was developed by Robert Morris, a 23-year-old graduate student from Cornell University.

1989

The first documented ransomware known as the AIDS trojan, post which the use of ransomware scams has grown internationally



1990

The increase in virus activity fueled the antivirus industry.

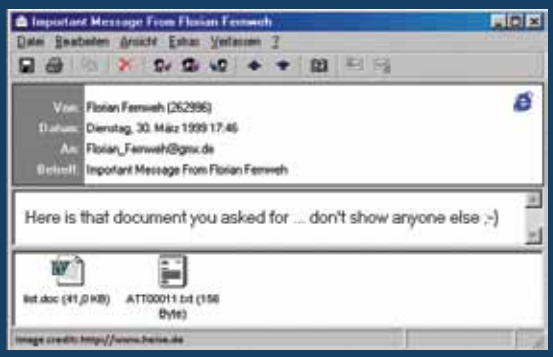
1996

The first known DDoS attack occurred when Panix, one of the oldest internet service providers, was knocked offline for several days by a SYN flood, a technique that has become a classic DDoS attack.

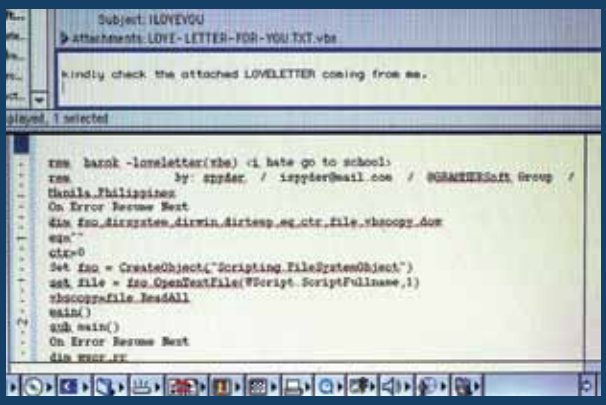
35 YEARS
1987 - 2022

1999

David Smith created a virus ‘Melissa’ that distributed itself via Microsoft Outlook that then send an email with the subject “Important Message.” and an attachment titled list.doc which, when opened, would cause a barrage of pornography sites to open. It caused $80 million of damage.



2000



Another email virus spread with the subject ‘ILOVEYOU’ and an attached file named ‘LOVE-LETTER-FOR-YOU.txt.vbs’. The infection spread so quickly that the Pentagon and the CIA shut down their email systems until the coast was clear. This virus infected more than 50 million computers.

2003

For the first time, the US government recognized viruses as a threat due to the growing number of cyberattacks. The US Gov founded the Department of Homeland Security and established the National Cyber Security Division, the first official task force dedicated to cybersecurity.

The Trusted Computing Group (TCG) developed the Trusted Platform Module (TPM) chip- a processor that can provide additional security capabilities at the hardware level. The first widely deployed TPM was TPM 1.1b with basic functions including key generation (limited to RSA keys), storage, secure authorization, and device-health attestation.

2004

Unified Threat Management (UTM) is a concept that was used for the first time in an IDC report. UTM security appliances integrate multiple security features onto a single hardware platform, including network firewall capabilities, network intrusion detection and prevention, and gateway antivirus.

2005

Coined by Mark Nicolett and Amrit Williams of Gartner, Security information and event management (SIEM) is a field where software products and services combine SIM (security information management) and SEM (security event management) functions into one security management system, providing real-time analysis of security alerts generated by applications and network hardware.

2005 was also the year of the first Data Breach to compromise more than 1 million records, when DSW Shoe Warehouse was compromised and hackers stole 1.4 million credit card numbers.

2010

Iran's nuclear program was under attack by Stuxnet, which is considered to be the world's first ever cyberweapon. It is infamous for its role in eviscerating (albeit temporarily) Iran's nuclear program – an event considered to be the first act of international cyber warfare.

John Kindervag, an analyst at Forrester Research, used the term 'zero trust' model which means that devices should not be trusted by default, even if they are connected to a permissioned network such as a corporate LAN and even if they were previously verified.

35 YEARS
1987 - 2022

2012

Traditional cybersecurity programs based on 'signatures' began to fail, thus the next-gen antivirus began using big data analysis by taking a broad, holistic view of user behaviors, network traffic, and application activity.

2013

Former CIA employee for the US Government, Edward Snowden copied and leaked classified information from the National Security Agency (NSA).

Nearly 3 billion Yahoo users' personal data was stolen leading to a $35 million fine by the SEC, and 40 consumer class action lawsuits. It was an unprecedented scale of cyberattack, yet Yahoo didn't report the largest data breach until 2016.

2015

Hackers calling themselves the "Impact Team" stole 32 million records from users of the world's leading extramarital affair site, Ashley Madison- resulting in separations, divorces, and even suicides.

2016

The first wide ranging IoT attack happened with the help of the Mirai botnet, a malware that converts IoT devices into bots, allowing anyone to build their own botnet army made of IoT devices. However, there were multiple instances of IoT attacks in the early 2000s, such as remotely hacking a sewage treatment plant, shutting down train signaling systems, halting production in auto-manufacturing plants, etc.

2017

WannaCry ransomware infects 230,000 computers in one day.

2018

The European Union began enforcing the General Data Protection Regulation (GDPR) for companies to have a response plan in case of a data breach.

2019

The year saw the rising adoption of

- Multi-Factor Authentication (MFA)
- Network Behavioral Analysis (NBA) – identifying malicious files based on behavioral deviations or anomalies
- Threat intelligence and update automation
- Real-time protection – also referred to as on-access scanning, background guard, resident shield and auto-protect
- Sandboxing – creating an isolated test environment where you can execute a suspicious file or URL
- Forensics – replaying attacks to help security teams better mitigate future breaches
- Back-up and mirroring
- Web Application Firewalls (WAF) – protecting against cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection

35 YEARS
1987 - 2022

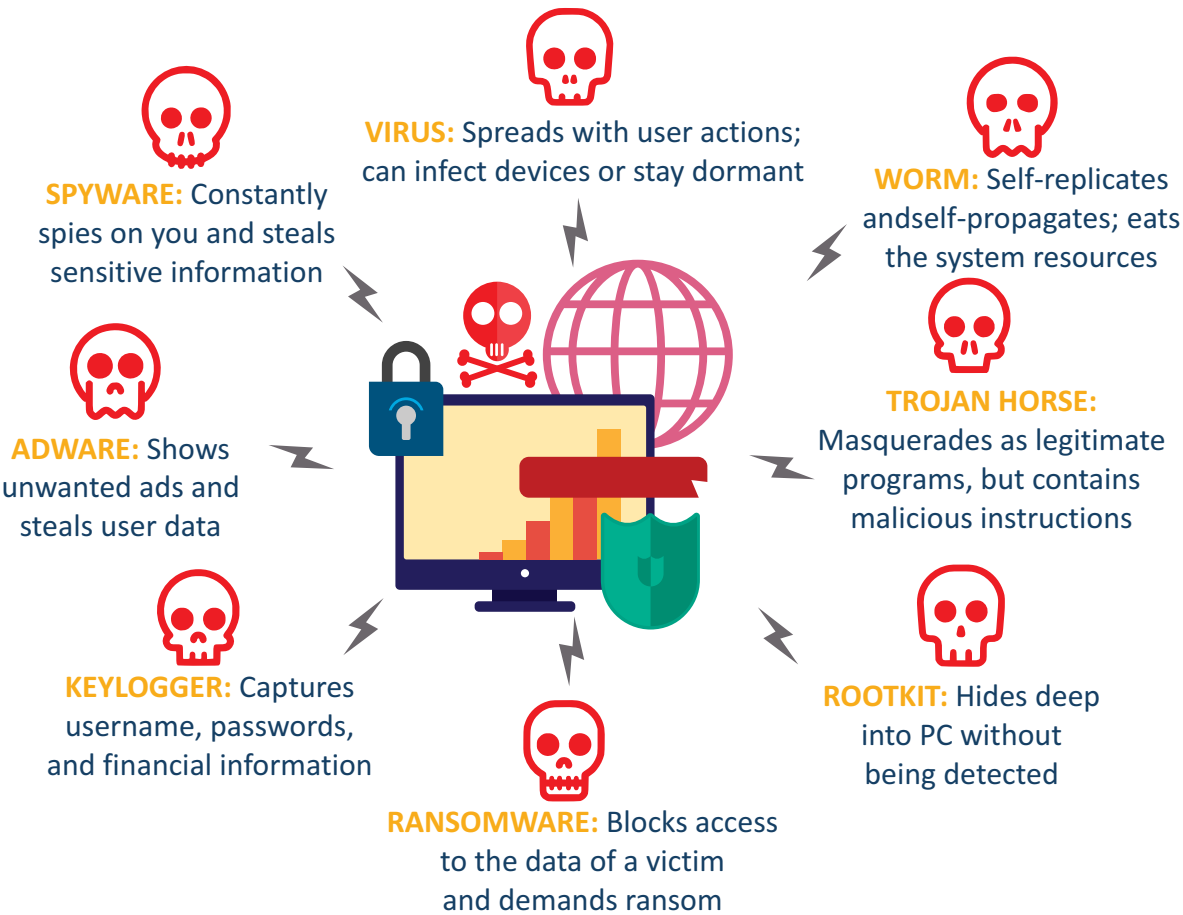
2020

US IT firm SolarWinds' Orion platform became the subject of a cyberattack that spread to its clients and went undetected for months.

2021

Russian ransomware-as-a-service gang REvil hit Apple supplier Quanta with a $50 million ransomware attack.

Types of Malwares



CyberMedia

LEADING TECH MEDIA PLATFORM & NETWORK SINCE 1982

6
Brands

3500+
Impact Articles

40+
Webinars & Virtual Roundtables

10000+
Attendees Across Verticals

150,000+
People Influenced

150+
Industry Leaders & Tech Experts

COMMUNITIES

Technology Decision Makers - Enterprise and SMB, Telecom, Channel Partners, Start-ups, DeepTech, Functional Heads and many more

MOVED THE NEEDLE DURING COVID-19 CRISIS

CREATING HIGH IMPACT & INFLUENTIAL CONTENT

IN THE LAST 661 DAYS

CMR
- From Survival to Revival
- Proactive Business Recovery
- Changing Customer Expectation in Crisis
- Cyber-Sanitize your business
- Proactive Sales Strategies for faster business recovery
- New IT Priorities 2020

CIOL
- CXO of the Week
- CiOL Live Video Series
- Start-Up Circle
- CiOL Cloud Burst
- CiOL Live Tech News

DQ Channels
- Are There any Make in India IT Products for Us to Use?
- Cloud Adoption in Digital World
- Govt to Harness IT to Empower MSME Sector

DATAQUEST
- DQ Tech Talk Series
- Business Continuity Planning Series
- Dataquest Digital Indexing
- DeepTech (India's largest Virtual Conference)

PCQUEST
- Secure Smart & Intelligent Network
- App Modernisation
- Collaboration in WFH environment
- DevOps
- CyberMedia Labs Product Review

VOICE&DATA
- Business After Covid
- TLF Dialogue Series
- 25 Years of Mobile Telephony India

and many more....

Rajiv Pathak | rajivp@cybermedia.co.in | 8010757100

https://AI

AI & Ethics: 'The dog ate my homework' excuse won't work here

Pratima H
pcquest@cybermedia.co.in

What will work is a good mix of honesty and courage to ask the right questions and the humility to go back to school, advises this veteran tech wizard whose deep-end experience straddles corporate war-rooms as well as university classrooms

The beauty of any problem is that whenever we get stuck at something, thinking it as a dead-end, just changing one's way of looking at it can be a miraculous way out of it. Everything – no matter how new or unusual- boils down to the simple and fundamental problems, principles and questions that humanity has embraced time and again. That's the drift we get while looking at the problem of AI's ethical dilemmas from the unique point of view of Information Systems Professor Tej Anand who directs Maryland Smith's newly launched Blockchain Business Imperative. He has spent the first 10 years of his career working in AI and Data research and product development in many companies such as Philips Research Laboratories, A. C. Nielsen, and NCR/Teradata. He has also worked as a senior business-technology executive in many companies and his research interests cover technology ethics and blockchain governance, among other areas. Excerpts from a conversation with a sweet voice and a strong mind.

▼ Recently there was something reassuring in AI Ethics leader Kathy Baxter's win over preserving the AI ethics responsibility over a business goal of a new product launch. But are these victories few and far between? What is your reckoning of the progress being made on the tough path of AI Ethics?

The very fact that everyone is talking about such issues and that this topic is at the front-end of people's thoughts – that means that we are in the right direction. There is still a lot of

work to do and a lot of ideas need to translate into action. This, however, should be expected not just from large-marquee companies but also from small companies that actually deploy AI. The concern is not just about the transparency of an algorithm but about how it is being used eventually. We have to make Maths subservient to critical thinking. Our world is still a juxtaposition of algorithms and human beings.

▾ But 90 per cent of customers feel companies have the responsibility to improve the state of the world (as per a Salesforce Ethical Business & Leadership Survey). When customers expect companies to handle the AI trust part – is that right? Can users shun all their responsibility?

AI Accountability is another open question. For instance, as a teacher I have a certain degree of accountability – for every grade, every lecture, every student interaction in my scope. But who is accountable for an algorithm- the company that designed it or the company who gave the data to train it or the citizens/customers whose data was used here? We have not created a framework yet. The question is complex when we think of it in terms of AI. But what if we think in terms of it as a software? When a company builds any software, should it understand the software and be accountable? When we look at some precedents here, we can find some answers easily. Software is never a turn-key deployment. There are many knobs to move up and down there, and many features to switch on and off. That's something that will happen to AI.

I would say that asking such questions is not just a sign of moral responsibility but a sound business practice too. The business value necessitates that approach.

▾ It's not easy though. There are many paradoxes here when we think of AI and Ethics.

Well, if we get the newness out and go back to basic questions, do our answers change? We learn to do things a certain way in a Maths calculus class, for instance. When we bump into a new problem, we can solve it by applying the same principles. If the parent principles apply, we get answers. If they don't apply, at least we know something better and then we can ask what has changed. Like- when the dotcom boom happened, we all thought that it would be a complete breakthrough and a new business model. Ultimately, the successful companies turned out to be the ones that worked on good-old business formulas- profitability, customer satisfaction and financial health.

▾ Speaking of that, what do you think of Web 3 Models and Metaverse?

It is getting a little muddled now. Actually when Web 3 began, it was not about Metaverse. I give an example in my class when I talk of Internet – I show an image of a farmer holding a phone, and travelling on a bullock cart. Because that's what Internet did. It was all about democratization. The whole Web 3 disruption was all about core tenets of Internet in the first place- decentralisation, democratisation and removal of middlemen. I believe in that power but I also worry if some initial players are not actually decentralised anymore. Do we want to go back to Square One?

▾ Would you agree that interoperability would be a good thing for Blockchains to ensure these core tenets?

Yes, that can help. Like what Polygon attempted. These areas help but we have to keep the non-technical people in mind. It should all be easy to use - for the average person. It should be simple to run with commodity hardware and without heavy electricity bills. We need another Hotmail moment in Blockchain. Like a catalyst that can really propel everything to the mainstream. Blockchain needs that moment. And I don't see NFTs or Crypto as that moment.

▾ What's your view of Zero Knowledge Proof models – to enhance security and privacy?

They do conform to the ethics of Blockchain. They also improve the quality of information in a Blockchain. They are successful in getting important information without sacrificing privacy. ■

Yes!
I want to subscribe to PCQuest

Subscribe to Digital Edition @ ₹1300

	Period	Issues	Print Subscription Rate		Digital Subscription Rate
			New Subs.	Renewal	
☐	1 Year	12	₹1500/-	₹1350/-	₹1300/-
☐	2 Year	24	₹3000/-	₹2700/-	₹2340/- Save 10%
☐	3 Year	36	₹4500/-	₹4050/-	₹3120/- Save 20%

or Subscribe online: subscriptions.cybermedia.co.in/pcquest

Please tick your subscription choice above, fill the form below in CAPITAL LETTERS and mail it to us at rse@cybermedia.co.in

☐ I want to avail premium service of receiving my subscription copy by courier. Tick which ever is applicable.

☐ ₹500/- 1 year, ☐ ₹950/- 2 years, ☐ ₹1400/- 3 years

Name: Mr/Ms _____ Date of Birth: M M Y Y Y Y

Organisation: _____ Designation: _____

Delivery Address: _____

_____

City: _____ State: _____ Postal Code: _____

Mob [•]: _____ Tel: _____ Email [•]: _____

☐ I am paying ₹ _____ by DD/Cheque No.: _____ Dated: M M Y Y Y Y

Payable at (specify bank and city) _____

OR

☐ **Please Remit for ₹ _____ Through RTGS/NEFT to our A/C details given below:**

Bank Name: ICICI Bank Limited A/c No. 017705000132, Branch & IFS Code: Gurgaon, ICIC0000177

[•] Essential fields

Signature _____ Date: M M Y Y Y Y Subscription No. (for renewal) _____

Order form can be mailed with payment (cheque/DD) to:

Sarita Shridhar, Cyber Media (India) Ltd, Cyber House, B-35, Sector 32, Gurgaon - 122001 Tel: 0124 - 4822222, 91-9810499208

Terms & Conditions:

• This offer is valid for a limited. • Rates and offer valid only in India. • Please allow 4-6 weeks for delivery of your first copy of the magazine by post & 8-10 weeks for delivery of your assured free gift. • Send crossed Cheques in favour of Cyber Media (India) Ltd. • Please write your name and address on the reverse side of the cheque or DD. All outstation cheques should be payable at par. • Cyber Media (India) Ltd. will not be responsible for postal delays, transit losses or mutilation of subscription form. • Cyber Media (India) Ltd. reserves the right to terminate or extend this offer or any part thereof. The decision to accept or reject any or all forms received is at the absolute discretion of the publishing company without assigning any reason. • Please include pin code for prompt devlivery of your copy. • In case payment is through credit card, date of birth must be mentioned. • Request for cancellation of subscription will not be entertained once the free gift has been dispatched. • All disputed shall be subjected to Delhi jurisdiction only.

Low-code may open AI doors for many businesses

Ashok Pandey
ashokpa@cybermedia.co.in

Every company wants to put AI in its business, but most of the businesses are not blessed with a dedicated team of developers and data scientists at their beck and call. But now they can do so even without acquiring those skill sets and **Anithalakshmi Arun, Program Manager & Architect, Low Code Practice, Indium Software** explains how low-code platforms can help...

▼ Low-code development can boost AI adoption

For any organization AI adoption is a challenge. The contributing factors include - availability of skilled resources, the cost of building AI solutions, the availability and usability of data, time taken to complete the cycle of build/deploy, time to market, cost of maintenance and making incremental improvements. Despite these challenges, the need for AI is inevitable.

Low-code, with its visual development, intuitive modeling, user-friendly graphical user interface (GUI), and pre-built integrations is a great enabler for AI adoption. AI applications involving conversational bots

using Natural language processing (NLP), Machine learning (ML), deep learning, visual recognition etc. are much simpler to build with the low-code platforms.

Not only Low-code is used to build AI-driven applications, but the platform by itself provides AI assistance in form of a 'co-pilot' utilizing ML, and predictive behaviors to understand the project needs and extend guidance, suggestions, and automation throughout the development journey.

▾ Low-code empowering businesses

Low-code/no-code empowers business agility and accelerates business outcomes, primarily because it bridges the gap between business and IT with the democratization of application development. Business teams, with their better understanding of end customers, are ideal candidates to build and test applications that have a greater chance of success with the customers.

Intuitive drag and drop of templates, forms, in-built applications, a visual integrated development environment (IDE), model-driven environment with connectors and out-of-the-box widgets to connect with multiple systems breaks the barrier of programming and coding skills. Though it does not mean that citizen developers will replace programmers, there is an opportunity for them to evolve beyond their current function.

▾ Revolutionizing digital transformation

All businesses attempt to become customer-centric and focus on enhancing customer experience. And digital transformation is a key step towards this goal. Unlike the past, where tech teams were driving IT projects, Digital transformation initiatives are primarily driven by business teams. They want to try out new things, apps, workflows to know what's working or not working with their customers. And the competition as such, they are always in a hurry. This is where low-code comes into the picture.

With a drag and drop interface and with minimal support from IT, business teams can create apps, workflows and explore what works for their business and their customers, extremely reducing the time to market.

▾ The rapid adoption of low-code cloud-based software

Most low-code/no-code platforms are PaaS (Platform-as-a-service). Hence, the need to build and invest in on-premise infrastructure is long gone. Also, most low-code platforms have built-in automated testing, deployment, and security (DevSecOps). The platform's agility, scalability, and convenience reduce software development effort and time to a fraction of the traditional methods.

▾ Aiding intelligent business process management

Low-code /no-code platforms are bundled with built-in tools for creating business rules and to set approval workflows. The platforms are feature-rich with Workflow designer, Form modeling, Role-based Access Control, KPI based reports and dashboards, Notifications with email and mobile application alerts for quick intervention, Configurable Checklists and Audit Points, and Exceptions rule configurations. The best part is these are mostly wizard based and can be built by a citizen developer.

▾ Future of low-code/no-code development in terms of enterprise resilience

According to Forrester, the low-code automation market was worth $4 billion in 2019 and is likely to hit $21.2 billion by 2022. According to Gartner's Low-Code Development Technologies Evaluation Guide from 2019, 75 per cent of large enterprises will use at least four low-code development tools for IT application development and citizen development by 2024.

Gone are the days when enterprises used multiple platforms to develop and maintain multiple applications. The overhead cost of maintenance and non-uniformity caused a lot of inefficiencies. Investing in a single platform for application development across the organization led to efficient management on a single platform, which included reliability, security, scalability, and infrastructure monitoring. This also reduces the total cost of ownership across the geographical region and business units. ■

https://METAVERSE

What it takes to build a human-centric Metaverse

V. Srinivasa Rao
pcquest@cybermedia.co.in

It will take time to unlock the full potential and to experience all features of the Metaverse. The hardware to get an immersive experience within Metaverse may not be affordable to all people at this juncture and we certainly can't ignore the possible negative implications

We as human beings have a few dreams which we can't realize due to so many constraints - could be financial, skills, stamina, IQ and others! For example, I dream of conversing with Karna and Lord Srikrishna, Bheeshma, and Suyodhan in Hastinapur in the Raj Darbar. I could meet them and have a conversation to stop the Mahabharat War. Yes, it is possible for you just by sitting at home.

I want to meet my close friend who is 8,000 miles away but not able to. So, imagine that within a few seconds, I will be at my friend's home in the USA, and we both have a personalized conversation. Once done, I will come back to my home in India. All I could do without even going out just from home.

Ghantasala, SP Balasubramanyam, and Kishorekumar's music program is happening, and I want to attend that concert, enjoy the show in a big crowd just sitting at home.

My daughter is struggling to understand the planet Mars. So, my daughter and I go to Mars and then explore and experience the geography of Mars, all just by sitting at home. We do not need to spend millions of dollars to go to Mars using Elon Musk's Space Shuttle.

All this looks like fiction and probably reminds us of old mythology films. But do not worry; Metaverse is here to give that experience.

▾ Web 3.0, Hardware, variety of Metaverse and its affordability

In Web 1.0, people started viewing static web pages over the internet in which the provider-maintained content. In the era of Web 2.0, people started generating content themselves using social media; there is a lot of interaction over webpages and software applications and have been communicating and collaborating using audio/video conference, telepresence, accessing videos and seeing movies.

In both Web 1.0 and 2.0 eras, people just viewed and interacted with the internet /web. Welcome to Web 3.0, in which people live and immerse into the web. Metaverse is

V. SRINIVASA RAO, Chairman- Open Digital Innovation, IET Future Tech Panel and Chairman & MD, BT&BT

the real-life application of Web 3.0.

In Metaverse the virtual universe connects with the physical universe (where we live) and allows the people (in their digital avatar) to work, play, stay connected with friends, attend conferences, concerts, make virtual trips, and do virtual shopping in their preferred places anywhere in the world.

Many complex technologies are required to connect the Virtual Universe with the Physical Universe to unlock the true potential of Metaverse.

- People need to wear Virtual Reality (VR) headset, VR Suit, Haptic gloves (for

What is Metaverse?

Meta means BEYOND, and Verse means UNIVERSE. That means we are creating a new universe beyond our physical limitations using technologies and will get immersed into this new universe to explore and experience the unexplored things in our life due to various constraints.

Technologies like virtual reality, augmented reality, artificial intelligence, sophisticated modeling techniques, electromyography, Blockchain, 3D reconstruction, Internet of Things create this new universe.

Metaverse is a new imaginative three-dimensional virtual universe created with the digital version of physical places and things (the virtual replica or digital twin), virtual places and things and People (in the form of Avatars).

human body motion and touch), and Augmented Reality (AR) glasses.

- Brain Computer Interface (BCI) to send the human brain electrical pulses in the form of actions to its Virtual Replica (Avatar)) of the person in the Metaverse.
- Internet of Things (IoT) to send the data from physical places/things to its virtual replica in Metaverse (Digital Twin).

Metaverse is still in the incubation phase, and it will take a few more years to reach its mature stage. Having said this, Metaverse could be used in education, healthcare, entertainment, e-commerce, and other industries. There will not be one Metaverse, and we might have Consumer Metaverse, Business Metaverse, Industry Metaverse, Society Metaverse, Government Metaverse, Entertainment Metaverse, Healthcare Metaverse, Education Metaverse, etc.

Metaverse creates a virtual world and helps people get experiential learning of new skills, helps innovators explore various alternatives before designing best in class products, and youth enjoy entertaining events and many more.

As Metaverse is run on the internet, it can be accessed from anywhere, anytime, irrespective of cities or villages. However, the hardware to get an immersive experience within Metaverse is expensive at this juncture. Therefore, to unlock the full potential and to experience all features of the Metaverse, it may not be affordable to all people at this juncture.

▼ Minimizing the side effects/negative effects of Metaverse

While Metaverse has many advantages, we can't ignore the negative implications. A few examples are:

- Metaverse Bullying with griefers (A person who harasses or deliberately provokes other people (Avatars) to spoil their enjoyment) creates a lot of challenges for people. Male Avatars may create an embarrassing situation for Women Avatars.
- Metaverse needs a lot of moderators and safety measures to ensure that they block the people (Avatars) who are involved in hate speech, spreading misinformation, etc.
- Develop Metaverse Etiquette to unlock the true potential of Metaverse with minimal or no side/adverse effects.

- Mobile phones, the Internet, social media have impacted culture, family relationships and family values. With Metaverse, imagine if all the family members wear VR headsets or AR glasses and spend longer time in the imaginary virtual world, that would impact relationships and lead to physical and mental illnesses.
- Dark Metaverse may emerge in which illegal and unethical activities may be performed by a few people in the form of their AVATARS and may impact their behaviors to involve in crimes in the real world.
- Many youths may get addicted to Porn Metaverses to get immersive sex experience, and it may cause significant distractions and may seriously impact their education and future.
- A lot of data about people will be available through Avatars (actions, conversations, connections, etc.) in the Metaverse and hence safeguarding people's safety and privacy is crucial.

Need for Metaverse Hardware and Avatars Innovations

The Metaverse's avatars need a lot of improvement to exactly resemble the actual person. A lot of work is happening in this area. We used to have massive computers a few years back, and now we are getting computers in miniature forms like wearable devices and mobile phones. Similarly, the innovations are required to optimize the size of VR Headsets, AR glasses and other Metaverse infrastructure. Metaverse also requires high processing GPUs and high bandwidth using 5G. It may take 5-10 years to enjoy the fruits of Metaverse at an affordable price. ■

The author is Chairman- Open Digital Innovation, IET Future Tech Panel and Chairman & MD, BT&BT

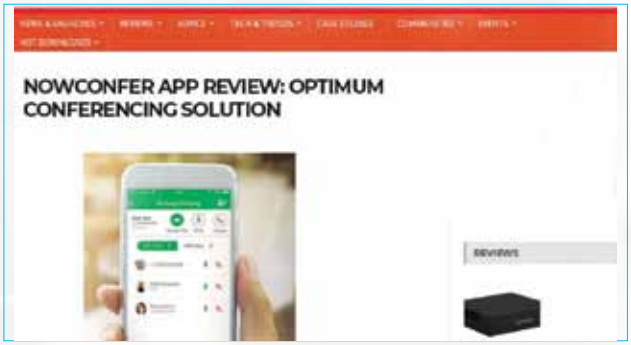
Real life applications of Metaverse

- Nike bought a virtual shoe company to sell the same within Metaverse using Blockchain Non-Fungible Tokens (NFT). That means Nike set up its showroom in Metaverse, and People (in their avatar form) purchase virtual shoes by paying for cryptocurrencies.
- Decentraland established a real estate Metaverse in which people purchase virtual land parcels using Blockchain Non-Fungible Tokens. Later, they could construct their own virtual offices, virtual shopping malls, virtual entertainment theatres in Decentraland.
- Facebook has started many Metaverse initiatives like Horizon Home, Gaming, Fitness and Education.
- Microsoft Mesh has been creating Collaboration Workplaces within Metaverse to improve employee productivity and engagement.
- The Sandbox is a virtual world where players can build, own, and monetize their gaming experiences in the Ethereum blockchain.

PRODUCT REVIEWS

A Powerful Marketing Vehicle

Thousands & thousands of products are launched every year. But a bunch of them are reviewed. A good product backed by experts' review translate into increased user interest and hence sales. Get your product reviewed by CyberMedia Labs which is run by a team of experts/product technologists having 10+ years of experience.



For more product reviews by CyberMedia Labs

SOME OF THE CATEGORIES CYBERMEDIA LABS SPECIALIZES IN:

• Firewalls	• UTMs	• Thin Clients
• IT Infrastructure Hardware & Software	• Networking Devices	• Printers & MFDs
• Audio Equipment	• Cameras	• Smartphones & Tablets
• TVs & Display	• Computers & Laptops	• Tools
• Games	• Mobile Apps	• Imaging

PCQUEST DATAQUEST CIOL VOICE&DATA DQ Channels THE DQ WEEK

To leverage the opportunity of product reviews by CyberMedia Labs

Contact us:
Rajiv Pathak
Marketing
marketing@cybermedia.co.in,
+91 8010757100, 0124 482 2222, ext: 219

Ashok Pandey
ashokpa@cybermedia.co.in

GRAPHIC CARD

AMD

RADEON RX 6600 XT GRAPHICS CARD

Price: **₹ 31,990**

Overall: 9/10

SCORE
PRICE: **8/10**
PERFORMANCE: **9/10**
FEATURES: **9/10**

KEY SPECS
Boost Clock : up to 2607 MHz (Reference card: 2589 MHz); Game Clock : up to 2428 MHz (Reference card: 2359 MHz); Stream Processors - 2048; Memory Clock - 16000 MHz; Memory Size - 8 GB; Memory Type - GDDR6; Memory Bus - 128 bit; Memory Bandwidth (GB/sec) -256 GB/s; Card Bus - PCI-E 4.0 x 8; Digital max resolution - 7680x4320; Multi-view - 4

PROS:
Good gaming performance; 4K resolution, suports up to 8k; Runs cool; Silent

CONS:
No major overclocking gains

AMD introduced its new graphics card for the new age graphics card Radeon RX 6600 XT GPU. The AMD Radeon graphics card has basic reference designs of RX 6600 XT cards. The GPU is positioned on the boundary of high-performance 1080p and midrange 1440p play in AMD's stack, at least in terms of power.

Setting a new standard for 1080p gaming, the Radeon RX 6600 XT harnesses breakthrough RDNA 2 gaming architecture, 32MB of Infinity Cache, AMD Smart Access Memory and powerful software features such as AMD FidelityFX Super Resolution, AMD Radeon Boost, and AMD Radeon Anti-Lag to provide an exceptional gaming experience.

Performance

To test the gaming GPU we installed this machine on our test bed (3.6 GHz Intel Core i7 CPU on Gigabyte motherboard, 8 GB Kingston RAM, WD 512 GB SSD, ViewSonic gaming monitor running on Windows 10 OS). We ran through various synthetic and real-world testing and focused on the esports aspect of the card. We also ran tests to know the card's abilities to handle AAA games.

To check its real world's capabilities, we installed games like Assassin's Creed: Odyssey, The Thief, Shadow of Mordor and Halo Infinite. The RX 6600 XT is a midrange GPU focused on 1080p performance and offers the AAA gaming experience.

Playing games like Halo, Thief, NFS, etc. on it is a pleasure. It is silent, cool and comes factory overclocked at a boost frequency of 2607 MHz. With it, you can play all games perfectly at up to 8K at 7680X4320. You can play all the modern and latest games on this FHD to 8K card.

To overclock this card, one can use AMD's Radeon Software utility, I was able to achieve a small, yet stable boost. However, there was no significant performance gains with manual overclocking. The AMD GPU delivered awesome performance on synthetic benchmarks and scored 59347 on Geekbench, 7546 on 3D Mark 11, 11513 on 3D graphics mark, 8427 on GPU Basemark, and 3632 on Unigine Heaven Benchmark.

Bottomline: The mid-range AMD Radeon RX 6600 XT graphics card comes with decent overclock capability and RDNA 2 gaming architecture. It is an efficient GPU that can handle up to 8k resolution and four monitors at a time. This card is offering rich gaming performance, yet is available at a slightly higher price point.

https:// REVIEW

Ashok Pandey
ashokpa@cybermedia.co.in

ZUNPULSE

SMART BULB 12W

SMART BULB

Price: **₹ 1,090, (₹ 640 on Flipkart)**

Is there any good news? Enjoy that with colorful light and soothing music. But to do so, you need a smart bulb, like Zunpulse Smart Bulb 12W. The smart bulb allows you to control your home's ambience with your phone and choose from 16 million colors, brightness control, temperature control, and 8 preset modes all in the same smart bulb.

Setup

It's a LED bulb with smart features and wireless connectivity. You can install it in B22 holder and switch on the power. To use the smart features, you can install the Zunpulse app from Google Play and the Apple app store. Using the app you can set up the bulb with your Wi-Fi network. Follow the instructions on the app to connect your bulb with Wi-Fi. Once setup is done you can connect the bulb with your voice assistant – Amazon Alexa or Google Home.

Setup on the app is fairly easy, even it helps you to connect the bulb with your smart assistant but you might face some difficulties while doing that. I had to do it manually and that too took a huge effort.

Features

Zunpulse Smart Bulb offered global remote access which provides you with multi-user access from any time or any place to your smart bulb. One can easily manage the bulb using a smartphone or smart assistants like Alexa and Google Home. If you moved out, without turning your bulbs off, you would receive notifications to turn them off.

Using the app you can control the brightness of the bulb. You can change the bulb color to any one of your favourites. Having almost 16 million color options, you could set your room's ambience as per your mood. It comes with 8 preset modes and 3 lighting modes, one can create numerous ambiences as per one's mood.

Overall: 8/10

SCORE

PRICE: **9/10**
PERFORMANCE: **8/10**
FEATURES: **8/10**

KEY SPECS
Wi-Fi 2.4 GHz; Alexa, Google Assistant and Android/iOS compatible; !2 watt; 16 million color; 8 pre-set modes - party, music, date, reading, baby, meditation, movie and plant

PROS:
8 preset modes and 3 lighting modes, intuitive app

CONS:
Alexa setup can trouble

Performance

Having different preset modes, you can make your movie experience fun with a stunning ambience. You can turn your weekend fun by setting the party ambience or perfect bright light for a soothing reading experience. It also has a plant mode for growing houseplants, this mode helps to increase the rate of growth.

We are using this smart bulb for the last three weeks, the light brightness is decent enough. It works perfectly in different color schemes. The app interface is quite intuitive, anyone can access different settings easily and set the scene and schedule the On/Off timer. The only challenge we faced was the Amazon Alexa setup, it took a lot of effort. Modes like movie, date, meditation etc. work perfectly but with music and party mode it only changes the color of light, there is no music sync available hope Zunpulse would add it in future. ■

Bottomline: You can change the color as per your mood, different preset modes and various other features. This smart light is available at an affordable price and can be set up with your voice assistant.

Ashok Pandey
ashokpa@cybermedia.co.in

SMART PLUG

ZUNPULSE

SMART PLUG 16A

Price: **₹ 1,490, (₹ 469 on Tata Cliq)**

Do you want to convert your home into a smart but at an affordable price? Zunpulse smart plus lets you control and monitor your appliances smartly. This smart 16A plug can be connected to any 16A plug to connect non-smart appliances like their Fridge, TV, Geyser, etc.

Build and features

The smart plug has a round shape with three plug pins and one power button on it. The outer shell is made of solid plastic. It is a kind of extension to your existing plug but with smart features. Just plug it into any regular socket and then plug your appliance. Press the power button placed on the smart plug and it will start blinking, looking for connectivity.

Install the Zunpulse app available from Google and Apple app store. Follow some simple steps to connect the plug to your wi-fi and Alexa or Google

Overall: 8/10

SCORE

PRICE: **9/10**
PERFORMANCE: **8/10**
FEATURES: **8/10**

KEY SPECS
2.4 Ghz Wi-Fi Connectivity; Power Supply Control; Global Remote Access; Plug and Play

PROS:
Elegant design, solid body, remote control and schedule

CONS:
Alexa setup can trouble

Home devices for voice control.

Performance

Setting up the smart plug would take a few minutes only, the app configuration is also quite simple. Alexa can trouble you to set up for voice command. Once setup is done, you can easily create a schedule for your geyser or coffee maker kind of appliance. If you forgot to turn off your appliance, even when you are not at home, you can control them wirelessly. It works smoothly without giving you any trouble. Scheduling comes handy for your trouble-free mornings, also when you are coming back home. ■

Bottomline: At a fairly decent price, Zunpulse smart plug is a perfect choice to convert your home into smart. This plug lets you control any of your appliances remotely and even you can create a schedule for them.

https:// REVIEW

Ashok Pandey
ashokpa@cybermedia.co.in

KENT

CAMEYE HOMECAM 360

HOMECAM

Price: **₹ 4,990**

You always try to keep your eyes on your family, whether child or elderly, you want to keep them safe from potential dangers. KENT CamEye can become your third eye. The HomeCam 360 Wi-Fi camera is fully-equipped with numerous features including 360° Panoramic View and smart AI-based alerts.

Setup and features

The next generation smart Wi-Fi home camera has a small footprint that can be installed on any flat surface. You can also mount it using an optional mounting kit to mount on a wall or ceiling. Beneath, you can find one micro-USB port for power, a MicroSD card slot for video recording up to 128 GB and a mic. At the back, a speaker is placed enabling two-way communication. It supports wireless connectivity Wi-Fi 2.4 GHz, simply connect the camera to your home or office Wi-Fi to track all the activities live or when you get some motion alerts.

HomeCam 360 has a 2 MP camera that can record videos in FHD (1080p) resolution at 15 fps. It can rotate 360 degrees horizontally and 60 degrees vertically. It also supports night vision up to 9.15 meters (30 feet).

To set up, plug the camera into a power source, it will rotate and then the light will blink and it will scan the available wi-fi network. You can scan the given QR code printed at the back to install the Kent CamEye app from Google and Apple app store. The App is quite easy to use with a user-friendly interface. Signup on the app, then give it a name and connect to your home/office wi-fi. Once done, you get 15 days of free cloud recording.

Performance

This 360-degree camera packs smart AI-based alerts to help you safeguard your home and family from potential dangers. You can see every corner of your room clearly with a 2 MP 1080p camera even at night. It comes with AI motion detection that alerts you whenever there is any movement in the room. It also rotates automatically to follow a moving person or object. If you want to speak to your children or elderly, then you can do that using its 2-way calling via the app or Alexa device.

It also comes with an automatic privacy mode that lets you disable live streaming and recording basis phone's geo-location or pre-set time. The intruder alarm is quite useful when your children or elderly are alone, it raises a loud audible alarm on detecting motion or human.

The free subscription ends in 15 days, so to continue to cloud recording KENT would charge you INR 400 for a month. There are different plans that you can choose as per your requirement. If you don't want to go for a subscription, can record it on your MicroSD card. Using the app you can rotate the camera in different directions. It gives you clear video with wide coverage. You can change the video streaming quality from low (360p), medium (720p) to high (1080p). ■

Overall: 9/10

SCORE

PRICE: **9/10**
PERFORMANCE: **9/10**
FEATURES: **9/10**

KEY SPECS
2 MP Camera; FHD (1080p) video quality @15 fps; microSD Card up to 128 GB; Night Vision up to 9.15 meter (30 feet); 6 Infrared LEDs; Wi-Fi 2.4 GHz

PROS:
360/65-degree rotation, price, 2-way calling, night vision

CONS:
None

Bottomline: With two-way calling, motion sensors and various alert options, Kent CamEye HomeCam 360 is a perfect camera to track your family. The app is intuitive and lets you customise settings as per your requirements. Decently priced HomeCam 360 comes with a pocket-friendly cloud subscription plan.

nemasis®
Vulnerability Management Suite

REDUCE THE SECURITY RISK TO YOUR IT ECOSYSTEM

with Nemasis PRO and get a better understanding of any vulnerabilities in your network.

Key Features:

- Reports in Compliances format.
- Real-time Customizable Dashboards
- Credential Management for Authenticated Scans
- Integration with other solutions (SIEM, CRM, Log Aggregators)
- Passive Vulnerability Scanner (PVS)
- Alerting Actions
- Distributed Scanner Support
- Data Analysis and Output Formats

Scan QR code & get your FREE trial for **Nemasis** NOW!!!

MicroWorld Technologies Inc.
Email: sales@nemasisva.com

An ISO 27001 Certified Company
Website: www.nemasisva.com

RNI No. 45949/87 DPR No. DL(S)17/3319/2020-22 (Published on 1st of every month)
Posting Date: 12&13 every month. Posted at Lodhi Road HPO